



Cisco IOS Security Configuration Guide: Secure Connectivity

Release 12.2SR

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco IOS Security Configuration Guide: Secure Connectivity
© 2009 Cisco Systems, Inc. All rights reserved.



About Cisco IOS and Cisco IOS XE Software Documentation

Last Updated: March 5, 2009

This document describes the objectives, audience, conventions, and organization used in Cisco IOS and Cisco IOS XE software documentation, collectively referred to in this document as Cisco IOS documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

- [Documentation Objectives, page i](#)
- [Audience, page i](#)
- [Documentation Conventions, page ii](#)
- [Documentation Organization, page iii](#)
- [Additional Resources and Documentation Feedback, page xi](#)

Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section includes the following topics:

- [Typographic Conventions, page ii](#)
- [Command Syntax Conventions, page ii](#)
- [Software Conventions, page iii](#)
- [Reader Alert Conventions, page iii](#)

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to <i>public</i> , do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
<i>italic</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS uses the following program code conventions:

Convention	Description
Courier font	Courier font is used for information that is displayed on a PC or terminal screen.
Bold Courier font	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

The Cisco IOS documentation set uses the following conventions for reader alerts:



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

- [Cisco IOS Documentation Set, page iv](#)
- [Cisco IOS Documentation on Cisco.com, page iv](#)
- [Configuration Guides, Command References, and Supplementary Resources, page v](#)

Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
 - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS features.
 - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Cisco IOS XE, and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in [Table 2 on page xi](#).

Configuration Guides, Command References, and Supplementary Resources

[Table 1](#) lists, in alphabetical order, Cisco IOS and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

[Table 2](#) lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS AppleTalk Configuration Guide</i>	AppleTalk protocol.
<i>Cisco IOS XE AppleTalk Configuration Guide</i>	
<i>Cisco IOS AppleTalk Command Reference</i>	
<i>Cisco IOS Asynchronous Transfer Mode Configuration Guide</i>	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.
<i>Cisco IOS Asynchronous Transfer Mode Command Reference</i>	

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> <i>Cisco IOS Bridging Command Reference</i> <i>Cisco IOS IBM Networking Command Reference</i>	<ul style="list-style-type: none"> Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
<i>Cisco IOS Broadband and DSL Configuration Guide</i> <i>Cisco IOS XE Broadband and DSL Configuration Guide</i> <i>Cisco IOS Broadband and DSL Command Reference</i>	Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).
<i>Cisco IOS Carrier Ethernet Configuration Guide</i> <i>Cisco IOS Carrier Ethernet Command Reference</i>	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).
<i>Cisco IOS Configuration Fundamentals Configuration Guide</i> <i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i> <i>Cisco IOS Configuration Fundamentals Command Reference</i>	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
<i>Cisco IOS DECnet Configuration Guide</i> <i>Cisco IOS XE DECnet Configuration Guide</i> <i>Cisco IOS DECnet Command Reference</i>	DECnet protocol.
<i>Cisco IOS Dial Technologies Configuration Guide</i> <i>Cisco IOS XE Dial Technologies Configuration Guide</i> <i>Cisco IOS Dial Technologies Command Reference</i>	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).
<i>Cisco IOS Flexible NetFlow Configuration Guide</i> <i>Cisco IOS Flexible NetFlow Command Reference</i>	Flexible NetFlow.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS H.323 Configuration Guide</i>	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
<i>Cisco IOS High Availability Configuration Guide</i> <i>Cisco IOS XE High Availability Configuration Guide</i> <i>Cisco IOS High Availability Command Reference</i>	A variety of High Availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
<i>Cisco IOS Integrated Session Border Controller Command Reference</i>	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).
<i>Cisco IOS Intelligent Services Gateway Configuration Guide</i> <i>Cisco IOS Intelligent Services Gateway Command Reference</i>	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
<i>Cisco IOS Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS XE Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS Interface and Hardware Component Command Reference</i>	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
<i>Cisco IOS IP Addressing Services Configuration Guide</i> <i>Cisco IOS XE Addressing Services Configuration Guide</i> <i>Cisco IOS IP Addressing Services Command Reference</i>	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
<i>Cisco IOS IP Application Services Configuration Guide</i> <i>Cisco IOS XE IP Application Services Configuration Guide</i> <i>Cisco IOS IP Application Services Command Reference</i>	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
<i>Cisco IOS IP Mobility Configuration Guide</i> <i>Cisco IOS IP Mobility Command Reference</i>	Mobile ad hoc networks (MANet) and Cisco mobile networks.
<i>Cisco IOS IP Multicast Configuration Guide</i> <i>Cisco IOS XE IP Multicast Configuration Guide</i> <i>Cisco IOS IP Multicast Command Reference</i>	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS IP Routing Protocols Configuration Guide</i> <i>Cisco IOS XE IP Routing Protocols Configuration Guide</i> <i>Cisco IOS IP Routing Protocols Command Reference</i>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
<i>Cisco IOS IP SLAs Configuration Guide</i> <i>Cisco IOS XE IP SLAs Configuration Guide</i> <i>Cisco IOS IP SLAs Command Reference</i>	Cisco IOS IP Service Level Agreements (IP SLAs).
<i>Cisco IOS IP Switching Configuration Guide</i> <i>Cisco IOS XE IP Switching Configuration Guide</i> <i>Cisco IOS IP Switching Command Reference</i>	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
<i>Cisco IOS IPv6 Configuration Guide</i> <i>Cisco IOS XE IPv6 Configuration Guide</i> <i>Cisco IOS IPv6 Command Reference</i>	For IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document at the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
<i>Cisco IOS ISO CLNS Configuration Guide</i> <i>Cisco IOS XE ISO CLNS Configuration Guide</i> <i>Cisco IOS ISO CLNS Command Reference</i>	ISO connectionless network service (CLNS).
<i>Cisco IOS LAN Switching Configuration Guide</i> <i>Cisco IOS XE LAN Switching Configuration Guide</i> <i>Cisco IOS LAN Switching Command Reference</i>	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
<i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</i>	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
<i>Cisco IOS Mobile Wireless Home Agent Configuration Guide</i> <i>Cisco IOS Mobile Wireless Home Agent Command Reference</i>	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
<i>Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</i>	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
<i>Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide</i> <i>Cisco IOS Mobile Wireless Radio Access Networking Command Reference</i>	Cisco IOS radio access network products.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i> <i>Cisco IOS XE Multiprotocol Label Switching Configuration Guide</i> <i>Cisco IOS Multiprotocol Label Switching Command Reference</i>	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
<i>Cisco IOS Multi-Topology Routing Configuration Guide</i> <i>Cisco IOS Multi-Topology Routing Command Reference</i>	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
<i>Cisco IOS NetFlow Configuration Guide</i> <i>Cisco IOS XE NetFlow Configuration Guide</i> <i>Cisco IOS NetFlow Command Reference</i>	Network traffic data analysis, aggregation caches, export features.
<i>Cisco IOS Network Management Configuration Guide</i> <i>Cisco IOS XE Network Management Configuration Guide</i> <i>Cisco IOS Network Management Command Reference</i>	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS Software (XSM Configuration).
<i>Cisco IOS Novell IPX Configuration Guide</i> <i>Cisco IOS XE Novell IPX Configuration Guide</i> <i>Cisco IOS Novell IPX Command Reference</i>	Novell Internetwork Packet Exchange (IPX) protocol.
<i>Cisco IOS Optimized Edge Routing Configuration Guide</i> <i>Cisco IOS Optimized Edge Routing Command Reference</i>	Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
<i>Cisco IOS Quality of Service Solutions Configuration Guide</i> <i>Cisco IOS XE Quality of Service Solutions Configuration Guide</i> <i>Cisco IOS Quality of Service Solutions Command Reference</i>	Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED).
<i>Cisco IOS Security Configuration Guide</i> <i>Cisco IOS XE Security Configuration Guide</i> <i>Cisco IOS Security Command Reference</i>	Access control lists (ACLs), authentication, authorization, and accounting (AAA), firewalls, IP security and encryption, neighbor router authentication, network access security, network data encryption with router authentication, public key infrastructure (PKI), RADIUS, TACACS+, terminal access security, and traffic filters.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Service Selection Gateway Configuration Guide</i> <i>Cisco IOS Service Selection Gateway Command Reference</i>	Subscriber authentication, service access, and accounting.
<i>Cisco IOS Software Activation Configuration Guide</i> <i>Cisco IOS Software Activation Command Reference</i>	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
<i>Cisco IOS Software Modularity Installation and Configuration Guide</i> <i>Cisco IOS Software Modularity Command Reference</i>	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes and patches.
<i>Cisco IOS Terminal Services Configuration Guide</i> <i>Cisco IOS Terminal Services Command Reference</i> <i>Cisco IOS XE Terminal Services Command Reference</i>	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
<i>Cisco IOS Virtual Switch Command Reference</i>	<p>Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP).</p> <p>Note For information about virtual switch configuration, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.</p>
<i>Cisco IOS Voice Configuration Library</i> <i>Cisco IOS Voice Command Reference</i>	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
<i>Cisco IOS VPDN Configuration Guide</i> <i>Cisco IOS XE VPDN Configuration Guide</i> <i>Cisco IOS VPDN Command Reference</i>	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy, L2TP extended failover, L2TP security VPDN, multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82: tunnel assignment ID, shell-based authentication of VPDN users, tunnel authentication via RADIUS on tunnel terminator.
<i>Cisco IOS Wide-Area Networking Configuration Guide</i> <i>Cisco IOS XE Wide-Area Networking Configuration Guide</i> <i>Cisco IOS Wide-Area Networking Command Reference</i>	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25.
<i>Cisco IOS Wireless LAN Configuration Guide</i> <i>Cisco IOS Wireless LAN Command Reference</i>	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title	Description
<i>Cisco IOS Master Command List, All Releases</i>	Alphabetical list of all the commands documented in all Cisco IOS releases.
<i>Cisco IOS New, Modified, Removed, and Replaced Commands</i>	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
<i>Cisco IOS Software System Messages</i>	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software.
<i>Cisco IOS Debug Command Reference</i>	Alphabetical list of debug commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at the following URL: http://www.cisco.com/go/mibs
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2008–2009 Cisco Systems, Inc. All rights reserved.



Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

Last Updated: March 5, 2009

This document provides basic information about the command-line interface (CLI) in Cisco IOS and Cisco IOS XE software and how you can use some of the CLI features. This document contains the following sections:

- [Initially Configuring a Device, page i](#)
- [Using the CLI, page ii](#)
- [Saving Changes to a Configuration, page xii](#)
- [Additional Information, page xii](#)

For more information about using the CLI, see the “[Using the Cisco IOS Command-Line Interface](#)” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the “[About Cisco IOS and Cisco IOS XE Software Documentation](#)” document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

**Note**

The AUX port on the Route Processor (RP) installed in a Cisco ASR1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

- [Understanding Command Modes, page ii](#)
- [Using the Interactive Help Feature, page v](#)
- [Understanding Command Syntax, page vi](#)
- [Understanding Enable and Enable Secret Passwords, page viii](#)
- [Using the Command History Feature, page viii](#)
- [Abbreviating Commands, page ix](#)
- [Using Aliases for CLI Commands, page ix](#)
- [Using the no and default Forms of Commands, page x](#)
- [Using the debug Command, page x](#)
- [Filtering Output Using Output Modifiers, page x](#)
- [Understanding CLI Error Messages, page xi](#)

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

[Table 1](#) lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1 *CLI Command Modes*

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	Router>	Issue the logout or exit command.	<ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the enable command.	Router#	Issue the disable command or the exit command to return to user EXEC mode.	<ul style="list-style-type: none"> • Issue show and debug commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the configure terminal command.	Router(config)#	Issue the exit command or the end command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the interface command.	Router(config-if)#	Issue the exit command to return to global configuration mode or the end command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the line vty or line console command.	Router(config-line)#	Issue the exit command to return to global configuration mode or the end command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the reload command. Press the Break key during the first 60 seconds while the system is booting.	rommon # > The # symbol represents the line number and increments at each prompt.	Issue the continue command.	<ul style="list-style-type: none"> Run as the default operating mode when a valid image cannot be loaded. Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on the Cisco ASR1000 series router)	<p>The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload.</p> <ul style="list-style-type: none"> A user-configured access policy was configured using the transport-map command, which directed the user into diagnostic mode. The router was accessed using an RP auxiliary port. A break signal (Ctrl-C, Ctrl-Shift-6, or the send break command) was entered, and the router was configured to enter diagnostic mode when the break signal was received. 	Router(diag) #	<p>If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode.</p> <p>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI.</p> <p>If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.</p>	<ul style="list-style-type: none"> Inspect various states on the router, including the Cisco IOS state. Replace or roll back the configuration. Provide methods of restarting the Cisco IOS software or other processes. Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components. Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```



Note

A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. [Table 2](#) describes how to use the Help feature.

Table 2 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the help feature in any command mode.
?	Lists all commands available for a particular command mode.
<i>partial command?</i>	Provides a list of commands that begin with the character string (no space between the command and the question mark).
<i>partial command</i> <Tab>	Completes a partial command name (no space between the command and <Tab>).
<i>command ?</i>	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
<i>command keyword ?</i>	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help
```

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

?

```
Router# ?
```

Exec commands:

access-enable	Create a temporary access-List entry
access-profile	Apply user-profile to interface
access-template	Create a temporary access-List entry
alps	ALPS exec commands
archive	manage archive files

<snip>

partial command?

```
Router(config)# zo?
```

zone zone-pair

partial command<Tab>

```
Router(config)# we<Tab> webvpn
```

command ?

```
Router(config-if)# pppoe ?
```

enable	Enable pppoe
max-sessions	Maximum PPPOE sessions

command keyword ?

```
Router(config-if)# pppoe enable ?
```

group	attach a BBA group
-------	--------------------

<cr>

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. [Table 3](#) describes these conventions.

Table 3 *CLI Syntax Conventions*

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```

Router(config)# ethernet cfm domain ?
WORD domain name
Router(config)# ethernet cfm domain dname ?
level
Router(config)# ethernet cfm domain dname level ?
<0-7> maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
<cr>
Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>
Router(config)# logging host ?
Hostname or A.B.C.D IP address of the syslog server
ipv6 Configure IPv6 syslog server
Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>

```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored, but trailing spaces are recognized.



Note

Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.

- Press Ctrl-N or the down arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.



Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The CLI command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or un	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias mode command-alias original-command**. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** and **default** forms of commands are described in the command pages of command references.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS and Cisco IOS XE software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at

http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.



Caution

Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

Three output modifiers are available and are described as follows:

- **begin** *regular expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression “protocol.”

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. [Table 5](#) shows the common CLI error messages.

Table 5 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: “show con”	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at “^” marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following documents:

- [Cisco IOS Release 12.2SR System Message Guide](#)
- [Cisco IOS System Messages, Volume 1 of 2](#) (Cisco IOS Release 12.4)
- [Cisco IOS System Messages, Volume 2 of 2](#) (Cisco IOS Release 12.4)

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- “Using the Cisco IOS Command-Line Interface” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:
http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
or
“Using Cisco IOS XE Software” chapter of the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*:
http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/Using_CLI.html
- Cisco Product Support Resources
<http://www.cisco.com/web/psa/products/index.html>
- Support area on Cisco.com (also search for documentation by task or product)
<http://www.cisco.com/en/US/support/index.html>
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)
<http://www.cisco.com/kobayashi/sw-center/>
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software
<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)
<http://tools.cisco.com/Support/CLILookup>

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2008–2009 Cisco Systems, Inc. All rights reserved.



Overview: Secure Connectivity

First Published: March 31, 2009

Last Updated: March 31, 2009

Contents

- [About This Guide, page 1](#)
- [Related Documents, page 3](#)

About This Guide

The *Cisco IOS Security Configuration Guide: Secure Connectivity* describes how you can use IP security (IPsec) with Internet Key Exchange (IKE), Public Key Infrastructure (PKI), and virtual private network (VPN) technologies to manage and secure your networks and to deliver reliable transport for complex mission-critical traffic, such as voice and client-server applications, without compromising communications quality.

This chapter includes the following:

- [IPsec, page 1](#)
- [IKE, page 2](#)
- [PKI, page 2](#)
- [VPNs, page 2](#)

IPsec

IPsec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec provides data authentication and anti-replay services in addition to data confidentiality services.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

IKE

IKE is a key management protocol standard that is used in conjunction with the IPsec standard. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard.

PKI

PKI offers a scalable method of securing networks, reducing management overhead, and simplifying the deployment of network infrastructures by deploying Cisco IOS security protocols, including IPsec, secure shell (SSH), and secure socket layer (SSL). Cisco IOS software can also use PKI for authorization using access lists and authentication resources.

VPNs

VPN solutions are built on five underlying VPN technologies: Standard IPsec, Dynamic Multipoint VPN (DMVPN), Easy VPN, generic routing encapsulation (GRE) tunneling, and Group Encrypted Transport VPN (GET VPN). Each technology has its benefits and is customized to meet specific deployment requirements. [Table 1](#) provides a comparison of these technologies.

Table 1 **Comparison of VPN Solutions**

Standard IPsec VPN	
Benefits <ul style="list-style-type: none"> Provides encryption between sites. Supports quality of service (QoS). 	When to Use <ul style="list-style-type: none"> When multivendor interoperability is required.
Cisco DMVPN	
Benefits <ul style="list-style-type: none"> Simplifies encryption configuration and management for point-to-point GRE tunnels. Provides on-demand spoke-to-spoke tunnels. Supports QoS, multicast, and routing. 	When to Use <ul style="list-style-type: none"> To simplify configuration for hub-and-spoke VPNs while supporting QoS, multicast, and routing. To provide low-scale, on-demand meshing.
Cisco Easy VPN	
Benefits <ul style="list-style-type: none"> Simplifies IPsec and remote-site device management through dynamic configuration policy-push. Supports QoS. 	When to Use <ul style="list-style-type: none"> When simplifying overall VPN and management is the primary goal (but only if limited networking features are required). To provide a simple, unified configuration framework for a mix of Cisco VPN products.
Cisco GRE-Based VPN	

Table 1 **Comparison of VPN Solutions (continued)**

Benefits <ul style="list-style-type: none"> Enables transport of multicast and the routing of traffic across an IPsec VPN. Supports non-IP protocols. Supports QoS. 	When to Use <ul style="list-style-type: none"> When routing must be supported across the VPN. For the same functions as hub-and-spoke DMVPN but when a more detailed configuration is required.
Cisco GET VPN	
Benefits <ul style="list-style-type: none"> Simplifies encryption integration on IP and Multiprotocol Label Switching (MPLS) WANs. Simplifies encryption management through use of group keying instead of point-to-point key pairs. Enables scalable and manageable any-to-any connectivity between sites. Supports QoS , multicast, and routing. 	When to Use <ul style="list-style-type: none"> To add encryption to MPLS or IP WANs while preserving any-to-any connectivity and networking features. To enable scalable, full-time meshing for IPsec VPNs. To enable participation of smaller routers in meshed networks. To simplify encryption key management while supporting QoS, multicast, and routing.

Related Documents

In addition to this document, there are other documents on Cisco.com about secure connectivity, too numerous to list here. For more information about or additional documentation for secure connectivity, search Cisco.com, specifying the desired subject or title.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



Internet Key Exchange for IPsec VPNs



Configuring Internet Key Exchange for IPsec VPNs

This module describes how to configure the Internet Key Exchange (IKE) protocol for basic IP Security (IPsec) virtual private networks (VPNs). IKE is a key management protocol standard that is used in conjunction with the IPsec standard. IPsec is an IP security feature that provides robust authentication and encryption of IP packets.

IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard.

IKE is a hybrid protocol, which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.)

Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the [“Feature Information for Configuring IKE for IPsec VPNs”](#) section on page 24.

Contents

- [Prerequisites for IKE Configuration, page 2](#)
- [Restrictions for IKE Configuration, page 2](#)
- [Information About Configuring IKE for IPsec VPNs, page 2](#)
- [How to Configure IKE for IPsec VPNs, page 4](#)
- [Configuration Examples for an IKE Configuration, page 19](#)
- [Where to Go Next, page 22](#)
- [Additional References, page 22](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for IKE Configuration

- You should be familiar with the concepts and tasks explained in the module “Configuring Security for VPNs with IPsec.”
- Ensure that your access control lists (ACLs) are compatible with IKE. Because IKE negotiation uses User Datagram Protocol (UDP) on port 500, your ACLs must be configured so that UDP port 500 traffic is not blocked at interfaces used by IKE and IPsec. In some cases you might need to add a statement to your ACLs to explicitly permit UDP port 500 traffic.

Restrictions for IKE Configuration

The following restrictions are applicable when configuring IKE negotiation:

- The initiating router *must not* have a certificate associated with the remote peer.
- The preshared key *must* be by fully qualified domain name (FQDN) on both peers. (To configure the preshared key, enter the **crypto isakmp key** command.)
- The communicating routers *must* have a FQDN host entry for each other in their configurations.
- The communicating routers *must* be configured to authenticate by hostname, *not* by IP address; thus, you should use the **crypto isakmp identity hostname** command.

Information About Configuring IKE for IPsec VPNs

To configure IKE for IPsec VPNs, you should understand the following concepts:

- [Supported Standards for Use with IKE, page 2](#)
- [IKE Benefits, page 4](#)
- [IKE Main Mode and Aggressive Mode, page 4](#)

Supported Standards for Use with IKE

Cisco implements the following standards:

- IPsec—IP Security Protocol. IPsec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
- ISAKMP—Internet Security Association and Key Management Protocol. A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.
- Oakley—A key exchange protocol that defines how to derive authenticated keying material.
- Skeme—A key exchange protocol that defines how to derive authenticated keying material, with rapid key refreshment.

The component technologies implemented for use by IKE include the following:

- **AES**—Advanced Encryption Standard. A cryptographic algorithm that protects sensitive, unclassified information. AES is privacy transform for IPsec and IKE and has been developed to replace the DES. AES is designed to be more secure than DES: AES offers a larger key size, while ensuring that the only known approach to decrypt a message is for an intruder to try every possible key. AES has a variable key length—the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.
- **DES**—Data Encryption Standard. An algorithm that is used to encrypt packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPsec packet.

Cisco IOS software also implements Triple DES (168-bit) encryption, depending on the software versions available for a specific platform. Triple DES (3DES) is a strong form of encryption that allows sensitive information to be transmitted over untrusted networks. It enables customers, particularly in the finance industry, to utilize network-layer encryption.

**Note**

Cisco IOS images that have strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to United States government export controls, and have a limited distribution. Images that are to be installed outside the United States require an export license. Customer orders might be denied or subject to delay because of United States government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

- **SEAL**—Software Encryption Algorithm. An alternative algorithm to software-based DES, 3DES, and AES. SEAL encryption uses a 160-bit encryption key and has a lower impact to the CPU when compared to other software-based algorithms.
- **Diffie-Hellman**—A public-key cryptography protocol that allows two parties to establish a shared secret over an unsecure communications channel. Diffie-Hellman is used within IKE to establish session keys. 768-bit (the default), 1024-bit, and 1536-bit Diffie-Hellman groups are supported.
- **MD5 (HMAC variant)**—Message Digest 5. A hash algorithm used to authenticate packet data. HMAC is a variant that provides an additional level of hashing.
- **SHA (HMAC variant)**—Secure Hash Algorithm. A hash algorithm used to authenticate packet data. HMAC is a variant that provides an additional level of hashing.
- **RSA signatures and RSA encrypted nonces**—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA signatures provide nonrepudiation, and RSA encrypted nonces provide repudiation. (Repudiation and nonrepudiation have to do with traceability.)

IKE interoperates with the following standard:

X.509v3 certificates—Used with the IKE protocol when authentication requires public keys. This certificate support allows the protected network to scale by providing the equivalent of a digital ID card to each device. When two devices intend to communicate, they exchange digital certificates to prove their identity (thus removing the need to manually exchange public keys with each peer or to manually specify a shared key at each peer).

IKE Benefits

IKE automatically negotiates IPsec security associations (SAs) and enables IPsec secure communications without costly manual preconfiguration. Specifically, IKE provides the following benefits:

- Eliminates the need to manually specify all the IPsec security parameters in the crypto maps at both peers.
- Allows you to specify a lifetime for the IPsec SA.
- Allows encryption keys to change during IPsec sessions.
- Allows IPsec to provide anti-replay services.
- Permits certification authority (CA) support for a manageable, scalable IPsec implementation.
- Allows dynamic authentication of peers.

IKE Main Mode and Aggressive Mode

IKE has two phases of key negotiation: phase 1 and phase 2. Phase 1 negotiates a security association (a key) between two IKE peers. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During phase 2 negotiation, IKE establishes keys (security associations) for other applications, such as IPsec.

Phase 1 negotiation can occur using main mode or aggressive mode. Main mode tries to protect all information during the negotiation, meaning that no information is available to a potential attacker. When main mode is used, the identities of the two IKE peers are hidden. Although this mode of operation is very secure, it is relatively costly in terms of the time it takes to complete the negotiation. Aggressive mode takes less time to negotiate keys between peers; however, it gives up some of the security provided by main mode negotiation. For example, the identities of the two parties trying to establish a security association are exposed to an eavesdropper.

The two modes serve different purposes and have different strengths. Main mode is slower than aggressive mode, but main mode is more secure and more flexible because it can offer an IKE peer more security proposals than aggressive mode. Aggressive mode is less flexible and not as secure, but much faster.

In Cisco IOS software, the two modes are not configurable. The default action for IKE authentication (rsa-sig, rsa-encr, or preshared) is to initiate main mode; however, in cases where there is no corresponding information to initiate authentication, and there is a preshared key associated with the hostname of the peer, Cisco IOS software can initiate aggressive mode. Cisco IOS software will respond in aggressive mode to an IKE peer that initiates aggressive mode.

How to Configure IKE for IPsec VPNs

If you do not want IKE to be used with your IPsec implementation, you can disable it at all IPsec peers via the **no crypto isakmp** command, skip the rest of this chapter, and begin your IPsec VPN.



Note

If you disable IKE, you will have to manually specify all the IPsec SAs in the crypto maps at all peers, the IPsec SAs of the peers will never time out for a given IPsec session, the encryption keys will never change during IPsec sessions between the peers, anti-replay services will not be available between the peers, and public key infrastructure (PKI) support cannot be used.

IKE is enabled by default. IKE does not have to be enabled for individual interfaces, but it is enabled globally for all interfaces at the router.

Perform the following tasks to provide authentication of IPsec peers, negotiate IPsec SAs, and establish IPsec keys:

- [Creating IKE Policies: Security Parameters for IKE Negotiation, page 5](#) (required)
- [Configuring IKE Authentication, page 9](#) (required)
- [Configuring IKE Mode Configuration, page 17](#)

Creating IKE Policies: Security Parameters for IKE Negotiation

An IKE policy defines a combination of security parameters to be used during the IKE negotiation. You must create an IKE policy at each peer participating in the IKE exchange.

If you do not configure any IKE policies, your router will use the default policy, which is always set to the lowest priority and which contains the default value of each parameter.

About IKE Policies

Because IKE negotiations must be protected, each IKE negotiation begins by agreement of both peers on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations and mandates how the peers are authenticated.

After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these SAs apply to all subsequent IKE traffic during the negotiation.

You can configure multiple, prioritized policies on each peer—each with a different combination of parameter values. However, at least one of these policies must contain exactly the same encryption, hash, authentication, and Diffie-Hellman parameter values as one of the policies on the remote peer. For each policy that you create, you assign a unique priority (1 through 10,000, with 1 being the highest priority).



Tip

If you are interoperating with a device that supports only one of the values for a parameter, your choice is limited to the value supported by the other device. Aside from this limitation, there is often a trade-off between security and performance, and many of these parameter values represent such a trade-off. You should evaluate the level of security risks for your network and your tolerance for these risks.

IKE Peers Agreeing Upon a Matching IKE Policy

When the IKE negotiation begins, IKE searches for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the policies received from the other peer. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer's policy specifies a lifetime that is less than or equal to the lifetime in the policy being compared. (If the lifetimes are not identical, the shorter lifetime—from the remote peer's policy—will be used.)

If a match is found, IKE will complete negotiation, and IPsec security associations will be created. If no acceptable match is found, IKE refuses negotiation and IPsec will not be established.

**Note**

Depending on which authentication method is specified in a policy, additional configuration might be required (as described in the section “[Configuring IKE Authentication](#)”). If a peer’s policy does not have the required companion configuration, the peer will not submit the policy when attempting to find a matching policy with the remote peer.

Restrictions

If you are configuring an AES IKE policy, note the following restrictions:

- Your router must support IPsec and long keys (the “k9” subsystem).
- AES cannot encrypt IPsec and IKE traffic if an acceleration card is present.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy** *priority*
4. **encryption** {des | 3des | aes | aes 192 | aes 256}
5. **hash** {sha | md5}
6. **authentication** {rsa-sig | rsa-encr | pre-share}
7. **group** {1 | 2 | 5}
8. **lifetime** *seconds*
9. **exit**
10. **exit**
11. **show crypto isakmp policy**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp policy <i>priority</i> Example: Router(config)# crypto isakmp policy 10	Defines an IKE policy and enters config-isakmp configuration mode. <ul style="list-style-type: none"> <i>priority</i>—Uniquely identifies the IKE policy and assigns a priority to the policy. Valid values: 1 to 10,000; 1 is the highest priority.
Step 4	encryption {des 3des aes aes 192 aes 256} Example: Router(config-isakmp)# encryption aes 256	Specifies the encryption algorithm. By default, the des keyword is used. <ul style="list-style-type: none"> des—56-bit DES-CBC 3des—168-bit DES aes—128-bit AES aes 192—192-bit AES aes 256—256-bit AES
Step 5	hash {sha md5} Example: Router(config-isakmp)# hash sha	Specifies the hash algorithm. By default, SHA-1 (sha) is the used. Note MD5 has a smaller digest and is considered to be slightly faster than SHA-1.
Step 6	authentication {rsa-sig rsa-encr pre-share} Example: Router(config-isakmp)# authentication pre-share	Specifies the authentication method. By default, RSA signatures are used. <ul style="list-style-type: none"> rsa-sig—RSA signatures require that you configure your peer routers to obtain certificates from a CA. rsa-encr—RSA encrypted nonces require that you ensure each peer has the other peer's RSA public keys. pre-share—Preshared keys require that you separately configure these preshared keys.

	Command or Action	Purpose
Step 7	group {1 2 5} Example: Router(config-isakmp)# group 1	Specifies the Diffie-Hellman group identifier. By default, D-H group 1 is used. <ul style="list-style-type: none"> 1—768-bit Diffie-Hellman 2—1024-bit Diffie-Hellman 5—1536-bit Diffie-Hellman Note The 1024-bit and 1536-bit Diffie-Hellman options are harder to “crack,” but require more CPU time to execute.
Step 8	lifetime <i>seconds</i> Example: Router(config-isakmp)# lifetime 180	Specifies the lifetime of the IKE SA. <ul style="list-style-type: none"> <i>seconds</i>—Time, in seconds, before each SA expires. Valid values: 60 to 86,400 seconds; default value: 86,400. Note The shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec SAs can be set up more quickly.
Step 9	exit Example: Router(config-isakmp)# exit	Exits config-isakmp configuration mode.
Step 10	exit Example: Router(config)# exit	Exits the global configuration mode.
Step 11	show crypto isakmp policy Example: Router# show crypto isakmp policy	(Optional) Displays all existing IKE policies.
Step 12	—	Repeat these steps for each policy you want to create.

**Note**

These parameters apply to the IKE negotiations after the IKE SA is established.

Examples

The following sample output from the **show crypto isakmp policy** command displays a warning message after a user tries to configure an IKE encryption method that the hardware does not support:

```
Router# show crypto isakmp policy
```

```
Protection suite of priority 1
  encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
  hash algorithm:          Secure Hash Standard
  authentication method: Pre-Shared Key
```

```
Diffie-Hellman group:  #1 (768 bit)
lifetime:              3600 seconds, no volume limit
```

Troubleshooting Tips

- Clear (and reinitialize) IPsec SAs by using the **clear crypto sa EXEC** command.

Using the **clear crypto sa** command without parameters will clear out the full SA database, which will clear out active security sessions. You may also specify the **peer**, **map**, or **entry** keywords to clear out only a subset of the SA database. For more information, see the **clear crypto sa** command in the *Cisco IOS Security Command Reference*, Release 12.4.

- The default policy and default values for configured policies do not show up in the configuration when you issue the **show running-config** command. To see the default policy and any default values within configured policies, use the **show crypto isakmp policy** command.
- Any IPsec transforms or IKE encryption methods that the current hardware does not support should be disabled; they are ignored whenever an attempt to negotiate with the peer is made.

If a user enters an IPsec transform or an IKE encryption method that the hardware does not support, a warning message will be generated. These warning messages are also generated at boot time. When an encrypted card is inserted, the current configuration is scanned. If any IPsec transforms or IKE encryption methods are found that are not supported by the hardware, a warning message will be generated.

What to Do Next

Depending on which authentication method you specified in your IKE policies (RSA signatures, RSA encrypted nonces, or preshared keys), you must do certain additional configuration tasks before IKE and IPsec can successfully use the IKE policies. For information on completing these additional tasks, refer to the following section “[Configuring IKE Authentication](#).”

To configure an AES-based transform set, see the module “Configuring Security for VPNs with IPsec.”

Configuring IKE Authentication

After you have created at least one IKE policy in which you specified an authentication method (or accepted the default method), you need to configure an authentication method. IKE policies cannot be used by IPsec until the authentication method is successfully configured.

To configure IKE authentication, you should perform one of the following tasks, as appropriate:

- [Configuring RSA Keys Manually for RSA Encrypted Nonces, page 11](#)
- [Configuring Preshared Keys, page 13](#)
- Configuring RSA Keys to Obtain Certificates from a CA. For information on completing this task, see the module “Deploying RSA Keys Within a PKI.”

IKE Authentication Methods: Overview

IKE authentication consists of three options—RSA signatures, RSA encrypted nonces, and preshared keys. Each authentication method requires additional configuration as follows:

RSA Signatures

With RSA signatures, you can configure the peers to obtain certificates from a CA. (The CA must be properly configured to issue the certificates.) Using a CA can dramatically improve the manageability and scalability of your IPsec network. Additionally, RSA signature-based authentication uses only two public key operations, whereas RSA encryption uses four public key operations, making it costlier in terms of overall performance. To properly configure CA support, see the chapter “Implementing and Managing a PKI.”

The certificates are used by each peer to exchange public keys securely. (RSA signatures requires that each peer has the public signature key of the remote peer.) When both peers have valid certificates, they will automatically exchange public keys with each other as part of any IKE negotiation in which RSA signatures are used.

You can also exchange the public keys manually, as described in the section “[Configuring RSA Keys Manually for RSA Encrypted Nonces](#).”

RSA signatures provide nonrepudiation for the IKE negotiation. And, you can prove to a third party after the fact that you did indeed have an IKE negotiation with the remote peer.

RSA Encrypted Nonces

With RSA encrypted nonces, you must ensure that each peer has the public keys of the other peers.

Unlike RSA signatures, the RSA encrypted nonces method can not use certificates to exchange public keys. Instead, you ensure that each peer has the others’ public keys by one of the following methods:

- Manually configuring RSA keys as described in the section “[Configuring RSA Keys Manually for RSA Encrypted Nonces](#).”

or

- Ensuring that an IKE exchange using RSA signatures with certificates has already occurred between the peers. (The peers’ public keys are exchanged during the RSA-signatures-based IKE negotiations if certificates are used.)

To make that the IKE exchange happens, specify two policies: a higher-priority policy with RSA encrypted nonces and a lower-priority policy with RSA signatures. When IKE negotiations occur, RSA signatures will be used the first time because the peers do not yet have each other’s public keys. Then future IKE negotiations can use RSA encrypted nonces because the public keys will have been exchanged.



Note This alternative requires that you already have CA support configured.

RSA encrypted nonces provide repudiation for the IKE negotiation; however, unlike RSA signatures, you cannot prove to a third party that you had an IKE negotiation with the remote peer.

Preshared Keys

With preshared keys, you must configure them as described in the section “[Configuring Preshared Keys](#).”

Preshared keys are clumsy to use if your secured network is large, and they do not scale well with a growing network. However, they do not require use of a CA, as do RSA signatures, and might be easier to set up in a small network with fewer than ten nodes. RSA signatures also can be considered more secure when compared with preshared key authentication.

**Note**

If RSA encryption is configured and signature mode is negotiated (and certificates are used for signature mode), the peer will request both signature and encryption keys. Basically, the router will request as many keys as the configuration will support. If RSA encryption is not configured, it will just request a signature key.

Prerequisites

You must have configured at least one IKE policy, which is where the authentication method was specified (or RSA signatures was accepted by default).

Configuring RSA Keys Manually for RSA Encrypted Nonces

To manually configure RSA keys, perform this task for each IPsec peer that uses RSA encrypted nonces in an IKE policy.

**Note**

This task can be performed only if a CA is not in use.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa** {general-keys | usage-keys} [label *key-label*] [exportable] [modulus *modulus-size*]
4. **exit**
5. **show crypto key mypubkey rsa**
6. **configure terminal**
7. **crypto key pubkey-chain rsa**
8. **named-key** *key-name* [encryption | signature]
or
addressed-key *key-address* [encryption | signature]
9. **address** *ip-address*
10. **key-string** *key-string*
11. **quit**
12. Repeat these steps at each peer that uses RSA encrypted nonces in an IKE policy.
13. **exit**
14. **exit**
15. **show crypto key pubkey-chain rsa** [name *key-name* | address *key-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto key generate rsa {general-keys usage-keys} [label key-label] [exportable] [modulus modulus-size] Example: Router(config)# crypto key generate rsa general-keys modulus 360	Generates RSA keys. <ul style="list-style-type: none"> If a <i>key-label</i> argument is not specified, the default value, which is the fully qualified domain name (FQDN) of the router, is used.
Step 4	exit Example: Router(config)# exit	(Optional) Exits global configuration mode.
Step 5	show crypto key mypubkey rsa Example: Router# show crypto key mypubkey rsa	(Optional) Displays the generated RSA public keys.
Step 6	configure terminal Example: Router# configure terminal	Returns to global configuration mode.
Step 7	crypto key pubkey-chain rsa Example: Router(config)# crypto key pubkey-chain rsa	Enters public key configuration mode (so you can manually specify the RSA public keys of other devices).
Step 8	named-key key-name [encryption signature] Example: Router(config-pubkey-chain)# named-key otherpeer.example.com or addressed-key key-address [encryption signature] Example: Router(config-pubkey-chain)# addressed-key 10.1.1.2 encryption	Indicates which remote peer's RSA public key you are going to specify and enters public key configuration mode. If the remote peer uses its host name as its ISAKMP identity, use the named-key command and specify the remote peer's FQDN, such as somerouter.example.com, as the <i>key-name</i> . If the remote peer uses its IP address as its ISAKMP identity, use the addressed-key command and specify the remote peer's IP address as the <i>key-address</i> .

	Command or Action	Purpose
Step 9	address <i>ip-address</i> Example: Router(config-pubkey-key)# address 10.5.5.1	Specifies the IP address of the remote peer. If you use the named-key command, you need to use this command to specify the IP address of the peer.
Step 10	key-string <i>key-string</i> Example: Router(config-pubkey-key)# key-string Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973 Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5 Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8 Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21	Specifies the RSA public key of the remote peer. (This key was previously viewed by the administrator of the remote peer when the RSA keys of the remote router were generated.)
Step 11	quit Example: Router(config-pubkey-k)# quit	Returns to public key chain configuration mode.
Step 12	—	Repeat these steps at each peer that uses RSA encrypted nonces in an IKE policy.
Step 13	exit Example: Router(config-pubkey-c)# exit	Returns to global configuration mode.
Step 14	exit Example: Router(config)# exit	Returns to EXEC mode.
Step 15	show crypto key pubkey-chain rsa [<i>name key-name</i> <i>address key-address</i>] Example: Router# show crypto key pubkey-chain rsa	(Optional) Displays either a list of all RSA public keys that are stored on your router or details of a particular RSA key that is stored on your router.

Configuring Preshared Keys

To configure preshared keys, perform these steps at each peer that uses preshared keys in an IKE policy.

Setting ISAKMP Identity for Preshared Keys

You should set the ISAKMP identity for each peer that uses preshared keys in an IKE policy.

When two peers use IKE to establish IPsec SAs, each peer sends its identity to the remote peer. Each peer sends either its host name or its IP address, depending on how you have set the ISAKMP identity of the router.

By default, a peer's ISAKMP identity is the IP address of the peer. If appropriate, you could change the identity to be the peer's host name instead. As a general rule, set the identities of all peers the same way—either all peers should use their IP addresses or all peers should use their hostnames. If some peers use their host names and some peers use their IP addresses to identify themselves to each other, IKE negotiations could fail if the identity of a remote peer is not recognized and a DNS lookup is unable to resolve the identity.

Mask Preshared Keys

A mask preshared key allows a group of remote users with the same level of authentication to share an IKE preshared key. The preshared key of the remote peer must match the preshared key of the local peer for IKE authentication to occur.

A mask preshared key is usually distributed through a secure out-of-band channel. In a remote peer-to-local peer scenario, any remote peer with the IKE preshared key configured can establish IKE SAs with the local peer.

If you specify the **mask** keyword with the **crypto isakmp key** command, it is up to you to use a subnet address, which will allow more peers to share the same key. That is, the preshared key is no longer restricted to use between two users.



Note

Using 0.0.0.0 as a subnet address is not recommended because it encourages group preshared keys, which allow all peers to have the same group key, thereby reducing the security of your user authentication.

Disable Xauth on a Specific IPsec Peer

Disabling Extended Authentication (Xauth) for static IPsec peers prevents the routers from being prompted for Xauth information—username and password.

Without the ability to disable Xauth, a user cannot select which peer on the same crypto map should use Xauth. That is, if a user has router-to-router IPsec on the same crypto map as a VPN-client-to-Cisco-IOS IPsec, both peers are prompted for a username and password. In addition, a remote static peer (a Cisco IOS router) cannot establish an IKE SA with the local Cisco IOS router. (Xauth is not an optional exchange, so if a peer does not respond to an Xauth request, the IKE SA is deleted.) Thus, the same interface cannot be used to terminate IPsec to VPN clients (that need Xauth) as well as other Cisco IOS routers (that cannot respond to Xauth) unless this feature is implemented.



Note

Xauth can be disabled only if preshared keys are used as the authentication mechanism for the given crypto map.

Restrictions

- Preshared do not scale well with a growing network.
- Mask preshared keys have the following restrictions:
 - The SA cannot be established between the IPsec peers until all IPsec peers are configured for the same preshared key.

- The mask preshared key must be distinctly different for remote users requiring varying levels of authorization. You must configure a new preshared key for each level of trust and assign the correct keys to the correct parties. Otherwise, an untrusted party may obtain access to protected data.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp identity {address | hostname}**
4. **ip host *hostname* *address1* [*address2*...*address8*]**
5. **crypto isakmp key *keystring* **address** *peer-address* [**mask**] [**no-xauth**]**
or
crypto isakmp key *keystring* **hostname *hostname* [**no-xauth**]**
6. **crypto isakmp key *keystring* **address** *peer-address* [**mask**] [**no-xauth**]**
or
crypto isakmp key *keystring* **hostname *hostname* [**no-xauth**]**
7. Repeat these steps for each peer that uses preshared keys.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp identity {address hostname} Example: Router(config)# crypto isakmp identity address	Specifies the peer's ISAKMP identity by IP address or by hostname at the local peer. <ul style="list-style-type: none"> address—Typically used when there is only one interface (and therefore only one IP address) that will be used by the peer for IKE negotiations, and the IP address is known. hostname—Should be used if there is more than one interface on the peer that might be used for IKE negotiations, or if the interface's IP address is unknown (such as with dynamically assigned IP addresses).
Step 4	ip host hostname address1 [address2...address8] Example: Router(config)# ip host RemoteRouter.example.com 192.168.0.1	If the local peer's ISAKMP identity was specified using a hostname, maps the peer's host name to its IP address(es) at all the remote peers. (This step might be unnecessary if the hostname or address is already mapped in a DNS server.)
Step 5	crypto isakmp key keystring address peer-address [mask] [no-xauth] Example: Router(config)# crypto isakmp key sharedkeystring address 192.168.1.33 no-xauth or crypto isakmp key keystring hostname hostname [no-xauth] Example: Router(config) crypto isakmp key sharedkeystring hostname RemoteRouter.example.com	Specifies at the local peer the shared key to be used with a particular remote peer. If the remote peer specified its ISAKMP identity with an address, use the address keyword in this step; otherwise use the hostname keyword in this step. <ul style="list-style-type: none"> no-xauth—Prevents the router from prompting the peer for Xauth information. Use this keyword if router-to-router IPsec is on the same crypto map as VPN-client-to-Cisco IOS IPsec. <p>Note According to the design of preshared key authentication in IKE main mode, preshared keys must be based on the IP address of the peers. Although you can send hostname as the identity of preshared key authentication, the key is searched on the IP address of the peer; if the key is not found (based on the IP address) the negotiation will fail.</p>

	Command or Action	Purpose
Step 6	<pre>crypto isakmp key <i>keystring</i> address <i>peer-address</i> [<i>mask</i>] [<i>no-xauth</i>]</pre> <p>Example:</p> <pre>Router(config) crypto isakmp key sharedkeystring address 10.0.0.1</pre> <p>or</p> <pre>crypto isakmp key <i>keystring</i> hostname <i>hostname</i> [no-xauth]</pre> <p>Example:</p> <pre>Router(config) crypto isakmp key sharedkeystring hostname LocalRouter.example.com</pre>	<p>Specifies at the remote peer the shared key to be used with the local peer.</p> <p>This is the same key you just specified at the local peer.</p> <p>If the local peer specified its ISAKMP identity with an address, use the address keyword in this step; otherwise use the hostname keyword in this step.</p>
Step 7	—	Repeat these steps at each peer that uses preshared keys in an IKE policy.

Configuring IKE Mode Configuration

Perform the following task to configure IKE mode configuration.

About IKE Mode Configuration

IKE mode configuration, as defined by the Internet Engineering Task Force (IETF) , allows a gateway to download an IP address (and other network level configuration) to the client as part of an IKE negotiation. Using this exchange, the gateway gives IP addresses to the IKE client to be used as an “inner” IP address encapsulated under IPsec. This method provides a known IP address for the client that can be matched against IPsec policy.

To implement IPsec VPNs between remote access clients that have dynamic IP addresses and a corporate gateway, you have to dynamically administer scalable IPsec policy on the gateway once each client is authenticated. With IKE Mode Configuration, the gateway can set up scalable policy for a very large set of clients irrespective of the IP addresses of those clients.

There are two types of IKE Mode Configuration:

- Gateway initiation—Gateway initiates the configuration mode with the client. Once the client responds, the IKE modifies the identity of the sender, the message is processed, and the client receives a response.
- Client initiation—Client initiates the configuration mode with the gateway. The gateway responds with an IP address that it has allocated for the client.

Restrictions

IKE Mode Configuration has the following restrictions:

- Interfaces with crypto maps that are configured for IKE Mode Configuration may experience a slightly longer connection setup time, which is true even for IKE peers that refuse to be configured or do not respond to the configuration mode request. In both cases, the gateway initiates the configuration of the client.
- This feature was not designed to enable the configuration mode for every IKE connection by default. Configure this feature at the global crypto map level.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip local pool** *pool-name start-addr end-addr*
4. **crypto isakmp client configuration address-pool local** *pool-name*
5. **crypto map** *tag* **client configuration address** [**initiate** | **respond**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip local pool pool-name start-addr end-addr Example: Router(config) ip local pool ire 172.16.23.0 172.16.23.255	Defines an existing local address pool that defines a set of addresses.
Step 4	crypto isakmp client configuration address-pool local pool-name Example: Router(config) crypto isakmp client configuration address-pool local ire	References the local address pool in the IKE configuration.
Step 5	crypto map tag client configuration address [initiate respond] Example: Router(config)# crypto map dyn client configuration address initiate	Configures IKE Mode Configuration in global crypto map configuration mode.

Configuration Examples for an IKE Configuration

This section contains the following configuration examples:

- [Creating IKE Policies: Examples, page 19](#)
- [Configuring IKE Authentication: Example, page 21](#)

Creating IKE Policies: Examples

This section contains the following examples, which show how to configure a 3DES IKE policy and an AES IKE policy:

- [Creating 3DES IKE Policies: Example, page 20](#)
- [Creating an AES IKE Policy: Example, page 20](#)

Creating 3DES IKE Policies: Example

This example creates two IKE policies, with policy 15 as the highest priority, policy 20 as the next priority, and the existing default priority as the lowest priority. It also creates a preshared key to be used with policy 20 with the remote peer whose IP address is 192.168.224.33.

```
crypto isakmp policy 15
  encryption 3des
  hash md5
  authentication rsa-sig
  group 2
  lifetime 5000
!
crypto isakmp policy 20
  authentication pre-share
  lifetime 10000
!
crypto isakmp key 1234567890 address 192.168.224.33
```

In the example, the encryption des of policy 15 would not appear in the written configuration because this is the default value for the encryption algorithm parameter.

If the **show crypto isakmp policy** command is issued with this configuration, the output is as follows:

```
Protection suite priority 15
encryption algorithm:3DES - Triple Data Encryption Standard (168 bit keys)
hash algorithm:Message Digest 5
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#2 (1024 bit)
lifetime:5000 seconds, no volume limit
Protection suite priority 20
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:preshared Key
Diffie-Hellman group:#1 (768 bit)
lifetime:10000 seconds, no volume limit
Default protection suite
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#1 (768 bit)
lifetime:86400 seconds, no volume limit
```

Note that although the output shows “no volume limit” for the lifetimes, you can configure only a time lifetime (such as 86,400 seconds); volume-limit lifetimes are not configurable.

Creating an AES IKE Policy: Example

The following example is sample output from the **show running-config** command. In this example, the AES 256-bit key is enabled.

```
Current configuration : 1665 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname "Router1"
!
!
ip subnet-zero
!
```

```

!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 10
  encryption aes 256
  authentication pre-share
  lifetime 180
crypto isakmp key cisco123 address 10.0.110.1
!
!
crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac
  mode transport
!
crypto map aesmap 10 ipsec-isakmp
  set peer 10.0.110.1
  set transform-set aesset
  match address 120
!
.
.
.

```

Configuring IKE Authentication: Example

The following example shows how to manually specify the RSA public keys of two IPsec peer—the peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-usage keys:

```

crypto key pubkey-chain rsa
  named-key otherpeer.example.com
  address 10.5.5.1
  key-string
005C300D 06092A86 4886F70D 01010105
00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4
64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
D58AD221 B583D7A4 71020301 0001
  quit
exit
addressed-key 10.1.1.2 encryption
  key-string
00302017 4A7D385B 1234EF29 335FC973
2DD50A37 C4F4B0FD 9DADE748 429618D5
18242BA3 2EDFBDD3 4296142A DDF7D3D8
08407685 2F2190A0 0B43F1BD 9A8A26DB
07953829 791FCDE9 A98420F0 6A82045B
90288A26 DBC64468 7789F76E EE21
  quit
exit
addressed-key 10.1.1.2 signature
  key-string
0738BC7A 2BC3E9F0 679B00FE 53987BCC
01030201 42DD06AF E228D24C 458AD228
58BB5DDD F4836401 2A2D7163 219F882E
64CE69D4 B583748A 241BED0F 6E7F2F16
0DE0986E DF02031F 4B0B0912 F68200C4
C625C389 0BFF3321 A2598935 C1B1
  quit
exit

```

```
exit
```

Where to Go Next

After you have successfully configured IKE negotiation, you can begin configuring IPsec. For information on completing these tasks, see the module “Configuring Security for VPNs With IPsec.”

Additional References

The following sections provide references related to configuring IKE for IPsec VPNs.

Related Documents

Related Topic	Document Title
IPsec configuration	Configuring Security for VPNs with IPsec
Configuring RSA keys to obtain certificates from a CA	Deploying RSA Keys Within a PKI
IKE, IPsec, and PKI configuration commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Security Command Reference

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409	The Internet Key Exchange (IKE)
RFC 2412	The OAKLEY Key Determination Protocol

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Glossary

anti-replay—Security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks. IPsec provides optional anti-replay services by use of a sequence number and the use of authentication.

data authentication—Verification of the integrity and origin of the data.

Data authentication can refer either to integrity alone or to both of these concepts (although data origin authentication is dependent upon data integrity).

peer—In the context of this chapter, a “peer” is a router or other device that participates in IPsec and IKE.

PFS—perfect forward secrecy. Cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not also compromised, because subsequent keys are not derived from previous keys.

repudiation—Quality that prevents a third party from being able to prove that a communication between two other parties ever took place. Repudiation is a desirable quality if you do not want your communications to be traceable.

nonrepudiation—Quality that allows a third party to prove that a communication between two other parties took place. Nonrepudiation is desirable if you want to be able to trace your communications and prove that they occurred.

SA—security association. How two or more entities utilize security services to communicate securely.

For example, an IPsec SA defines the encryption algorithm (if used), the authentication algorithm, and the shared session key to be used during the IPsec connection. Both IPsec and IKE require and use SAs to identify the parameters of their connections. IKE can negotiate and establish its own SA. The IPsec SA is established either by IKE or by manual user configuration.



Note

Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Configuring IKE for IPsec VPNs

[Table 43](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

[Table 43](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 43 *Feature Information for Configuring IKE for IPsec VPNs*

Feature Name	Software Releases	Feature Configuration Information
Ability to Disable Extended Authentication for Static IPsec Peers	12.2(4)T	<p>This feature allows a user to disable Xauth while configuring the preshared key for router-to-router IPsec. Thus, the router will not prompt the peer for a username and password, which are transmitted when Xauth occurs for VPN-client-to-Cisco-IOS IPsec.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Configuring Preshared Keys <p>The following command was modified by this feature: crypto isakmp key</p>
Advanced Encryption Standard (AES)	12.2(8)T	<p>This feature adds support for the new encryption standard AES, which is a privacy transform for IPsec and IKE and has been developed to replace DES.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Supported Standards for Use with IKE • Creating IKE Policies: Security Parameters for IKE Negotiation <p>The following commands were modified by this feature: crypto ipsec transform-set, encryption (IKE policy), show crypto isakmp policy, show crypto ipsec transform-set</p>
SEAL Encryption	12.3(7)T	<p>This feature adds support for SEAL encryption in IPsec.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Supported Standards for Use with IKE <p>The following command was modified by this feature: crypto ipsec transform-set</p>
IKE Extended Authentication (Xauth)	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Wildcard Pre-Shared Key	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
IKE - Diffie-Hellman (768 Bit or 1024 Bit) PKCS #3 Support	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Table 43 **Feature Information for Configuring IKE for IPsec VPNs (continued)**

Feature Name	Software Releases	Feature Configuration Information
IKE Phase 1 Main Mode and Phase 1 Aggressive Mode	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
IKE - RSA Signature	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



Call Admission Control for IKE

First Published: May 17, 2004

Last Updated: February 23, 2009

The Call Admission Control for IKE feature describes the application of Call Admission Control (CAC) to the Internet Key Exchange (IKE) protocol in Cisco IOS. CAC limits the number of simultaneous IKE security associations (SAs) (that is, calls to CAC) that a router can establish.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Call Admission Control for IKE” section on page 9](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Catalyst OS, and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Call Admission Control for IKE, page 2](#)
- [Information About Call Admission Control for IKE, page 2](#)
- [How to Configure Call Admission Control for IKE, page 3](#)
- [Configuration Examples for Call Admission Control for IKE, page 6](#)
- [Additional References, page 6](#)
- [Command Reference, page 8](#)
- [Feature Information for Call Admission Control for IKE, page 9](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Call Admission Control for IKE

- Configure IKE on the router. Refer to the *Cisco IOS Security Configuration Guide*, Release 12.3.

Information About Call Admission Control for IKE

To configure CAC for IKE, you need to understand the following concepts:

- [IKE Session, page 2](#)
- [Security Association Limit, page 2](#)
- [System Resource Usage, page 3](#)

IKE Session

There are two ways to limit the number of IKE SAs that a router can establish to or from another router:

- Configure the absolute IKE SA limit by entering the **crypto call admission limit** command. The router drops new IKE SA requests when the value has been reached.
- Configure the system resource limit by entering the **call admission limit** command. The router drops new IKE SA requests when the level of system resources that are configured in the unit of charge is being used.

For information about using these commands, see the “[Command Reference](#)” section on page 8.

CAC is applied only to new SAs (that is, when an SA does not already exist between the peers). Every effort is made to preserve existing SAs. Only new SA requests will ever be denied due to a lack of system resources or because the configured IKE SA limit has been reached.

Security Association Limit

An SA is a description of how two or more entities will utilize security services to communicate securely on behalf of a particular data flow. IKE requires and uses SAs to identify the parameters of its connections. IKE can negotiate and establish its own SA. An IKE SA is used by IKE only, and it is bidirectional. An IKE SA cannot limit IPsec.

IKE drops SA requests based on a user-configured SA limit. To configure an IKE SA limit, enter the **crypto call admission limit** command. When there is a new SA request from a peer router, IKE determines if the number of active IKE SAs plus the number of SAs being negotiated meets or exceeds the configured SA limit. If the number is greater than or equal to the limit, the new SA request is rejected and a syslog is generated. This log contains the source destination IP address of the SA request.

Limit on Number of In-negotiation IKE Connections

Effective with Cisco IOS Release 12.4(6)T, a limit on the number of in-negotiation IKE connections can be configured. This type of IKE connection represents either an aggressive mode IKE SA or a main mode IKE SA prior to its authentication and actual establishment.

Using the **crypto call admission limit ike in-negotiation-sa {number}** command allows the configured number of in-negotiation IKE SAs to start negotiation without contributing to the maximum number of IKE SAs allowed.

System Resource Usage

CAC polls a global resource monitor so that IKE knows when the router is running short of CPU cycles or memory buffers. You can configure a limit, in the range to 100000, that represents the level of system resource usage in system resource usage units. When that level of resources is being used, IKE drops (will not accept new) SA requests. To configure the system resource usage limit, enter the **call admission limit** command.

For each incoming new SA request, the current load on the router is converted into a numerical value, representing the system resource usage level, and is compared to the resource limit set by the **call admission limit** command. If the current load is more than the configured resource limit, IKE drops the new SA request. Load on the router includes active SAs, CPU usage, and SA requests being considered.

The **call admission load** command configures a multiplier value from 0 to 1000 that represents a scaling factor for current system resource usage and a load metric poll rate of 1 to 32 seconds. The numerical value for the system resource usage level is calculated by the formula (scaling factor * current system resource usage) / 100. It is recommended that the **call admission load** command not be used unless advised by a Cisco Technical Assistance Center (TAC) engineer.

How to Configure Call Admission Control for IKE

This section contains the following procedures:

- [Configuring the IKE Security Association Limit, page 3](#) (optional)
- [Configuring the System Resource Limit, page 4](#) (optional)
- [Verifying the Call Admission Control for IKE Configuration, page 5](#) (optional)

**Note**

You must perform one of the configuration procedures—the configuration procedures are the first two listed.

Configuring the IKE Security Association Limit

Perform this task to configure the absolute IKE SA limit. The router drops new IKE SA requests when the limit has been reached.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto call admission limit {ike {in-negotiation-sa *number* | sa *number* } }**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto call admission limit {ike {in-negotiation-sa number} sa number}} Example: Router(config)# crypto call admission limit ike sa 25	Specifies the maximum number of IKE SAs that the router can establish before IKE begins rejecting new SA requests.
Step 4	exit Example: Router(config)# exit	Returns to privileged EXEC mode.

Configuring the System Resource Limit

Perform this task to configure the system resource limit. The router drops new IKE SA requests when the level of system resources that are configured in the unit of charge is being used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call admission limit** *charge*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	call admission limit charge Example: Router(config)# call admission limit 1000	Sets the level of the system resources that, when used, causes IKE to stop accepting new SA requests. <ul style="list-style-type: none"> <i>charge</i>—Valid values are 1 to 100000. Note See “System Resource Usage” section on page 3
Step 4	exit Example: Router(config)# exit	Returns to privileged EXEC mode.

Verifying the Call Admission Control for IKE Configuration

To verify the CAC for IKE configuration, perform the following steps.

SUMMARY STEPS

1. show call admission statistics
2. show crypto call admission statistics

DETAILED STEPS



Note

For detailed field descriptions of the command output, see the [“Command Reference” section on page 8](#).

Step 1 show call admission statistics

Use this command to monitor the global CAC configuration parameters and the behavior of CAC.

```
Router# show call admission statistics
```

```
Total Call admission charges: 82, limit 1000
Total calls rejected 1430, accepted 0
Load metric: charge 82, unscaled 82%
```

Step 2 show crypto call admission statistics

Use this command to monitor crypto CAC statistics.

```
Router# show crypto call admission statistics
```

```
-----  
Crypto Call Admission Control Statistics  
-----  
System Resource Limit: 90 Max IKE SAs: 0 Max in nego: 25  
Total IKE SA Count: 359 active: 338 negotiating: 21  
Incoming IKE Requests: 1297 accepted: 166 rejected: 1131  
Outgoing IKE Requests: 1771 accepted: 195 rejected: 1576  
Rejected IKE Requests: 2707 rsrc low: 1314 SA limit: 1393  
-----
```

Configuration Examples for Call Admission Control for IKE

This section provides the following configuration examples:

- [Configuring the IKE Security Association Limit: Example, page 6](#)
- [Configuring the System Resource Limit: Example, page 6](#)

Configuring the IKE Security Association Limit: Example

The following example shows how to specify that there can be a maximum of 25 SAs before IKE starts rejecting new SA requests:

```
Router(config)# crypto call admission limit ike sa 25
```

Configuring the System Resource Limit: Example

The following example shows how to specify that IKE should drop SA requests when the level of system resources that are configured in the unit of charge reaches 9000:

```
Router(config)# call admission limit 9000
```

Additional References

The following sections provide references related to Call Admission Control for IKE.

Related Documents

Related Topic	Document Title
IKE commands	• Cisco IOS Security Command Reference

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC #2409	<i>The Internet Key Exchange</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

- **call admission limit**
- **clear crypto call admission statistics**
- **crypto call admission limit**
- **show call admission statistics**
- **show crypto call admission statistics**

Feature Information for Call Admission Control for IKE

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, Catalyst OS, and Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Call Admission Control for IKE

Feature Name	Releases	Feature Information
Call Admission Control for IKE	12.3(8)T	The Call Admission Control for IKE feature describes the application of Call Admission Control (CAC) to the Internet Key Exchange (IKE) protocol in Cisco IOS. CAC limits the number of simultaneous IKE security associations (SAs) (that is, calls to CAC) that a router can establish.
	12.2(18)SXD1	
	12.4(6)T	
	12.2(33)SRA	
	12.2(33)SXH	
Cisco IOS XE Release 2.1		In Cisco IOS Release 12.3(8)T, this feature was introduced.
		This feature was integrated into Cisco IOS Release 12.2(18)SXD1 and implemented on the Cisco 6500 and Cisco 7600 routers.
		In Cisco IOS Release 12.4(6)T, the ability to configure a limit on the number of in-negotiation IKE connections was added to this and subsequent T-train releases.
		In 12.2(33)SRA, the ability to configure a limit on the number of in-negotiation IKE connections was added.
		In Cisco IOS Release 12.2(33)SXH, the ability to configure a limit on the number of in-negotiation IKE connections was added.
		In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR 1000 Series Routers.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2004—2009 Cisco Systems, Inc. All rights reserved.



Certificate to ISAKMP Profile Mapping

First Published: May 17, 2004

Last Updated: August 21, 2007

The Certificate to ISAKMP Profile Mapping feature enables you to assign an Internet Security Association and Key Management Protocol (ISAKMP) profile to a peer on the basis of the contents of arbitrary fields in the certificate. In addition, this feature allows you to assign a group name to those peers that are assigned an ISAKMP profile.

History for Certificate to ISAKMP Profile Mapping Feature

Release	Modification
12.3(8)T	This feature was introduced.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Certificate to ISAKMP Profile Mapping, page 2](#)
- [Restrictions for Certificate to ISAKMP Profile Mapping, page 2](#)
- [Information About Certificate to ISAKMP Profile Mapping, page 2](#)
- [How to Configure Certificate to ISAKMP Profile Mapping, page 3](#)
- [Configuration Examples for Certificate to ISAKMP Profile Mapping, page 7](#)
- [Additional References, page 10](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 12](#)

Prerequisites for Certificate to ISAKMP Profile Mapping

- You should be familiar with configuring certificate maps.
- You should be familiar with configuring ISAKMP profiles.

Restrictions for Certificate to ISAKMP Profile Mapping

This feature will not be applicable if you use Rivest, Shamir, and Adelman- (RSA-) signature or RSA-encryption authentication without certificate exchange. ISAKMP peers must be configured to do RSA-signature or RSA-encryption authentication using certificates.

Information About Certificate to ISAKMP Profile Mapping

To configure the Certificate to ISAKMP Profile Mapping feature, you should understand the following concepts:

- [Certificate to ISAKMP Profile Mapping Overview, page 2](#)
- [How Certificate to ISAKMP Profile Mapping Works, page 2](#)
- [Assigning an ISAKMP Profile and Group Name to a Peer, page 3](#)

Certificate to ISAKMP Profile Mapping Overview

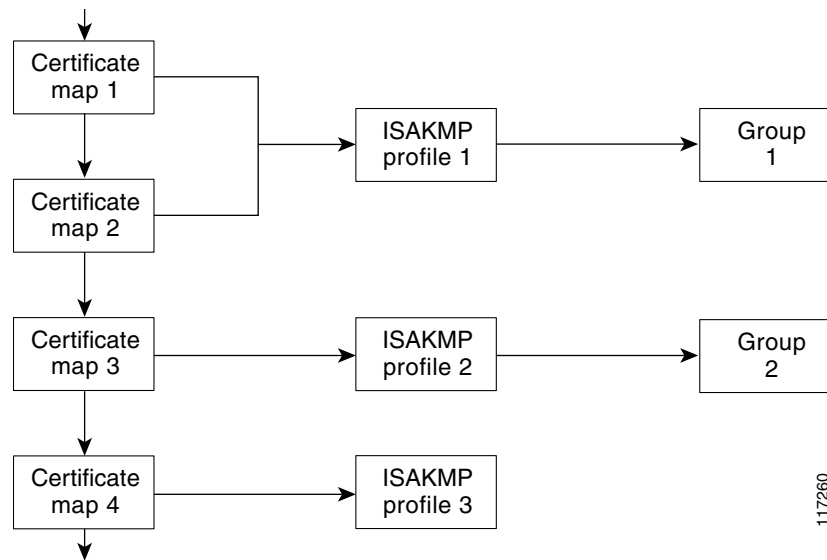
Prior to Cisco IOS Release 12.3(8)T, the only way to map a peer to an ISAKMP profile was as follows. The ISAKMP identity field in the ISAKMP exchange was used for mapping a peer to an ISAKMP profile. When certificates were used for authentication, the ISAKMP identity payload contained the subject name from the certificate. If a certificate authority (CA) did not provide the required group value in the first Organizational Unit (OU) field of a certificate, an ISAKMP profile could not be assigned to a peer.

Effective with Cisco IOS Release 12.3(8)T, a peer can still be mapped as explained above. However, the Certificate to ISAKMP Profile Mapping feature enables you to assign an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate. You are no longer limited to assigning an ISAKMP profile on the basis of the subject name of the certificate. In addition, this feature allows you to assign a group to a peer to which an ISAKMP profile has been assigned.

How Certificate to ISAKMP Profile Mapping Works

[Figure 1](#) illustrates how certificate maps may be attached to ISAKMP profiles and assigned group names.

Figure 1 *Certificate Maps Mapped for Profile Group Assignment*



A certificate map can be attached to only one ISAKMP profile although an ISAKMP profile can have several certificate maps attached to it.

Certificate maps provide the ability for a certificate to be matched with a given set of criteria. ISAKMP profiles can bind themselves to certificate maps, and if the presented certificate matches the certificate map present in an ISAKMP profile, the peer will be assigned the ISAKMP profile. If the ISAKMP profile contains a client configuration group name, the same group name will be assigned to the peer. This ISAKMP profile information will override the information in the ID_KEY_ID identity or in the first OU field of the certificate.

Assigning an ISAKMP Profile and Group Name to a Peer

To assign an ISAKMP profile to a peer on the basis of arbitrary fields in the certificate, use the **match certificate** command after the ISAKMP profile has been defined.

To associate a group name with an ISAKMP profile that will be assigned to a peer, use the **client configuration group** command, also after the ISAKMP profile has been defined.

How to Configure Certificate to ISAKMP Profile Mapping

This section contains the following procedures:

- [Mapping the Certificate to the ISAKMP Profile, page 4](#) (required)
- [Verifying That the Certificate Has Been Mapped, page 4](#) (optional)
- [Assigning the Group Name to the Peer, page 5](#) (required)
- [Monitoring and Maintaining Your Certificate to ISAKMP Profile Mapping, page 6](#) (optional)

Mapping the Certificate to the ISAKMP Profile

To map the certificate to the ISAKMP profile, perform the following steps. This configuration will enable you to assign the ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate.

SUMMARY STEPS

- 1. `enable`
- 2. `configure terminal`
- 3. `crypto isakmp profile profile-name`
- 4. `match certificate certificate-map`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router# <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>crypto isakmp profile profile-name</code> Example: Router (config)# <code>crypto isakmp profile vpnprofile</code>	Defines an ISAKMP profile and enters into crypto ISAKMP profile configuration mode.
Step 4	<code>match certificate certificate-map</code> Example: Router (conf-isa-prof)# <code>match certificate map1</code>	Accepts the name of a certificate map.

Verifying That the Certificate Has Been Mapped

The following `show` command may be used to verify that the subject name of the certificate map has been properly configured.

SUMMARY

- 1. `enable`
- 2. `show crypto ca certificates`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	show crypto ca certificates Example: Router# show crypto ca certificates	Displays information about your certificate.

Assigning the Group Name to the Peer

To associate a group name with a peer when the peer is mapped to an ISAKMP profile, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **client configuration group** *group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp profile <i>profile-name</i> Example: Router (config)# crypto isakmp profile vpnprofile	Defines an ISAKMP profile and enters into isakmp profile configuration mode.
Step 4	client configuration group <i>group-name</i> Example: Router (conf-isa-prof)# client configuration group group1	Accepts the name of a group that will be assigned to a peer when the peer is assigned this crypto ISAKMP profile.

Monitoring and Maintaining Your Certificate to ISAKMP Profile Mapping

To monitor and maintain your certificate to ISAKMP profile mapping, you may use the following **debug** command.

SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router# enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug crypto isakmp	Displays output showing that the certificate has gone through certificate map matching and that the certificate matches the ISAKMP profile.
	Example: Router# debug crypto isakmp	The command may also be used to verify that the peer has been assigned a group.

Configuration Examples for Certificate to ISAKMP Profile Mapping

This section contains the following configuration examples:

- [Certificates Mapped to the ISAKMP Profile on the Basis of Arbitrary Fields: Example, page 7](#)
- [Group Name Assigned to a Peer That Is Associated with an ISAKMP Profile: Example, page 7](#)
- [Mapping a Certificate to an ISAKMP Profile Verification: Example, page 8](#)
- [Group Name Assigned to a Peer Verification: Example, page 9](#)

Certificates Mapped to the ISAKMP Profile on the Basis of Arbitrary Fields: Example

The following configuration example shows that whenever a certificate contains “ou = green,” the ISAKMP profile “cert_pro” will be assigned to the peer:

```
crypto pki certificate map cert_map 10
  subject-name co ou = green
!
!
crypto isakmp identity dn
crypto isakmp profile cert_pro
  ca trust-point 2315
  ca trust-point LaBcA
  initiate mode aggressive
  match certificate cert_map
```

Group Name Assigned to a Peer That Is Associated with an ISAKMP Profile: Example

The following example shows that the group “some_group” is to be associated with a peer that has been assigned an ISAKMP profile:

```
crypto isakmp profile id_profile
  ca trust-point 2315
```

```
match identity host domain cisco.com
client configuration group some_group
```

Mapping a Certificate to an ISAKMP Profile Verification: Example

The following examples show that a certificate has been mapped to an ISAKMP profile. The examples include the configurations for the responder and initiator, **show command** output verifying that the subject name of the certificate map has been configured, and **debug** command output showing that the certificate has gone through certificate map matching and been matched to the ISAKMP profile.

Responder Configuration

```
crypto pki certificate map cert_map 10
! The above line is the certificate map definition.
subject-name co ou = green
! The above line shows that the subject name must have "ou = green."
!
crypto isakmp profile certpro
! The above line shows that this is the ISAKMP profile that will match if the certificate
of the peer matches cert_map (shown on third line below).
ca trust-point 2315
ca trust-point LaBcA
match certificate cert_map
initiate mode aggressive
```

Initiator Configuration

```
crypto ca trustpoint LaBcA
enrollment url http://10.76.82.20:80/cgi-bin/openscep
subject-name ou=green,c=IN
! The above line ensures that the subject name "ou = green" is set.
revocation-check none
```

show crypto ca certificates Command Output for the Initiator

```
Router# show crypto ca certificates
```

```
Certificate
Status: Available
Certificate Serial Number: 21
Certificate Usage: General Purpose
Issuer:
  cn=blue-lab CA
  o=CISCO
  c=IN
Subject:
  Name: Router1.cisco.com
  c=IN
  ou=green
! The above line is a double check that "ou = green" has been set as the subject name.
  hostname=Router1.cisco.com
Validity Date:
  start date: 14:34:30 UTC Mar 31 2004
  end   date: 14:34:30 UTC Apr 1 2009
  renew date: 00:00:00 UTC Jan 1 1970
Associated Trustpoints: LaBcA
```

debug crypto isakmp Command Output for the Responder

```
Router# debug crypto isakmp
```

```

6d23h: ISAKMP (0:268435460): received packet from 192.0.0.2 dport 500 sport 500 Global (R)
MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:      ID payload
6d23h:      FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:      CERT payload
6d23h:      SIG payload
6d23h:      KEEPALIVE payload
6d23h:      NOTIFY payload
6d23h: ISAKMP:(0:4:HW:2):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:4:HW:2):Old State = IKE_R_MM4 New State = IKE_R_MM5

6d23h: ISAKMP:(0:4:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435460): ID payload
      next-payload : 6
      type          : 2
      FQDN name     : Router1.cisco.com
      protocol      : 17
      port          : 500
      length        : 28
6d23h: ISAKMP:(0:4:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:4:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:4:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:4:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:4:HW:2): OU = green
6d23h: ISAKMP:(0:4:HW:2): certificate map matches certpro profile
! The above line shows that the certificate has gone through certificate map matching and
that it matches the "certpro" profile.
6d23h: ISAKMP:(0:4:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:4:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:4:HW:2): CERT validity confirmed.

```

Group Name Assigned to a Peer Verification: Example

The following configuration and debug output show that a group has been assigned to a peer.

Initiator Configuration

```

crypto isakmp profile certpro
  ca trust-point 2315
  ca trust-point LaBcA
  match certificate cert_map
  client configuration group new_group
! The statement on the above line will assign the group "new_group" to any peer that
matches the ISAKMP profile "certpro."
  initiate mode aggressive
!

```

debug crypto isakmp profile Command Output for the Responder

The following debug output example shows that the peer has been matched to the ISAKMP profile named "certpro" and that it has been assigned a group named "new_group."

```

Router# debug crypto isakmp profile
6d23h: ISAKMP (0:268435461): received packet from 192.0.0.2 dport 500 sport 500 Global (R)
MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:      ID payload
6d23h:      FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:      CERT payload
6d23h:      SIG payload
6d23h:      KEEPALIVE payload

```

```

6d23h:          NOTIFY payload
6d23h: ISAKMP:(0:5:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:5:HW:2):Old State = IKE_R_MM4 New State = IKE_R_MM5

6d23h: ISAKMP:(0:5:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435461): ID payload
      next-payload : 6
      type          : 2
      FQDN name     : Router1.cisco.com
      protocol      : 17
      port          : 500
      length        : 28
6d23h: ISAKMP:(0:5:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:5:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:5:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:5:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:5:HW:2): OU = green
6d23h: ISAKMP:(0:5:HW:2): certificate map matches certpro profile
6d23h: ISAKMP:(0:5:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:5:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:5:HW:2): CERT validity confirmed.
6d23h: ISAKMP:(0:5:HW:2):Profile has no keyring, aborting key search
6d23h: ISAKMP:(0:5:HW:2): Profile certpro assigned peer the group named new_group

```

Additional References

The following sections provide references related to Certificate to ISAKMP Profile Mapping.

Related Documents

Related Topic	Document Title
Configuring ISAKMP profiles	VRF-Aware IPsec , Release 12.2 T
Security commands	Cisco IOS Security Command Reference , Release 12.4 T

Standards

Standards	Title
There are no new or modified standards associated with this feature.	—

MIBs

MIBs	MIBs Link
There are no new or modified MIBs associated with this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
There are no new or modified RFCs associated with this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **client configuration group**
- **match certificate (ISAKMP)**

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



Encrypted Preshared Key

The Encrypted Preshared Key feature allows you to securely store plain text passwords in type 6 (encrypted) format in NVRAM.

Feature History for Encrypted Preshared Key

Release	Modification
12.3(2)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Encrypted Preshared Key, page 2](#)
- [Information About Encrypted Preshared Key, page 2](#)
- [How to Configure an Encrypted Preshared Key, page 3](#)
- [Configuration Examples for Encrypted Preshared Key, page 11](#)
- [Where to Go Next, page 13](#)
- [Additional References, page 14](#)
- [Command Reference, page 15](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Encrypted Preshared Key

- Old ROM monitors (ROMMONs) and boot images cannot recognize the new type 6 passwords. Therefore, errors are expected if you boot from an old ROMMON.
- For Cisco 836 routers, please note that support for Advanced Encryption Standard (AES) is available only on IP plus images.

Information About Encrypted Preshared Key

Before Using the Encrypted Preshared Key feature, you should understand the following concepts:

- [Using the Encrypted Preshared Key Feature to Securely Store Passwords, page 2](#)
- [How to Configure an Encrypted Preshared Key, page 3](#)

Using the Encrypted Preshared Key Feature to Securely Store Passwords

Using the Encrypted Preshared Key feature, you can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encryption** command with the **password encryption aes** command to configure and enable the password (symmetric cipher AES is used to encrypt the keys). The password (key) configured using the **config-key password-encryption** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes** command without configuring the **key config-key password-encryption** command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

Changing a Password

If the password (master key) is changed, or reencrypted, using the **key config-key password-encryption** command, the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

Deleting a Password

If the master key that was configured using the **key config-key password-encryption** command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.



Caution

If the password configured using the **key config-key password-encryption** command is lost, it cannot be recovered. The password should be stored in a safe location.

Unconfiguring Password Encryption

If you later unconfigure password encryption using the **no password encryption aes** command, all existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the **key config-key password-encryption** command exists, the type 6 passwords will be decrypted as and when required by the application.

Storing Passwords

Because no one can “read” the password (configured using the **key config-key password-encryption** command), there is no way that the password can be retrieved from the router. Existing management stations cannot “know” what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encryption** command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

Configuring New or Unknown Passwords

If you enter or cut and paste cipher text that does not match the master key, or if there is no master key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

If a new master key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the **no key config-key password-encryption** command. Deleting the master key using the **no key config-key password-encryption** command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

Enabling the Encrypted Preshared Key

The **password encryption aes** command is used to enable the encrypted password.

How to Configure an Encrypted Preshared Key

This section contains the following procedures:

- [Configuring an Encrypted Preshared Key, page 4](#) (required)
- [Monitoring Encrypted Preshared Keys, page 5](#) (optional)
- [Configuring an ISAKMP Preshared Key, page 6](#) (optional)
- [Configuring an ISAKMP Preshared Key in ISAKMP Keyrings, page 7](#) (optional)
- [Configuring ISAKMP Aggressive Mode, page 8](#) (optional)
- [Configuring a Unity Server Group Policy, page 9](#) (optional)

- [Configuring an Easy VPN Client, page 10](#) (optional)

Configuring an Encrypted Preshared Key

To configure an encrypted preshared key, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key config-key password-encryption** *[text]*
4. **password encryption aes**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	key config-key password-encryption <i>[text]</i> Example: Router (config)# key config-key password-encryption	Stores a type 6 encryption key in private NVRAM. <ul style="list-style-type: none"> • If you want to key in interactively (using the enter key) and an encrypted key already exists, you will be prompted for the following: Old key, New key, and Confirm key. • If you want to key in interactively but an encryption key is not present, you will be prompted for the following: New key and Confirm key. • If you want to remove the password that is already encrypted, you will see the following prompt: “WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:”.
Step 4	password encryption aes Example: Router (config)# password-encryption aes	Enables the encrypted preshared key.

Troubleshooting Tips

If you see the warning message “ciphertext >[for username bar>] is incompatible with the configured master key,” you have entered or cut and pasted cipher text that does not match the master key or there is no master key. (The cipher text will be accepted or saved.) The warning message will allow you to locate the broken configuration line or lines.

Monitoring Encrypted Preshared Keys

To get logging output for encrypted preshared keys, perform the following steps.

1. **enable**
2. **password logging**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	password logging Example: Router# password logging	Provides a log of debugging output for a type 6 password operation.

Examples

The following **password logging** debug output shows that a new master key has been configured and that the keys have been encrypted with the new master key:

```
Router (config)# key config-key password-encrypt
New key:
Confirm key:
Router (config)#
01:40:57: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master keypas

Router (config)# key config-key password-encrypt
Old key:
New key:
Confirm key:
Router (config)#
01:42:11: TYPE6_PASS: Master key change heralded, re-encrypting the keys
with the new master key
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
```

What To Do Next

You can perform any of the following procedures. Each procedure is independent of the others.

- [Configuring an ISAKMP Preshared Key, page 6](#)
- [Configuring an ISAKMP Preshared Key in ISAKMP Keyrings, page 7](#)
- [Configuring ISAKMP Aggressive Mode, page 8](#)
- [Configuring a Unity Server Group Policy, page 9](#)
- [Configuring an Easy VPN Client, page 10](#)

Configuring an ISAKMP Preshared Key

To configure an ISAKMP preshared key, perform the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp key *keystring* address *peer-address***
4. **crypto isakmp key *keystring* hostname *hostname***

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp key <i>keystring</i> address <i>peer-address</i> Example: Router (config)# crypto isakmp key cisco address 10.2.3.4	Configures a preshared authentication key. <ul style="list-style-type: none">• The <i>peer-address</i> argument specifies the IP address of the remote peer.
Step 4	crypto isakmp key <i>keystring</i> hostname <i>hostname</i> Example: Router (config)# crypto isakmp key foo hostname foo.com	Configures a preshared authentication key. <ul style="list-style-type: none">• The <i>hostname</i> argument specifies the fully qualified domain name (FQDN) of the peer.

Example

The following sample output shows that an encrypted preshared key has been configured:

```
crypto isakmp key 6 _Hg[^^ECgLGgPF^RXTQfDDWQ][YAAB address 10.2.3.4
crypto isakmp key 6 `eR\eTRaKCUZPYYQfDgXRWi_AAB hostname foo.com
```

Configuring an ISAKMP Preshared Key in ISAKMP Keyrings

To configure an ISAKMP preshared key in ISAKMP keyrings, which are used in IPSec Virtual Route Forwarding (VRF) configurations, perform the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto keyring** *keyring-name*
4. **pre-shared-key address** *address* **key** *key*
5. **pre-shared-key hostname** *hostname* **key** *key*

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto keyring <i>keyring-name</i> Example: Router (config)# crypto keyring foo	Defines a crypto keyring to be used during Internet Key Exchange (IKE) authentication and enters keyring configuration mode.
Step 4	pre-shared-key address <i>address</i> key <i>key</i> Example: Router (config-keyring)# pre-shared-key address 10.2.3.5 key cisco	Defines a preshared key to be used for IKE authentication. <ul style="list-style-type: none">• The <i>address</i> argument specifies the IP address of the remote peer.
Step 5	pre-shared-key hostname <i>hostname</i> key <i>key</i> Example: Router (config-keyring)# pre-shared-key hostname foo.com key cisco	Defines a preshared key to be used for IKE authentication. <ul style="list-style-type: none">• The <i>hostname</i> argument specifies the FQDN of the peer.

Example

The following **show-running-config** sample output shows that an encrypted preshared key in ISAKMP keyrings has been configured.

```
crypto keyring foo
  pre-shared-key address 10.2.3.5 key 6 `WHCJYR_Z]GRPF^RXTQfDcfZ]GPAAB
  pre-shared-key hostname foo.com key 6 aE_REHDcOfYCPF^RXTQfDJYVVNSAAB
```

Configuring ISAKMP Aggressive Mode

To configure ISAKMP aggressive mode, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer ip-address** *ip-address*
4. **set aggressive-mode client-endpoint** *client-endpoint*
5. **set aggressive-mode password** *password*

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp peer ip-address <i>ip-address</i> Example: Router (config)# crypto isakmp peer ip-address 10.2.3.4	To enable an IP Security (IPSec) peer for IKE querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode and to enter ISAKMP peer configuration mode.
Step 4	set aggressive-mode client-endpoint <i>client-endpoint</i> Example: Router (config-isakmp-peer)# set aggressive-mode client-endpoint fqdn cisco.com	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.
Step 5	set aggressive-mode password <i>password</i> Example: Router (config-isakmp-peer)# set aggressive-mode password cisco	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

Example

The following **show-running-config** sample output shows that an encrypted preshared key in ISAKMP aggressive mode has been configured.

```
crypto isakmp peer address 10.2.3.4
  set aggressive-mode password 6 ^aKPIQ_KJE_PPF^RXTQfDTiaLNeAAB
  set aggressive-mode client-endpoint fqdn cisco.com
```

Configuring a Unity Server Group Policy

To configure a unity server group policy, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **pool** *name*
5. **domain** *name*
6. **key** *name*

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp client configuration group <i>group-name</i> Example: Router (config)# crypto isakmp client configuration group foo	Specifies the policy profile of the group that will be defined and enters ISAKMP group configuration mode.
Step 4	pool <i>name</i> Example: Router (config-isakmp-group)# pool foopool	Defines a local pool address.

	Command	Description
Step 5	domain name Example: Router (config-isakmp-group)# domain cisco.com	Specifies the Domain Name Service (DNS) domain to which a group belongs.
Step 6	key name Example: Router (config-isakmp-group)# key cisco	Specifies the IKE preshared key for group policy attribute definition.

Example

The following **show-running-config** sample output shows that an encrypted key has been configured for a unity server group policy:

```
crypto isakmp client configuration group foo
key 6 cZZgDZPOE\ddPF^RXTQfDTIaLNeAAB
domain cisco.com
pool foopool
```

Configuring an Easy VPN Client

To configure an Easy VPN client, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn name**
4. **peer ipaddress**
5. **mode client**
6. **group group-name key group-key**
7. **connect manual**

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command	Description
Step 3	crypto ipsec client ezvpn <i>name</i> Example: Router (config)# crypto ipsec client ezvpn foo	Creates a Cisco Easy VPN remote configuration and enters Cisco Easy VPN remote configuration mode.
Step 4	peer <i>ipaddress</i> Example: Router (config-isakmp-peer)# peer 10.2.3.4	Sets the peer IP address for the VPN connection.
Step 5	mode client Example: Router (config-isakmp-ezvpn)# mode client	Automatically configures the router for Cisco Easy VPNclient mode operation, which uses Network Address Translation (NAT) or Peer Address Translation (PAT) address translations.
Step 6	group <i>group-name</i> key <i>group-key</i> Example: Router (config-isakmp-ezvpn)# group foo key cisco	Specifies the group name and key value for the VPN connection.
Step 7	connect manual Example: Router (config-isakmp-ezvpn)# connect manual	Specifies the manual setting for directing the Cisco Easy VPN remote client to wait for a command or application program interface (API) call before attempting to establish the Cisco Easy VPN remote connection.

Example

The following **show-running-config** sample output shows that an Easy VPN client has been configured. The key has been encrypted.

```
crypto ipsec client ezvpn foo
connect manual
group foo key 6 gdMI`S^[GicPF^RXTQfDFKEO\RAAB
mode client
peer 10.2.3.4
```

Configuration Examples for Encrypted Preshared Key

This section provides the following configuration examples:

- [Encrypted Preshared Key: Example, page 12](#)
- [No Previous Key Present: Example, page 12](#)
- [Key Already Exists: Example, page 12](#)
- [Key Already Exists But the User Wants to Key In Interactively: Example, page 12](#)
- [No Key Present But the User Wants to Key In Interactively: Example, page 12](#)
- [Removal of the Password Encryption: Example, page 13](#)

Encrypted Preshared Key: Example

The following is an example of a configuration for which a type 6 preshared key has been encrypted. It includes the prompts and messages that a user might see.

```
Router (config)# crypto isakmp key cisco address 10.0.0.2
Router (config)# exit
Router# show running-config | include crypto isakmp key
crypto isakmp key cisco address 10.0.0.2
Router#
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)# password encryption aes
Router (config)# key config-key password-encrypt
New key:
Confirm key:
Router (config)#
01:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Router (config)# exit
Router # show running-config | include crypto isakmp key
crypto isakmp key 6 CXWdhVTZYB_Vcd^`cIHDOahiFTa address 10.0.0.2
```

No Previous Key Present: Example

In the following configuration example, no previous key is present:

```
Router (config)# key config-key password-encryption testkey 123
```

Key Already Exists: Example

In the following configuration example, a key already exists:

```
Router (config)# key config-key password-encryption testkey123
Old key:
Router (config)#
```

Key Already Exists But the User Wants to Key In Interactively: Example

In the following configuration example, the user wants to key in interactively, but a key already exists. The Old key, New key, and Confirm key prompts will show on your screen if you enter the **key config-key password-encryption** command and press the enter key to get into interactive mode.

```
Router (config)# key config-key password-encryption
Old key:
New key:
Confirm key:
```

No Key Present But the User Wants to Key In Interactively: Example

In the following example, the user wants to key in interactively, but no key is present. The New key and Confirm key prompts will show on your screen if you are in interactive mode.

```
Router (config)# key config-key password-encryption
New key:
```

Confirm key:

Removal of the Password Encryption: Example

In the following configuration example, the user wants to remove the encrypted password. The “WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:” prompt will show on your screen if you are in interactive mode.

```
Router (config)# no key config-key password-encryption
```

```
WARNING: All type 6 encrypted keys will become unusable. Continue with master key  
deletion ? [yes/no]: y
```

Where to Go Next

Configure any other preshared keys.

Additional References

The following sections provide references related to Encrypted Preshared Key.

Related Documents

Related Topic	Document Title
Configuring passwords	<ul style="list-style-type: none"> • Cisco IOS Security Command Reference • “About Cisco IOS and Cisco IOS XE Software Documentation” chapter of the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>

Standards

Standards	Title
This feature has no new or modified standards.	—

MIBs

MIBs	MIBs Link
This feature has no new or modified MIBs.	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFCs	Title
This feature has no new or modified RFCs.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **crypto ipsec client ezvpn (global)**
- **crypto isakmp client configuration group**
- **crypto isakmp key**
- **key config-key password-encryption**
- **password encryption aes**
- **password logging**
- **pre-shared-key**
- **set aggressive-mode password**

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Distinguished Name Based Crypto Maps

Feature History

Release	Modification
12.2(4)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This feature module describes the Distinguished Name Based Crypto Map feature in Cisco IOS Release 12.2(4)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 6](#)

Feature Overview

The Distinguished Name Based Crypto Maps feature allows you to configure the router to restrict access to selected encrypted interfaces for those peers with specific certificates, especially certificates with particular Distinguished Names (DNs).

Previously, if the router accepted a certificate or a shared secret from the encrypting peer, Cisco IOS did not have a method of preventing the peer from communicating with any encrypted interface other than the restrictions on the IP address of the encrypting peer. This feature allows you to configure which crypto maps are usable to a peer based on the DN that a peer used to authenticate itself, thereby, enabling you to control which encrypted interfaces a peer with a specified DN can access.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Benefits

The Distinguished Name Based Crypto Maps feature allows you to set restrictions in the router configuration that prevent peers with specific certificates—especially certificates with particular DNs—from having access to selected encrypted interfaces.

Restrictions

System Requirements

To configure this feature, your router must support IP Security.

Performance Impact

If you restrict access to a large number of DNs, it is recommended that you specify a few number of crypto maps referring to large identity sections instead of specifying a large number of crypto maps referring to small identity sections.

Related Documents

The following documents provide information related to the Distinguished Name Based Crypto Maps feature:

- *Cisco IOS Security Command Reference*, Release 12.2
- *Cisco IOS Security Configuration Guide*, Release 12.2

Supported Platforms

This feature is supported on the following platforms:

- Cisco 1700 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 7100 series
- Cisco 7200 series
- Cisco uBR905 Cable Access Router
- Cisco uBR925 Cable Access Router

Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Feature Navigator home page at the following URL: <http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

None

Prerequisites

Before configuring a DN based crypto map, you must perform the following tasks:

- Create an Internet Key Exchange (IKE) policy at each peer.
For more information on creating IKE policies, refer to the chapter “Configuring Internet Key Exchange Security Protocol” of the *Cisco IOS Security Configuration Guide*.
- Create crypto map entries for IPsec.
For more information on creating crypto map entries, refer to the chapter “Configuring IPsec Network Security” of the *Cisco IOS Security Configuration Guide*.

Configuration Tasks

See the following sections for configuration tasks for the Distinguished Name Based Crypto Maps feature. Each task in the list is identified as either required or optional.

- [Configuring DN Based Crypto Maps \(authenticated by DN\)](#) (required)
- [Configuring DN Based Crypto Maps \(authenticated by hostname\)](#) (required)
- [Applying Identity to DN Based Crypto Maps](#) (required)
- [Verifying DN Based Crypto Maps](#) (optional)

Configuring DN Based Crypto Maps (authenticated by DN)

To configure a DN based crypto map that can be used only by peers that have been authenticated by a DN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>Router(config)# crypto identity name</code>	Configures the identity of a router with the given list of DNs in the certificate of the router and enters crypto identity configuration mode.
Step 2	<code>Router(crypto-identity)# dn name=string [,name=string]</code>	Associates the identity of the router with the DN in the certificate of the router. Note The identity of the peer must match the identity in the exchanged certificate.

Configuring DN Based Crypto Maps (authenticated by hostname)

To configure a DN based crypto map that can be used only by peers that have been authenticated by a hostname, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>Router(config)# crypto identity name</code>	Configures the identity of a router with the given list of DNs in the certificate of the router and enters crypto identity configuration mode.
Step 2	<code>Router(crypto-identity)# fqdn name</code>	Associates the identity of the router with the hostname that the peer used to authenticate itself. Note The identity of the peer must match the identity in the exchanged certificate.

Applying Identity to DN Based Crypto Maps

To apply the identity (within the crypto map context), use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto map <i>map-name seq-num ipsec-isakmp</i>	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
Step 2	Router(config-crypto-map)# identity <i>name</i>	<p>Applies the identity to the crypto map.</p> <p>When this command is applied, only the hosts that match a configuration listed within the identity <i>name</i> can use the specified crypto map.</p> <p>Note If the identity command does not appear within the crypto map, the encrypted connection does not have any restrictions other than the IP address of the encrypting peer.</p>

Verifying DN Based Crypto Maps

To verify that this functionality is properly configured, use the following command in EXEC mode:

Command	Purpose
Router# show crypto identity	Displays the configured identities.

Troubleshooting Tips

If an encrypting peer attempts to establish a connection that is blocked by the DN based crypto map configuration, the following error message will be logged:

```
<time>: %CRYPTO-4-IKE_QUICKMODE_BAD_CERT: encrypted connection attempted with a peer
without the configured certificate attributes.
```

Configuration Examples

This section provides the following configuration example:

- [DN Based Crypto Map Configuration Example](#)

DN Based Crypto Map Configuration Example

The following example shows how to configure DN based crypto maps that have been authenticated by DN and hostname. Comments are included inline to explain various commands.

```
! DN based crypto maps require you to configure an IKE policy at each peer.
crypto isakmp policy 15
  encryption 3des
  hash md5
  authentication rsa-sig
  group 2
  lifetime 5000
crypto isakmp policy 20
```

```

authentication pre-share
lifetime 10000
crypto isakmp key 1234567890 address 171.69.224.33
!
! The following is an IPSec crypto map (part of IPSec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
set peer 172.21.114.196
set transform-set my-transformset
match address 124
identity to-bigbiz
!
crypto identity to-bigbiz
dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
set peer 172.21.115.119
set transform-set my-transformset
match address 125
identity to-little-com
!
crypto identity to-little-com
fqdn little.com
!

```

Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **crypto identity**
- **dn**
- **fqdn**
- **identity**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



VRF-Aware IPSec

The VRF-Aware IPSec feature introduces IP Security (IPSec) tunnel mapping to Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Using the VRF-Aware IPSec feature, you can map IPSec tunnels to Virtual Routing and Forwarding (VRF) instances using a single public-facing address.

Feature Specifications for VRF-Aware IPSec

Feature History

Release	Modification
12.2(15)T	This feature was introduced.

Supported Platforms

Cisco 1710, Cisco 1760, Cisco 2610-Cisco 2613, Cisco 2620-Cisco 2621, Cisco 2650-Cisco 2651, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7100, Cisco 7200, Cisco 7400, Cisco 870 Series

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for VRF-Aware IPSec, page 2](#)
- [Information About VRF-Aware IPSec, page 2](#)
- [How to Configure VRF-Aware IPSec, page 4](#)
- [Configuration Examples for VRF-Aware IPSec, page 22](#)
- [Additional References, page 34](#)
- [Command Reference, page 35](#)
- [Glossary, page 37](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for VRF-Aware IPsec

- If you are configuring VRF-Aware IPsec using a crypto map configuration and the Inside VRF (IVRF) is not the same as the Front Door VRF (FVRF), this feature is not interoperable with unicast reverse path forwarding (uRPF) if uRPF is enabled on the crypto map interface. If your network requires uRPF, it is recommended that you use Virtual Tunnel Interface (VTI) for IPsec instead of crypto maps.
- The VRF-Aware IPsec feature does not allow IPsec tunnel mapping between VRFs. For example, it does not allow IPsec tunnel mapping from VRF vpn1 to VRF vpn2.

Information About VRF-Aware IPsec

The VRF-Aware IPsec feature maps an IPsec tunnel to a MPLS VPN. To configure and use the feature, you need to understand the following concepts:

- [VRF Instance, page 2](#)
- [MPLS Distribution Protocol, page 2](#)
- [VRF-Aware IPsec Functional Overview, page 2](#)

VRF Instance

A VRF instance is a per-VPN routing information repository that defines the VPN membership of a customer site attached to the Provider Edge (PE) router. A VRF comprises an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table. A separate set of routing and CEF tables is maintained for each VPN customer.

MPLS Distribution Protocol

The MPLS distribution protocol is a high-performance packet-forwarding technology that integrates the performance and traffic management capabilities of data link layer switching with the scalability, flexibility, and performance of network-layer routing.

VRF-Aware IPsec Functional Overview

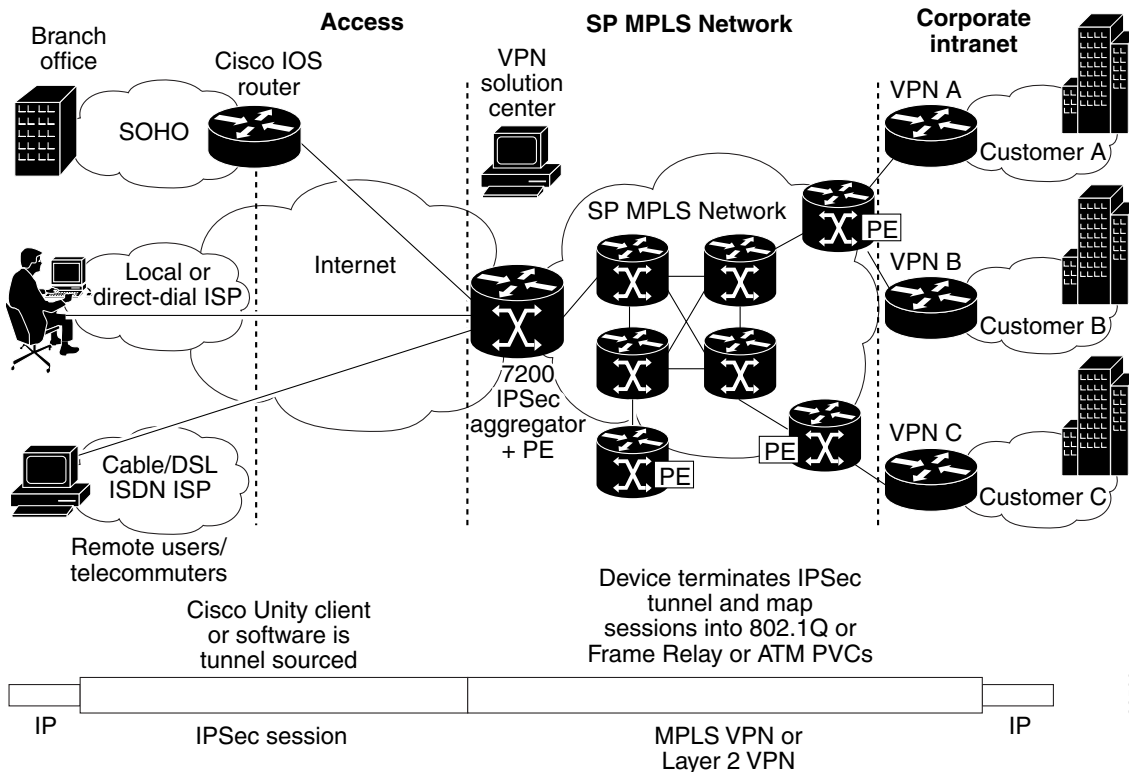
Front Door VRF (FVRF) and Inside VRF (IVRF) are central to understanding the feature.

Each IPsec tunnel is associated with two VRF domains. The outer encapsulated packet belongs to one VRF domain, which we shall call the FVRF, while the inner, protected IP packet belongs to another domain called the IVRF. Another way of stating the same thing is that the local endpoint of the IPsec tunnel belongs to the FVRF while the source and destination addresses of the inside packet belong to the IVRF.

One or more IPsec tunnels can terminate on a single interface. The FVRF of all these tunnels is the same and is set to the VRF that is configured on that interface. The IVRF of these tunnels can be different and depends on the VRF that is defined in the Internet Security Association and Key Management Protocol (ISAKMP) profile that is attached to a crypto map entry.

Figure 96 is an illustration of a scenario showing IPSec to MPLS and Layer 2 VPNs.

Figure 96 *IPSec to MPLS and Layer 2 VPNs*



88500

Packet Flow into the IPSec Tunnel

- A VPN packet arrives from the Service Provider MPLS backbone network to the PE and is routed through an interface facing the Internet.
- The packet is matched against the Security Policy Database (SPD), and the packet is IPSec encapsulated. The SPD includes the IVRF and the access control list (ACL).
- The IPSec encapsulated packet is then forwarded using the FVRF routing table.

Packet Flow from the IPSec Tunnel

- An IPSec-encapsulated packet arrives at the PE router from the remote IPSec endpoint.
- IPSec performs the Security Association (SA) lookup for the Security Parameter Index (SPI), destination, and protocol.
- The packet is decapsulated using the SA and is associated with IVRF.
- The packet is further forwarded using the IVRF routing table.

How to Configure VRF-Aware IPSec

This section contains the following procedures:

- [Configuring Crypto Keyrings, page 4](#) (Optional)
- [Configuring ISAKMP Profiles, page 6](#) (Required)
- [Configuring an ISAKMP Profile on a Crypto Map, page 10](#) (Required)
- [Configuring to Ignore Extended Authentication During IKE Phase 1 Negotiation, page 11](#) (Optional)
- [Verifying VRF-Aware IPSec, page 12](#)
- [Clearing Security Associations, page 13](#)
- [Troubleshooting VRF-Aware IPSec, page 13](#)

Configuring Crypto Keyrings

A crypto keyring is a repository of preshared and Rivest, Shamir, and Adelman (RSA) public keys. There can be zero or more keyrings on the Cisco IOS router.

Perform the following optional task to configure a crypto keyring.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto keyring** *keyring-name* [**vrf** *fvr-f-name*]
4. **description** *string* (Optional)
5. **pre-shared-key** {**address** *address* [*mask*] | **hostname** *hostname*} **key** *key* (Optional)
6. **rsa-pubkey** {**address** *address* | **name** *fqdn*} [**encryption** | **signature**] (Optional)
7. **address** *ip-address* (Optional)
8. **serial-number** *serial-number* (Optional)
9. **key-string**
10. **text**
11. **quit**
12. **exit**
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto keyring <i>keyring-name</i> [vrf <i>fvrfr-name</i>] Example: Router (config)# crypto keyring VPN1	Defines a keyring with <i>keyring-name</i> as the name of the keyring and enters keyring configuration mode. <ul style="list-style-type: none"> (Optional) The vrf keyword and <i>fvrfr-name</i> argument imply that the keyring is bound to Front Door Virtual Routing and Forwarding (FVRF). The key in the keyring is searched if the local endpoint is in FVRF. If vrf is not specified, the keyring is bound to the global.
Step 4	description <i>string</i> Router (config-keyring)# description The keys for VPN1	(Optional) Specifies a one-line description of the keyring.
Step 5	pre-shared-key { address <i>address</i> [<i>mask</i>] hostname <i>hostname</i> } key <i>key</i> Example: Router (config-keyring)# pre-shared-key address 10.72.23.11 key VPN1	(Optional) Defines a preshared key by address or host name.
Step 6	rsa-pubkey { address <i>address</i> name <i>fqdn</i> } [encryption signature] Example: Router(config-keyring)# rsa-pubkey name host.vpn.com	(Optional) Defines a Rivest, Shamir, and Adelman (RSA) public key by address or host name and enters rsa-pubkey configuration mode. <ul style="list-style-type: none"> By default, the key is used for signature. The optional encryption keyword specifies that the key should be used for encryption. The optional signature keyword specifies that the key should be used for signature. By default, the key is used for signature.
Step 7	address <i>ip-address</i> Example: Router(config-pubkey-key)# address 10.5.5.1	(Optional) Defines the RSA public key IP address.
Step 8	serial-number <i>serial-number</i> Example: Router(config-pubkey-key)# serial-number 1000000	(Optional) Specifies the serial number of the public key. The value is from 0 through infinity.

	Command or Action	Purpose
Step 9	key-string Example: Router (config-pubkey-key)# key-string	Enters into the text mode in which you define the public key.
Step 10	text Example: Router (config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973	Specifies the public key. Note Only one public key may be added in this step.
Step 11	quit Example: Router (config-pubkey)# quit	Quits to the public key configuration mode.
Step 12	exit Example: Router (config-pubkey)# exit	Exits to the keyring configuration mode.
Step 13	exit Example: Router(config-keyring)# exit#	Exits to global configuration mode.

Configuring ISAKMP Profiles

An ISAKMP profile is a repository for IKE Phase 1 and IKE Phase 1.5 configuration for a set of peers. An ISAKMP profile defines items such as keepalive, trustpoints, peer identities, and XAUTH AAA list during the IKE Phase 1 and Phase 1.5 exchange. There can be zero or more ISAKMP profiles on the Cisco IOS router.



Note

- If traffic from the router to a certification authority (CA) (for authentication, enrollment, or for obtaining a certificate revocation list [CRL]) or to an Lightweight Directory Access Protocol (LDAP) server (for obtaining a CRL) needs to be routed via a VRF, the **vrf** command must be added to the trustpoint. Otherwise, such traffic will use the default routing table.
- If a profile does not specify one or more trustpoints, all trustpoints in the router will be used to attempt to validate the certificate of the peer (Internet Key Exchange (IKE) main mode or signature authentication). If one or more trustpoints are specified, only those trustpoints will be used.

Restriction

A router initiating IKE and a router responding to the IKE request should have symmetrical trustpoint configurations. For example, a responding router (in IKE Main Mode) performing RSA signature encryption and authentication might use trustpoints that were defined in the global configuration when sending the CERT-REQ payloads. However, the router might use a restricted list of trustpoints that were defined in the ISAKMP profile for the certificate verification. If the peer (the IKE initiator) is configured

to use a certificate whose trustpoint is in the global list of the responding router but not in ISAKMP profile of the responding router, the certificate will be rejected. (However, if the initiating router does not know about the trustpoints in the global configuration of the responding router, the certificate can still be authenticated.)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **description** *string* (Optional)
5. **vrf** *ivrf-name* (Optional)
6. **keepalive** *seconds* **retry** *retry-seconds* (Optional)
7. **self-identity** {**address** | **fqdn** | **user-fqdn** *user-fqdn*} (Optional)
8. **keyring** *keyring-name* (Optional)
9. **ca trust-point** *trustpoint-name* (Optional)
10. **match identity** {**group** *group-name* | **address** *address* [*mask*] [*fvr*] | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}
11. **client configuration address** {**initiate** | **respond**} (Optional)
12. **client authentication list** *list-name* (Optional)
13. **isakmp authorization list** *list-name* (Optional)
14. **initiate mode aggressive**
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	crypto isakmp profile <i>profile-name</i>	Defines an Internet Security Association and Key Management Protocol (ISAKMP) profile and enters into isakmp profile configuration mode.
	Example: Router (config)# crypto isakmp profile vpnprofile	

	Command or Action	Purpose
Step 4	description <i>string</i> Example: Router (conf-isa-prof)# description configuration for VPN profile	(Optional) Specifies a one-line description of an ISAKMP profile.
Step 5	vrf <i>ivrf-name</i> Example: Router (conf-isa-prof)# vrf VPN1	(Optional) Maps the IPSec tunnel to a Virtual Routing and Forwarding (VRF) instance. Note The VRF also serves as a selector for matching the Security Policy Database (SPD). If the VRF is not specified in the ISAKMP profile, the IVRF of the IPSec tunnel will be the same as its FVRF.
Step 6	keepalive <i>seconds</i> retry <i>retry-seconds</i> Example: Router (conf-isa-prof)# keepalive 60 retry 5	(Optional) Allows the gateway to send dead peer detection (DPD) messages to the peer. <ul style="list-style-type: none"> If not defined, the gateway uses the global configured value. <i>seconds</i>—Number of seconds between DPD messages. The range is from 10 to 3600 seconds. retry <i>retry-seconds</i>—Number of seconds between retries if the DPD message fails. The range is from 2 to 60 seconds.
Step 7	self-identity { <i>address</i> <i>fqdn</i> <i>user-fqdn</i> <i>user-fqdn</i> } Example: Router (conf-isa-prof)# self-identity address	(Optional) Specifies the identity that the local Internet Key Exchange (IKE) should use to identify itself to the remote peer. <ul style="list-style-type: none"> If not defined, IKE uses the global configured value. address—Uses the IP address of the egress interface. fqdn—Uses the fully qualified domain name (FQDN) of the router. user-fqdn—Uses the specified value.
Step 8	keyring <i>keyring-name</i> Example: Router (conf-isa-prof)# keyring VPN1	(Optional) Specifies the keyring to use for Phase 1 authentication. <ul style="list-style-type: none"> If the keyring is not specified, the global key definitions are used.
Step 9	ca trust-point { <i>trustpoint-name</i> } Example: Router (conf-isa-prof)# ca trustpoint VPN1-trustpoint	(Optional) Specifies a trustpoint to validate a Rivest, Shamir, and Adelman (RSA) certificate. <ul style="list-style-type: none"> If no trustpoint is specified in the ISAKMP profile, all the trustpoints that are configured on the Cisco IOS router are used to validate the certificate.

	Command or Action	Purpose
Step 10	<p>match identity {group <i>group-name</i> address <i>address</i> [<i>mask</i>] [<i>fvrfl</i>] host <i>host-name</i> host domain <i>domain-name</i> user <i>user-fqdn</i> user domain <i>domain-name</i>}</p> <p>Example: Router (conf-isa-prof)# match identity address 10.1.1.1</p>	<p>Specifies the client IKE Identity (ID) that is to be matched.</p> <ul style="list-style-type: none"> • group <i>group-name</i>—Matches the <i>group-name</i> with the ID type ID_KEY_ID. It also matches the <i>group-name</i> with the Organizational Unit (OU) field of the Distinguished Name (DN). • address <i>address</i> [<i>mask</i>] <i>fvrfl</i>—Matches the <i>address</i> with the ID type ID_IPV4_ADDR. The <i>mask</i> argument can be used to specify a range of addresses. The <i>fvrfl</i> argument specifies that the address is in Front Door Virtual Routing and Forwarding (FVRF). • host <i>hostname</i>—Matches the <i>hostname</i> with the ID type ID_FQDN. • host domain <i>domainname</i>—Matches the <i>domainname</i> to the ID type ID_FQDN whose domain name is the same as the <i>domainname</i>. Use this command to match all the hosts in the domain. • user <i>username</i>—Matches the <i>username</i> with the ID type ID_USER_FQDN. • user domain <i>domainname</i>—Matches the ID type ID_USER_FQDN whose domain name matches the <i>domainname</i>.
Step 11	<p>client configuration address {initiate respond}</p> <p>Example: Router (conf-isa-prof)# client configuration address initiate</p>	<p>(Optional) Specifies whether to initiate the mode configuration exchange or responds to mode configuration requests.</p>
Step 12	<p>client authentication list <i>list-name</i></p> <p>Example: Router (conf-isa-prof)# client authentication list xauthlist</p>	<p>(Optional) Authentication, authorization, and accounting (AAA) to use for authenticating the remote client during the extended authentication (XAUTH) exchange.</p>
Step 13	<p>isakmp authorization list <i>list-name</i></p> <p>Example: Router (conf-isa-prof)# isakmp authorization list ikessaaalist</p>	<p>(Optional) Network authorization server for receiving the Phase 1 preshared key and other attribute-value (AV) pairs.</p>
Step 14	<p>initiate mode aggressive</p> <p>Example: Router (conf-isa-prof)# initiate mode aggressive</p>	<p>(Optional) Initiates aggressive mode exchange.</p> <ul style="list-style-type: none"> • If not specified, IKE always initiates Main Mode exchange.
Step 15	<p>exit</p> <p>Example: Router (conf-isa-prof)# exit</p>	<p>Exits to global configuration mode.</p>

What to Do Next

Go to the section “[Configuring an ISAKMP Profile on a Crypto Map](#).”

Configuring an ISAKMP Profile on a Crypto Map

An ISAKMP profile must be applied to the crypto map. The IVRF on the ISAKMP profile is used as a selector when matching the VPN traffic. If there is no IVRF on the ISAKMP profile, the IVRF will be equal to the FVRF. Perform this required task to configure an ISAKMP profile on a crypto map.

Prerequisites

Before configuring an ISAKMP profile on a crypto map, you must first have configured your router for basic IPSec.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name* **isakmp-profile** *isakmp-profile-name* (Optional)
4. **set isakmp-profile** *profile-name* (Optional)
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name</i> isakmp-profile <i>isakmp-profile-name</i> Example: Router (config)# crypto map vpnmap isakmp-profile vpnprofile	(Optional) Specifies the Internet Key Exchange and Key Management Protocol (ISAKMP) profile for the crypto map set and enters crypto map configuration mode. <ul style="list-style-type: none"> • The ISAKMP profile will be used during IKE exchange.

	Command or Action	Purpose
Step 4	set isakmp-profile <i>profile-name</i> Example: Router (config-crypto-map)# set isakmp-profile vpnprofile	(Optional) Specifies the ISAKMP profile to use when the traffic matches the crypto map entry.
Step 5	exit Example: Router (config-crypto-map)# exit	Exits to global configuration mode.

Configuring to Ignore Extended Authentication During IKE Phase 1 Negotiation

To ignore XAUTH during an IKE Phase 1 negotiation, use the **no crypto xauth** command. Use the **no crypto xauth** command if you do not require extended authentication for the Unity clients.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no crypto xauth** *interface*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	no crypto xauth <i>interface</i> Example: Router(config)# no crypto xauth ethernet0	Ignores XAUTH proposals for requests that are destined to the IP address of the interface. By default, Internet Key Exchange (IKE) processes XAUTH proposals.

Verifying VRF-Aware IPsec

To verify your VRF-Aware IPsec configurations, use the following **show** commands. These **show** commands allow you to list configuration information and security associations (SAs):

SUMMARY STEPS

- **enable**
- **show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *interface* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name*] [**detail**]
- **show crypto isakmp key**
- **show crypto isakmp profile**
- **show crypto key pubkey-chain rsa**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show crypto ipsec sa [map <i>map-name</i> address identity interface <i>interface</i> peer [vrf <i>fvrf-name</i>] address vrf <i>ivrf-name</i>] [detail] Example: Router# show crypto ipsec sa vrf vpn1	Allows you to view the settings used by current security associations (SAs).
Step 3	show crypto isakmp key Example: Router# show crypto isakmp key	Lists all the keyrings and their preshared keys. <ul style="list-style-type: none"> • Use this command to verify your crypto keyring configuration.
Step 4	show crypto isakmp profile Example: Router# show crypto isakmp profile	Lists all ISAKMP profiles and their configurations.
Step 5	show crypto key pubkey-chain rsa Example: Router# show crypto key pubkey-chain rsa	Views the Rivest, Shamir, and Adelman (RSA) public keys of the peer that are stored on your router. <ul style="list-style-type: none"> • The output is extended to show the keyring to which the public key belongs.

Clearing Security Associations

The following **clear** commands allow you to clear SAs.

SUMMARY STEPS

- **enable**
- **clear crypto sa** [**counters** | **map** *map-name* | **peer** [**vrf** *fvrf-name*] *address* | **spi** *address* {**ah** | **esp**} *spi* | **vrf** *ivrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	clear crypto sa [counters map <i>map-name</i> peer [vrf <i>fvrf-name</i>] <i>address</i> spi <i>address</i> { ah esp } <i>spi</i> vrf <i>ivrf-name</i>] Example: Router# clear crypto sa vrf VPN1	Clears the IPSec security associations (SAs).

Troubleshooting VRF-Aware IPSec

To troubleshoot VRF-Aware IPSec, use the following **debug** commands:

SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec**
3. **debug crypto isakmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug crypto ipsec Example: Router# debug crypto ipsec	Displays IP security (IPSec) events.
Step 3	debug crypto isakmp Example: Router(config)# debug crypto isakmp	Displays messages about Internet Key Exchange (IKE) events.

Debug Examples for VRF-Aware IPSec

The following sample debug outputs are for a VRF-aware IPSec configuration:

IPSec PE

Router# **debug crypto ipsec**

```

Crypto IPSEC debugging is on
IPSEC-PE#debug crypto isakmp
Crypto ISAKMP debugging is on
IPSEC-PE#debug crypto isakmp d
04:31:28: ISAKMP (0:12): purging SA., sa=6482B354, delme=6482B354
04:31:28: ISAKMP: Unlocking IKE struct 0x63C142F8 for declare_sa_dead(), count 0
IPSEC-PE#debug crypto isakmp detail
Crypto ISAKMP internals debugging is on
IPSEC-PE#
IPSEC-PE#
IPSEC-PE#
04:32:07: ISAKMP: Deleting peer node by peer_reap for 10.1.1.1: 63C142F8
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B DC887D4E
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.68.1.1
04:32:55: ISAKMP cookie AA8F7B41 49A60E88
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B DBC8E125
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 B4BDB5B7
04:32:55: ISAKMP (0:0): received packet from 10.1.1.1 dport 500 sport 500 Global (N) NEW
SA
04:32:55: ISAKMP: local port 500, remote port 500
04:32:55: ISAKMP: hash from 729FA94 for 619 bytes
04:32:55: ISAKMP: Packet hash:
64218CC0: B91E2C70 095A1346 9.,p.Z.F
64218CD0: 0EDB4CA6 8A46784F B314FD3B 00 .[L&.FxO.};;.
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:32:55: ISAKMP cookie AA8F7B41 F7ACF384
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:32:55: ISAKMP cookie AA8F7B41 0C07C670
04:32:55: ISAKMP: insert sa successfully sa = 6482B354
04:32:55: ISAKMP (0:13): processing SA payload. message ID = 0

```



```

04:32:55: ISAKMP (0:13): processing ID payload. message ID = 0
04:32:55: ISAKMP (0:13): peer matches vpn2-ra profile
04:32:55: ISAKMP: Looking for a matching key for 10.1.1.1 in default
04:32:55: ISAKMP: Created a peer struct for 10.1.1.1, peer port 500
04:32:55: ISAKMP: Locking peer struct 0x640BBB18, IKE refcount 1 for
crypto_ikmp_config_initialize_sa
04:32:55: ISAKMP (0:13): Setting client config settings 648252B0
04:32:55: ISAKMP (0:13): (Re)Setting client xauth list and state
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 157 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 123 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v2
04:32:55: ISAKMP (0:13): Authentication by xauth preshared
04:32:55: ISAKMP (0:13): Checking ISAKMP transform 1 against priority 1 policy
04:32:55: ISAKMP: encryption 3DES-CBC
04:32:55: ISAKMP: hash SHA
04:32:55: ISAKMP: default group 2
04:32:55: ISAKMP: auth XAUTHInitPreShared
04:32:55: ISAKMP: life type in seconds
04:32:55: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
04:32:55: ISAKMP (0:13): atts are acceptable. Next payload is 3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 157 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 123 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v2
04:32:55: ISAKMP (0:13): processing KE payload. message ID = 0
04:32:55: ISAKMP (0:13): processing NONCE payload. message ID = 0
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID is DPD
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 175 mismatch
04:32:55: ISAKMP (0:13): vendor ID is XAUTH
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): claimed IOS but failed authentication
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID is Unity
04:32:55: ISAKMP (0:13): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
04:32:55: ISAKMP (0:13): Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT

04:32:55: ISAKMP cookie gen for src 11.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 7AE6E1DF
04:32:55: ISAKMP: isadb_post_process_list: crawler: 4 AA 31 (6482B354)
04:32:55: crawler my_cookie AA8F7B41 F7ACF384
04:32:55: crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP: got callback 1
04:32:55: ISAKMP (0:13): SKEYID state generated
04:32:55: ISAKMP: Unity/DPD ID: vendor_id_payload:
next: 0xD, reserved: 0x0, len 0x14
04:32:55: ISAKMP: Unity/DPD ID payload dump:
63E66D70: 0D000014 ....
63E66D80: 12F5F28C 457168A9 702D9FE2 74CC0100 .ur.Eqh)p-.btL..
63E66D90: 00 .
04:32:55: ISAKMP: Unity/DPD ID: vendor_id_payload:
next: 0xD, reserved: 0x0, len 0x14
04:32:55: ISAKMP: Unity/DPD ID payload dump:
63E66D90: 0D000014 AFCAD713 68A1F1C9 6B8696FC ....JW.h!qIk..|
63E66DA0: 77570100 00 wW...
04:32:55: ISAKMP (0:13): constructed NAT-T vendor-03 ID
04:32:55: ISAKMP (0:13): SA is doing pre-shared key authentication plus XAUTH using id
type ID_IPV4_ADDR

```

```

04:32:55: ISAKMP (13): ID payload
      next-payload : 10
      type          : 1
      addr          : 172.16.1.1
      protocol      : 17
      port          : 0
      length        : 8
04:32:55: ISAKMP (13): Total payload length: 12
04:32:55: ISAKMP (0:13): constructed HIS NAT-D
04:32:55: ISAKMP (0:13): constructed MINE NAT-D
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
AG_INIT_EXCH
04:32:55: ISAKMP (0:13): Input = IKE_MSG_FROM_AAA, PRESHARED_KEY_REPLY
04:32:55: ISAKMP (0:13): Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B D99DA70D
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 9C69F917
04:32:55: ISAKMP:      isadb_post_process_list: crawler: 5 21FF 1 (6482B354)
04:32:55:      crawler my_cookie AA8F7B41 F7ACF384
04:32:55:      crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B 00583224
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 C1B006EE
04:32:55: ISAKMP:      isadb_post_process_list: crawler: 5 21FF 1 (6482B354)
04:32:55:      crawler my_cookie AA8F7B41 F7ACF384
04:32:55:      crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
AG_INIT_EXCH
04:32:55: ISAKMP: hash from 7003A34 for 132 bytes
04:32:55: ISAKMP: Packet hash:
64218CC0:      D1202D99 2BB49D38      Q -.+4.8
64218CD0: B8FBB1BE 7CDC67D7 4E26126C 63      8{1>|\gWN&.lc
04:32:55: ISAKMP (0:13): processing HASH payload. message ID = 0
04:32:55: ISAKMP:received payload type 17
04:32:55: ISAKMP (0:13): Detected NAT-D payload
04:32:55: ISAKMP (0:13): recalc my hash for NAT-D
04:32:55: ISAKMP (0:13): NAT match MINE hash
04:32:55: ISAKMP:received payload type 17
04:32:55: ISAKMP (0:13): Detected NAT-D payload
04:32:55: ISAKMP (0:13): recalc his hash for NAT-D
04:32:55: ISAKMP (0:13): NAT match HIS hash
04:32:55: ISAKMP (0:13): processing NOTIFY INITIAL_CONTACT protocol 1
      spi 0, message ID = 0, sa = 6482B354
04:32:55: ISAKMP (0:13): Process initial contact,
bring down existing phase 1 and 2 SA's with local 172.16.1.1 remote 10.1.1.1 remote port
500
04:32:55: ISAKMP (0:13): returning IP addr to the address pool
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 05D315C5
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B 041A85A6
04:32:55: ISAKMP (0:13): SA has been authenticated with 10.1.1.1
04:32:55: ISAKMP: Trying to insert a peer 172.16.1.1/10.1.1.1/500/, and inserted
successfully.
04:32:55: ISAKMP: set new node -803402627 to CONF_XAUTH
04:32:55: IPSEC(key_engine): got a queue event...
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) QM_IDLE
04:32:55: ISAKMP (0:13): purging node -803402627
04:32:55: ISAKMP: Sending phase 1 responder lifetime 86400

04:32:55: ISAKMP (0:13): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH

```

```

04:32:55: ISAKMP (0:13): Old State = IKE_R_AM2  New State = IKE_P1_COMPLETE

04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.168.1.1
04:32:55: ISAKMP cookie AA8F7B41 25EEF256
04:32:55: ISAKMP:      isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:32:55:      crawler my_cookie AA8F7B41 F7ACF384
04:32:55:      crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP (0:13): Need XAUTH
04:32:55: ISAKMP (0:13): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
04:32:55: ISAKMP (0:13): Old State = IKE_P1_COMPLETE  New State =
IKE_XAUTH_AAA_START_LOGIN_AWAIT

04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 2CCFA491
04:32:55: ISAKMP:      isadb_post_process_list: crawler: B 27FF 12 (6482B354)
04:32:55:      crawler my_cookie AA8F7B41 F7ACF384
04:32:55:      crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP: got callback 1
04:32:55: ISAKMP: set new node -1447732198 to CONF_XAUTH
04:32:55: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
04:32:55: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
04:32:55: ISAKMP (0:13): initiating peer config to 10.1.1.1. ID = -1447732198
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
CONF_XAUTH
04:32:55: ISAKMP (0:13): Input = IKE_MSG_FROM_AAA, IKE_AAA_START_LOGIN
04:32:55: ISAKMP (0:13): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT  New State =
IKE_XAUTH_REQ_SENT

04:33:00: ISAKMP (0:13): retransmitting phase 2 CONF_XAUTH -1447732198 ...
04:33:00: ISAKMP (0:13): incrementing error counter on sa: retransmit phase 2
04:33:00: ISAKMP (0:13): incrementing error counter on sa: retransmit phase 2
04:33:00: ISAKMP (0:13): retransmitting phase 2 -1447732198 CONF_XAUTH
04:33:00: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
CONF_XAUTH

04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 124D4618
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 B0C91917
04:33:03: ISAKMP:      isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:      crawler my_cookie AA8F7B41 F7ACF384
04:33:03:      crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 0E294692
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 091A7695
04:33:03: ISAKMP:      isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:      crawler my_cookie AA8F7B41 F7ACF384
04:33:03:      crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
CONF_XAUTH
04:33:03: ISAKMP: hash from 7292D74 for 92 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:      84A1AF24 5D92B116      .!/$}.1.
64218CD0: FC2C6252 A472C5F8 152AC860 63      |,bR$rEx.*H`c
04:33:03: ISAKMP (0:13): processing transaction payload from 11.1.1.1. message ID =
-1447732198
04:33:03: ISAKMP: Config payload REPLY
04:33:03: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
04:33:03: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
04:33:03: ISAKMP (0:13): deleting node -1447732198 error FALSE reason "done with xauth
request/reply exchange"
04:33:03: ISAKMP (0:13): Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_REQ_SENT  New State =
IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

```

```

04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 A1B3E684
04:33:03: ISAKMP:      isadb_post_process_list: crawler: B 27FF 12 (6482B354)
04:33:03:      crawler my_cookie AA8F7B41 F7ACF384
04:33:03:      crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP: got callback 1
04:33:03: ISAKMP: set new node 524716665 to CONF_XAUTH
04:33:03: ISAKMP (0:13): initiating peer config to 10.1.1.1. ID = 524716665
04:33:03: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
CONF_XAUTH
04:33:03: ISAKMP (0:13): Input = IKE_MSG_FROM_AAA, IKE_AAA_CONT_LOGIN
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT New State =
IKE_XAUTH_SET_SENT
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 5C83A09D
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 2BEBEFD4
04:33:03: ISAKMP:      isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:      crawler my_cookie AA8F7B41 F7ACF384
04:33:03:      crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B DA00A46B
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 FDD27773
04:33:03: ISAKMP:      isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:      crawler my_cookie AA8F7B41 F7ACF384
04:33:03:      crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
CONF_XAUTH
04:33:03: ISAKMP: hash from 7292A34 for 68 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:      5034B99E B8BA531F      P49.8:S.
64218CD0: 6267B8BD F3006989 DC118796 63      bg8=s.i.\...c
04:33:03: ISAKMP (0:13): processing transaction payload from 11.1.1.1. message ID =
524716665
04:33:03: ISAKMP: Config payload ACK
04:33:03: ISAKMP (0:13):      XAUTH ACK Processed
04:33:03: ISAKMP (0:13): deleting node 524716665 error FALSE reason "done with
transaction"
04:33:03: ISAKMP (0:13): Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE

04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 E0BB50E9
04:33:03: ISAKMP:      isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:      crawler my_cookie AA8F7B41 F7ACF384
04:33:03:      crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
04:33:03: ISAKMP (0:13): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 7794EF6E
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 C035AAE5
04:33:03: ISAKMP:      isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:      crawler my_cookie AA8F7B41 F7ACF384
04:33:03:      crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B F1FCC25A
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 31744F44
04:33:03: ISAKMP:      isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:      crawler my_cookie AA8F7B41 F7ACF384

```

```

04:33:03:          crawler his_cookie E46E088D F207FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
QM_IDLE
04:33:03: ISAKMP: set new node -1639992295 to QM_IDLE
04:33:03: ISAKMP: hash from 7293A74 for 100 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:          9D7DF4DF FE3A6403          .)t_~:d.
64218CD0: 3F1D1C59 C5D138CE 50289B79 07          ?..YEQ8NP(.y.
04:33:03: ISAKMP (0:13): processing transaction payload from 10.1.1.1. message ID =
-1639992295
04:33:03: ISAKMP: Config payload REQUEST
04:33:03: ISAKMP (0:13): checking request:
04:33:03: ISAKMP:      IP4_ADDRESS
04:33:03: ISAKMP:      IP4_NETMASK
04:33:03: ISAKMP:      IP4_DNS
04:33:03: ISAKMP:      IP4_DNS
04:33:03: ISAKMP:      IP4_NBNS
04:33:03: ISAKMP:      IP4_NBNS
04:33:03: ISAKMP:      SPLIT_INCLUDE
04:33:03: ISAKMP:      DEFAULT_DOMAIN
04:33:03: ISAKMP (0:13): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST
04:33:03: ISAKMP (0:13): Old State = IKE_P1_COMPLETE New State =
IKE_CONFIG_AUTHOR_AAA_AWAIT

04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 B02E0D67
04:33:03: ISAKMP:      isadb_post_process_list: crawler: C 27FF 12 (6482B354)
04:33:03:          crawler my_cookie AA8F7B41 F7ACF384
04:33:03:          crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP: got callback 1
04:33:03: ISAKMP (0:13): attributes sent in message:
04:33:03:      Address: 10.2.0.0
04:33:03: ISAKMP (0:13): allocating address 10.4.1.4
04:33:03: ISAKMP: Sending private address: 10.4.1.4
04:33:03: ISAKMP: Sending DEFAULT_DOMAIN default domain name: vpn2.com
04:33:03: ISAKMP (0:13): responding to peer config from 10.1.1.1. ID = -1639992295
04:33:03: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
CONF_ADDR
04:33:03: ISAKMP (0:13): deleting node -1639992295 error FALSE reason ""
04:33:03: ISAKMP (0:13): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR
04:33:03: ISAKMP (0:13): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State =
IKE_P1_COMPLETE

04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 881D5411
04:33:03: ISAKMP cookie gen for src 11.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 6FD82541
04:33:03: ISAKMP:      isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:          crawler my_cookie AA8F7B41 F7ACF384
04:33:03:          crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 8A94C1BE
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 F3BA766D
04:33:03: ISAKMP:      isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:          crawler my_cookie AA8F7B41 F7ACF384
04:33:03:          crawler his_cookie E46E088D F207FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
QM_IDLE
04:33:03: ISAKMP: set new node 17011691 to QM_IDLE
04:33:03: ISAKMP: hash from 70029F4 for 540 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:          AFBA30B2 55F5BC2D          /:02Uu<-
64218CD0: 3A86B1C9 00D2F5BA 77BF5589 07          :.1I.Ru:w?U..

```

```

04:33:03: ISAKMP (0:13): processing HASH payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing SA payload. message ID = 17011691
04:33:03: ISAKMP (0:13): Checking IPSec proposal 1
04:33:03: ISAKMP: transform 1, ESP_3DES
04:33:03: ISAKMP:   attributes in transform:
04:33:03: ISAKMP:     encaps is 1
04:33:03: ISAKMP:     SA life type in seconds
04:33:03: ISAKMP:     SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
04:33:03: ISAKMP:     SA life type in kilobytes
04:33:03: ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
04:33:03: ISAKMP:     authenticator is HMAC-SHA
04:33:03: ISAKMP (0:13): atts are acceptable.
04:33:03: IPSEC(validate_proposal_request): proposal part #1,
      (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
      local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
      remote_proxy= 10.4.1.4/255.255.255.255/0/0 (type=1),
      protocol= ESP, transform= esp-3des esp-sha-hmac ,
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
04:33:03: IPSEC(validate_transform_proposal): transform proposal not supported for
identity:
      {esp-3des esp-sha-hmac }
04:33:03: ISAKMP (0:13): IPSec policy invalidated proposal
04:33:03: ISAKMP (0:13): Checking IPSec proposal 2
04:33:03: ISAKMP: transform 1, ESP_3DES
04:33:03: ISAKMP:   attributes in transform:
04:33:03: ISAKMP:     encaps is 1
04:33:03: ISAKMP:     SA life type in seconds
04:33:03: ISAKMP:     SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
04:33:03: ISAKMP:     SA life type in kilobytes
04:33:03: ISAKMP:     SA life duration (VPI) of  0x0 0x46 0x50 0x0
04:33:03: ISAKMP:     authenticator is HMAC-MD5
04:33:03: ISAKMP (0:13): atts are acceptable.
04:33:03: IPSEC(validate_proposal_request): proposal part #1,
      (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
      local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
      remote_proxy= 10.4.1.4/255.255.255.255/0/0 (type=1),
      protocol= ESP, transform= esp-3des esp-md5-hmac ,
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
04:33:03: ISAKMP (0:13): processing NONCE payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing ID payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing ID payload. message ID = 17011691
04:33:03: ISAKMP (0:13): asking for 1 spis from ipsec
04:33:03: ISAKMP (0:13): Node 17011691, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
04:33:03: ISAKMP (0:13): Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
04:33:03: IPSEC(key_engine): got a queue event...
04:33:03: IPSEC(spi_response): getting spi 2749516541 for SA
      from 172.18.1.1      to 10.1.1.1      for prot 3
04:33:03: ISAKMP: received ke message (2/1)
04:33:04: ISAKMP (13): ID payload
      next-payload : 5
      type          : 1
      addr          : 10.4.1.4
      protocol      : 0
      port         : 0
04:33:04: ISAKMP (13): ID payload
      next-payload : 11
      type          : 4
      addr          : 0.0.0.0

```

```

        protocol      : 0
        port           : 0
04:33:04: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) QM_IDLE
04:33:04: ISAKMP (0:13): Node 17011691, Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY
04:33:04: ISAKMP (0:13): Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
04:33:04: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:04: ISAKMP cookie 3123100B 93DE46D2
04:33:04: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:04: ISAKMP cookie AA8F7B41 088A0A16
04:33:04: ISAKMP:      isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:04:      crawler my_cookie AA8F7B41 F7ACF384
04:33:04:      crawler his_cookie E46E088D F227FE4D
04:33:04: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:04: ISAKMP cookie 3123100B A8F23F73
04:33:04: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:04: ISAKMP cookie AA8F7B41 93D8D879
04:33:04: ISAKMP:      isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:04:      crawler my_cookie AA8F7B41 F7ACF384
04:33:04:      crawler his_cookie E46E088D F227FE4D
04:33:04: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
QM_IDLE
04:33:04: ISAKMP: hash from 7290DB4 for 60 bytes
04:33:04: ISAKMP: Packet hash:
64218CC0:      4BB45A92 7181A2F8      K4Z.q."x
64218CD0: 73CC12F8 091875C0 054F77CD 63      sL.x..u@.OwMc
04:33:04: ISAKMP: Locking peer struct 0x640BBB18, IPSEC refcount 1 for for stuff_ke
04:33:04: ISAKMP (0:13): Creating IPsec SAs
04:33:04:      inbound SA from 10.1.1.1 to 172.18.1.1 (f/i) 0/ 2
      (proxy 10.4.1.4 to 0.0.0.0)
04:33:04:      has spi 0xA3E24AFD and conn_id 5127 and flags 2
04:33:04:      lifetime of 2147483 seconds
04:33:04:      lifetime of 4608000 kilobytes
04:33:04:      has client flags 0x0
04:33:04:      outbound SA from 172.18.1.1      to 10.1.1.1      (f/i) 0/ 2 (proxy
0.0.0.0      to 10.4.1.4      )
04:33:04:      has spi 1343294712 and conn_id 5128 and flags A
04:33:04:      lifetime of 2147483 seconds
04:33:04:      lifetime of 4608000 kilobytes
04:33:04:      has client flags 0x0
04:33:04: ISAKMP (0:13): deleting node 17011691 error FALSE reason "quick mode done
(await)"
04:33:04: ISAKMP (0:13): Node 17011691, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
04:33:04: ISAKMP (0:13): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
04:33:04: IPSEC(key_engine): got a queue event...
04:33:04: IPSEC(initialize_sas): ,
      (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
      local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
      remote_proxy= 10.4.1.4/0.0.0.0/0/0 (type=1),
      protocol= ESP, transform= esp-3des esp-md5-hmac ,
      lifedur= 2147483s and 4608000kb,
      spi= 0xA3E24AFD(2749516541), conn_id= 5127, keysize= 0, flags= 0x2
04:33:04: IPSEC(initialize_sas): ,
      (key eng. msg.) OUTBOUND local= 172.18.1.1, remote= 10.1.1.1,
      local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
      remote_proxy= 10.4.1.4/0.0.0.0/0/0 (type=1),
      protocol= ESP, transform= esp-3des esp-md5-hmac ,
      lifedur= 2147483s and 4608000kb,
      spi= 0x50110CF8(1343294712), conn_id= 5128, keysize= 0, flags= 0xA
04:33:04: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:04: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
04:33:04: IPSEC(rte_mgr): VPN Route Added 10.4.1.4 255.255.255.255 via 10.1.1.1 in vpn2
04:33:04: IPSEC(add mtree): src 0.0.0.0, dest 10.4.1.4, dest_port 0

04:33:04: IPSEC(create_sa): sa created,

```

```
(sa) sa_dest= 172.18.1.1, sa_prot= 50,
    sa_spi= 0xA3E24AFD(2749516541),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 5127
04:33:04: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.1.1, sa_prot= 50,
    sa_spi= 0x50110CF8(1343294712),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 5128
04:33:53: ISAKMP (0:13): purging node -1639992295
04:33:54: ISAKMP (0:13): purging node 17011691
```

Configuration Examples for VRF-Aware IPSec

The following examples show how to configure VRF-Aware IPSec:

- [Static IPSec-to-MPLS VPN Example, page 22](#)
- [IPSec-to-MPLS VPN Using RSA Encryption Example, page 24](#)
- [IPSec-to-MPLS VPN with RSA Signatures Example, page 25](#)
- [Upgrade from Previous Versions of the Cisco Network-Based IPSec VPN Solution, page 28](#)

Static IPSec-to-MPLS VPN Example

The following sample shows a static configuration that maps IPSec tunnels to MPLS VPNs. The configurations map IPSec tunnels to MPLS VPNs “VPN1” and “VPN2.” Both of the IPSec tunnels terminate on a single public-facing interface.

IPSec PE Configuration

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
ip vrf vpn2
 rd 101:1
 route-target export 101:1
 route-target import 101:1
!
crypto keyring vpn1
 pre-shared-key address 172.16.1.1 key vpn1
crypto keyring vpn2
 pre-shared-key address 10.1.1.1 key vpn2
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
!
crypto isakmp profile vpn2
 vrf vpn2
 keyring vpn2
 match identity address 10.1.1.1 255.255.255.255
!
```



```

crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
!
crypto map crypmap 1 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set vpn1
  set isakmp-profile vpn1
  match address 101
crypto map crypmap 3 ipsec-isakmp
  set peer 10.1.1.1
  set transform-set vpn2
  set isakmp-profile vpn2
  match address 102
!
interface Ethernet1/1
  ip address 172.17.1.1 255.255.0.0
  tag-switching ip
!
interface Ethernet1/2
  ip address 172.18.1.1 255.255.255.0
  crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.168.1.2
ip route 10.1.1.1 255.255.255.255 172.18.1.2
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
ip route vrf vpn2 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 102 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255

```

IPSec Customer Provided Edge (CPE) Configuration for VPN1

```

crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key vpn1 address 172.18.1.1
!
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
  set peer 172.18.1.1
  set transform-set vpn1
  match address 101
!
interface FastEthernet1/0
  ip address 172.16.1.1 255.255.255.0
  crypto map vpn1
!
interface FastEthernet1/1
  ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!

```

IPSec CPE Configuration for VPN2

```

crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp key vpn2 address 172.18.1.1

```

```

!
!
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
!
crypto map vpn2 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn2
 match address 101
!
interface FastEthernet0
 ip address 10.1.1.1 255.255.255.0
 crypto map vpn2
!
interface FastEthernet1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255

```

IPSec-to-MPLS VPN Using RSA Encryption Example

The following example shows an IPSec-to-MPLS configuration using RSA encryption:

PE Router Configuration

```

ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
crypto isakmp policy 10
 authentication rsa-encr
!
crypto keyring vpn1
 rsa-publickey address 172.16.1.1 encryption
  key-string
    305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DBF381 00DDECC8
    DC4AA490 40320C52 9912D876 EB36717C 63DCA95C 7E5EC02A 84F276CE 292B42D7
    D664F324 3726F4E0 39D33093 ECB81B95 482511A5 F064C4B3 D5020301 0001
  quit
!
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
!
interface Ethernet1/1
 ip address 172.17.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.18.1.2

```

```
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
```

IPSec CPE Configuration for VPN1

```
crypto isakmp policy 10
 authentication rsa-encr
!
crypto key pubkey-chain rsa
 addressed-key 172.18.1.1 encryption
 key-string
 3082011B 300D0609 2A864886 F70D0101 01050003 82010800 30820103 0281FB00
 C90CC78A 6002BDBA 24683396 B7D7877C 16D08C47 E00C3C10 63CF13BC 4E09EA23
 92EB8A48 4113F5A4 8796C8BE AD7E2DC1 3B0742B6 7118CE7C 1B0E21D1 AA9724A4
 4D74FCEA 562FF225 A2B11F18 E53C4415 61C3B741 3A06E75D B4F9102D 6163EE40
 16C68FD7 6532F660 97B59118 9C8DE3E5 4E2F2925 BBB87FCB 95223D4E A5E362DB
 215CB35C 260080805 17BBE1EF C3050E13 031F3D5B 5C22D16C FC8B1EC5 074F07A5
 D050EC80 7890D9C5 EC20D6F0 173FE2BA 89F5B5F9 2EADC9A6 D461921E 3D5B60016
 ABB8B6B9 E2124A21 93F0E4AE B487461B E7F1F1C4 032A0B0E 80DC3E15 CB268EC9
 5D76B9BD 3C78CB75 CE9F68C6 484D6573 CBC3EB59 4B5F3999 8F9D0203 010001
 quit
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn1
 match address 101
!
interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 crypto map vpn1
!
interface FastEthernet1/1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
```

IPSec-to-MPLS VPN with RSA Signatures Example

The following shows an IPSec-to-MPLS VPN configuration using RSA signatures:

PE Router Configuration

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
crypto ca trustpoint bombo
 enrollment url http://172.31.68.59:80
 crl optional
!
crypto ca certificate chain bombo
 certificate 03C0
 308203BF 308202A7 A0030201 02020203 C0300D06 092A8648 86F70D01 01050500
 . . .
 quit
 certificate ca 01
 30820379 30820261 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
```

```

. . .
quit
!
crypto isakmp profile vpn1
  vrf vpn1
  ca trust-point bombo
  match identity address 172.16.1.1 255.255.255.255
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto map crypmap 1 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set vpn1
  set isakmp-profile vpn1
  match address 101
!
interface Ethernet1/1
  ip address 172.31.1.1 255.255.0.0
  tag-switching ip
!
interface Ethernet1/2
  ip address 172.18.1.1 255.255.255.0
  crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.18.1.2
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
!

```

IPSec CPE Configuration for VPN1

```

crypto ca trustpoint bombo
  enrollment url http://172.31.68.59:80
  crl optional
!
crypto ca certificate chain bombo
  certificate 03BF
    308203BD 308202A5 A0030201 02020203 BF300D06 092A8648 86F70D01 01050500
    . . .
  quit
  certificate ca 01
    30820379 30820261 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
    . . .
  quit
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
  set peer 172.18.1.1
  set transform-set vpn1
  match address 101
!
interface FastEthernet1/0
  ip address 172.16.1.1 255.255.255.0
  crypto map vpn1
!
interface FastEthernet1/1
  ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!

```

IPSec Remote Access-to-MPLS VPN Example

The following shows an IPSec remote access-to-MPLS VPN configuration. The configuration maps IPSec tunnels to MPLS VPNs. The IPSec tunnels terminate on a single public-facing interface.

PE Router Configuration

```

aaa new-model
!
aaa group server radius vpn1
  server-private 10.1.1.1 auth-port 1645 acct-port 1646 timeout 5 retransmit 3 key vpn1
!
aaa group server radius vpn2
  server-private 10.1.1.1 auth-port 1645 acct-port 1646 timeout 5 retransmit 3 key vpn2
!
aaa authorization network aaa-list group radius
!
ip vrf vpn1
  rd 100:1
  route-target export 100:1
  route-target import 100:1
!
ip vrf vpn2
  rd 101:1
  route-target export 101:1
  route-target import 101:1
!
crypto isakmp profile vpn1-ra
  vrf vpn1
  match identity group vpn1-ra
  client authentication list vpn1
  isakmp authorization list aaa-list
  client configuration address initiate
  client configuration address respond
crypto isakmp profile vpn2-ra
  vrf vpn2
  match identity group vpn2-ra
  client authentication list vpn2
  isakmp authorization list aaa-list
  client configuration address initiate
  client configuration address respond
!
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
!
crypto dynamic-map vpn1 1
  set transform-set vpn1
  set isakmp-profile vpn1-ra
  reverse-route
!
crypto dynamic-map vpn2 1
  set transform-set vpn2
  set isakmp-profile vpn2-ra
  reverse-route
!
!
crypto map ra 1 ipsec-isakmp dynamic vpn1
crypto map ra 2 ipsec-isakmp dynamic vpn2
!
interface Ethernet1/1
  ip address 172.17.1.1 255.255.0.0
  tag-switching ip

```

```

!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map ra
!
ip local pool vpn1-ra 10.4.1.1 10.4.1.254 group vpn1-ra
ip local pool vpn2-ra 10.4.1.1 10.4.1.254 group vpn2-ra
!

```

Upgrade from Previous Versions of the Cisco Network-Based IPSec VPN Solution

The VRF-Aware IPSec feature in the Cisco network-based IPSec VPN solution release 1.5 requires that you change your existing configurations.

The sample configurations that follow indicate the changes you must make to your existing configurations. These samples include the following:

- [Site-to-Site Configuration Upgrade, page 28](#)
- [Remote Access Configuration Upgrade, page 29](#)
- [Combination Site-to-Site and Remote Access Configuration Upgrade, page 31](#)

Site-to-Site Configuration Upgrade

The following configurations show the changes that are necessary for a site-to-site configuration upgrade from a previous version of the network-based IPSec VPN solution to the Cisco network-based IPSec VPN solution release 1.5:

Previous Version Site-to-Site Configuration

```

crypto isakmp key VPN1 address 172.21.25.74
crypto isakmp key VPN2 address 172.21.21.74
!
crypto ipsec transform-set VPN1 esp-des esp-sha-hmac
crypto ipsec transform-set VPN2 esp-3des esp-sha-hmac
!
crypto map VPN1 10 ipsec-isakmp
 set peer 172.21.25.74
 set transform-set VPN1
 match address 101
!
crypto map VPN2 10 ipsec-isakmp
 set peer 172.21.21.74
 set transform-set VPN2
 match address 102
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2

```

New Version Site-to-Site Configuration

The following is an upgraded version of the same site-to-site configuration to the Cisco network-based IPSec VPN solution release 1.5 solution:



Note

You must change to keyrings. The VRF-Aware IPSec feature requires that keys be associated with a VRF if the IKE local endpoint is in the VRF.

```
crypto keyring VPN1-KEYS vrf VPN1
pre-shared-key address 172.21.25.74 key VPN1
!
crypto keyring VPN2-KEYS vrf VPN2
pre-shared-key address 172.21.21.74 key VPN2
!
crypto ipsec transform-set VPN1 esp-des esp-sha-hmac
crypto ipsec transform-set VPN2 esp-3des esp-sha-hmac
!
crypto map VPN1 10 ipsec-isakmp
set peer 172.21.25.74
set transform-set VPN1
match address 101
!
crypto map VPN2 10 ipsec-isakmp
set peer 172.21.21.74
set transform-set VPN2
match address 102
!
interface FastEthernet0/0.1
encapsulation dot1Q 1 native
ip vrf forwarding VPN1
ip address 172.21.25.73 255.255.255.0
crypto map VPN1
!
interface FastEthernet0/0.2
encapsulation dot1Q 2 native
ip vrf forwarding VPN2
ip address 172.21.21.74 255.255.255.0
crypto map VPN2
```

Remote Access Configuration Upgrade

The following configurations show the changes that are necessary for a remote access configuration upgrade from a previous version of the network-based IPSec VPN solution to the Cisco network-based IPSec VPN solution release 1.5:

Previous Version Remote Access Configuration

```
crypto isakmp client configuration group VPN1-RA-GROUP
key VPN1-RA
pool VPN1-RA
!
crypto isakmp client configuration group VPN2-RA-GROUP
key VPN2-RA
pool VPN2-RA
!
crypto ipsec transform-set VPN1-RA esp-3des esp-sha-hmac
crypto ipsec transform-set VPN2-RA esp-3des esp-md5-hmac
!
crypto dynamic-map VPN1-RA 1
```

```

    set transform-set VPN1-RA
reverse-route
!
crypto dynamic-map VPN2-RA 1
set transform-set VPN2-RA
reverse-route
!
!
crypto map VPN1 client authentication list VPN1-RA-LIST
crypto map VPN1 isakmp authorization list VPN1-RA-LIST
crypto map VPN1 client configuration address initiate
crypto map VPN1 client configuration address respond
crypto map VPN1 10 ipsec-isakmp dynamic VPN1-RA
!
crypto map VPN2 client authentication list VPN2-RA-LIST
crypto map VPN2 isakmp authorization list VPN2-RA-LIST
crypto map VPN2 client configuration address initiate
crypto map VPN2 client configuration address respond
crypto map VPN2 10 ipsec-isakmp dynamic VPN2-RA
!
interface FastEthernet0/0.1
encapsulation dot1Q 1 native
ip vrf forwarding VPN1
ip address 172.21.25.73 255.255.255.0
crypto map VPN1
!
interface FastEthernet0/0.2
encapsulation dot1Q 2 native
ip vrf forwarding VPN2
ip address 172.21.21.74 255.255.255.0
crypto map VPN2

```

New Version Remote Access Configuration

In the following instance, there is no upgrade; it is recommended that you change to the following configuration:

```

crypto isakmp client configuration group VPN1-RA-GROUP
key VPN1-RA
pool VPN1-RA
!
crypto isakmp client configuration group VPN2-RA-GROUP
key VPN2-RA
pool VPN2-RA
!
crypto isakmp profile VPN1-RA
match identity group VPN1-RA-GROUP
client authentication list VPN1-RA-LIST
isakmp authorization list VPN1-RA-LIST
client configuration address initiate
client configuration address respond
!
crypto isakmp profile VPN2-RA
match identity group VPN2-RA-GROUP
client authentication list VPN2-RA-LIST
isakmp authorization list VPN2-RA-LIST
client configuration address initiate
client configuration address respond
!
crypto ipsec transform-set VPN1-RA esp-3des esp-sha-hmac
crypto ipsec transform-set VPN2-RA esp-3des esp-md5-hmac
!
crypto dynamic-map VPN1-RA 1

```



```

set transform-set VPN1-RA
set isakmp-profile VPN1-RA
reverse-route
!
crypto dynamic-map VPN2-RA 1
set transform-set VPN2-RA
set isakmp-profile VPN2-RA
reverse-route
!
crypto map VPN1 10 ipsec-isakmp dynamic VPN1-RA
!
crypto map VPN2 10 ipsec-isakmp dynamic VPN2-RA
!
interface FastEthernet0/0.1
encapsulation dot1Q 1 native
ip vrf forwarding VPN1
ip address 172.21.25.73 255.255.255.0
crypto map VPN1
!
interface FastEthernet0/0.2
encapsulation dot1Q 2 native
ip vrf forwarding VPN2
ip address 172.21.21.74 255.255.255.0
crypto map VPN2

```

Combination Site-to-Site and Remote Access Configuration Upgrade

The following configurations show the changes that are necessary for a site-to-site and remote access configuration upgrade from a previous version of the network-based IPSec VPN solution to the Cisco network-based IPSec VPN solution release 1.5:

Previous Version Site-to-Site and Remote Access Configuration

```

crypto isakmp key VPN1 address 172.21.25.74 no-xauth
crypto isakmp key VPN2 address 172.21.21.74 no-xauth
!
crypto isakmp client configuration group VPN1-RA-GROUP
key VPN1-RA
pool VPN1-RA
!
crypto isakmp client configuration group VPN2-RA-GROUP
key VPN2-RA
pool VPN2-RA
!
crypto ipsec transform-set VPN1 esp-des esp-sha-hmac
crypto ipsec transform-set VPN2 esp-3des esp-sha-hmac
!
crypto ipsec transform-set VPN1-RA esp-3des esp-sha-hmac
crypto ipsec transform-set VPN2-RA esp-3des esp-md5-hmac
!
crypto dynamic-map VPN1-RA 1
set transform-set VPN1-RA
reverse-route
!
crypto dynamic-map VPN2-RA 1
set transform-set VPN2-RA
reverse-route
!
crypto map VPN1 client authentication list VPN1-RA-LIST
crypto map VPN1 isakmp authorization list VPN1-RA-LIST
crypto map VPN1 client configuration address initiate

```

```

crypto map VPN1 client configuration address respond
crypto map VPN1 10 ipsec-isakmp
set peer 172.21.25.74
set transform-set VPN1
match address 101
crypto map VPN1 20 ipsec-isakmp dynamic VPN1-RA
!
crypto map VPN2 client authentication list VPN2-RA-LIST
crypto map VPN2 isakmp authorization list VPN2-RA-LIST
crypto map VPN2 client configuration address initiate
crypto map VPN2 client configuration address respond
crypto map VPN2 10 ipsec-isakmp
set peer 172.21.21.74
set transform-set VPN2
match address 102
crypto map VPN2 20 ipsec-isakmp dynamic VPN2-RA
!
interface FastEthernet0/0.1
encapsulation dot1Q 1 native
ip vrf forwarding VPN1
ip address 172.21.25.73 255.255.255.0
crypto map VPN1
!
interface FastEthernet0/0.2
encapsulation dot1Q 2 native
ip vrf forwarding VPN2
ip address 172.21.21.74 255.255.255.0
crypto map VPN2

```

New Version Site-to-Site and Remote Access Configuration

You must upgrade to this configuration:



Note

For site-to-site configurations that do not require XAUTH, configure an ISAKMP profile without XAUTH configuration. For remote access configurations that require XAUTH, configure an ISAKMP profile with XAUTH.

```

crypto keyring VPN1-KEYS vrf VPN1
pre-shared-key address 172.21.25.74 key VPN1
!
crypto keyring VPN2-KEYS vrf VPN2
pre-shared-key address 172.21.21.74 key VPN2
!
crypto isakmp client configuration group VPN1-RA-GROUP
key VPN1-RA
pool VPN1-RA
!
crypto isakmp client configuration group VPN2-RA-GROUP
key VPN2-RA
pool VPN2-RA
!
crypto isakmp profile VPN1
keyring VPN1-KEYS
match identity address 172.21.25.74 VPN1
!
crypto isakmp profile VPN2
keyring VPN2-KEYS
match identity address 172.21.21.74 VPN2
!
crypto isakmp profile VPN1-RA

```

```
match identity group VPN1-RA-GROUP
client authentication list VPN1-RA-LIST
isakmp authorization list VPN1-RA-LIST
client configuration address initiate
client configuration address respond
!
crypto isakmp profile VPN2-RA
match identity group VPN2-RA-GROUP
client authentication list VPN2-RA-LIST
isakmp authorization list VPN2-RA-LIST
client configuration address initiate
client configuration address respond
!
crypto ipsec transform-set VPN1 esp-des esp-sha-hmac
crypto ipsec transform-set VPN2 esp-3des esp-sha-hmac
!
crypto ipsec transform-set VPN1-RA esp-3des esp-sha-hmac
crypto ipsec transform-set VPN2-RA esp-3des esp-md5-hmac
!
crypto dynamic-map VPN1-RA 1
set transform-set VPN1-RA
set isakmp-profile VPN1-RA
reverse-route
!
crypto dynamic-map VPN2-RA 1
set transform-set VPN2-RA
set isakmp-profile VPN2-RA
reverse-route
!
crypto map VPN1 10 ipsec-isakmp
set peer 172.21.25.74
set transform-set VPN1
set isakmp-profile VPN1
match address 101
crypto map VPN1 20 ipsec-isakmp dynamic VPN1-RA
!
crypto map VPN2 10 ipsec-isakmp
set peer 172.21.21.74
set transform-set VPN2
set isakmp-profile VPN2
match address 102
crypto map VPN2 20 ipsec-isakmp dynamic VPN2-RA
!
interface FastEthernet0/0.1
encapsulation dot1Q 1 native
ip vrf forwarding VPN1
ip address 172.21.25.73 255.255.255.0
crypto map VPN1
!
interface FastEthernet0/0.2
encapsulation dot1Q 2 native
ip vrf forwarding VPN2
ip address 172.21.21.74 255.255.255.0
crypto map VPN2
```

Additional References

For additional information related to VRF-Aware IPSec, refer to the following references:

Related Documents

Related Topic	Document Title
IPSec configuration tasks	The chapter “ Configuring Security for VPNs with IPSec ” in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
IPSec commands	Cisco IOS Security Command Reference
IKE Phase 1 and Phase 2, aggressive mode, and main mode	The chapter “ Configuring Internet Key Exchange for IPSec VPNs ” in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
IKE dead peer detection	Easy VPN Server

Standards

Standards ¹	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

1. Not all supported standards are listed.

MIBs

MIBs ¹	MIBs Link
<ul style="list-style-type: none"> No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. 	<p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs ¹	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module:

New Commands

- **address**
- **ca trust-point**
- **client authentication list**
- **client configuration address**
- **crypto isakmp profile**
- **crypto keyring**
- **crypto map isakmp-profile**
- **initiate-mode**
- **isakmp authorization list**
- **keepalive (isakmp profile)**

- **keyring**
- **key-string**
- **match identity**
- **no crypto xauth**
- **pre-shared-key**
- **quit**
- **rsa-pubkey**
- **self-identity**
- **serial-number**
- **set isakmp-profile**
- **show crypto isakmp key**
- **show crypto isakmp profile**
- **vrf**

Modified Commands

- **clear crypto sa**
- **crypto isakmp peer**
- **crypto map isakmp-profile**
- **show crypto dynamic-map**
- **show crypto ipsec sa**
- **show crypto isakmp sa**
- **show crypto map (IPSec)**

For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Glossary

CA—certification authority. CA is an entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

CLI—command-line-interface. CLI is an interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.

client—Corresponding IPSec IOS peer of the UUT in the Multi Protocol Label Switching (MPLS) network.

dead peer—IKE peer that is no longer reachable.

DN—Distinguished Name. A DN is the global, authoritative name of an entry in the Open System Interconnection (OSI Directory [X.500]).

FQDN—fully qualified domain name. A FQDN is the full name of a system rather than just its host name. For example, aldebaran is a host name, and aldebaran.interop.com is an FQDN.

FR—Frame Relay. FR is an industry-standard, switch-data-link-layer protocol that handles multiple virtual circuits using high-level data link (HDLC) encapsulation between connected devices. Frame Relay is more efficient than X.25, the protocol for which it generally is considered a replacement.

FVRF—Front Door Virtual Routing and Forwarding (VRF) repository. FVRF is the VRF used to route the encrypted packets to the peer.

IDB—Interface descriptor block. An IDB subblock is an area of memory that is private to an application. This area stores private information and states variables that an application wants to associate with an IDB or an interface. The application uses the IDB to register a pointer to its subblock, not to the contents of the subblock itself.

IKE—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router, firewall, and host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service.

IKE keepalive—Bidirectional mechanism for determining the liveliness of an IKE peer.

IPSec—Security protocol for IP.

IVRF—Inside Virtual Routing and Forwarding. IVRF is the VRF of the plaintext packets.

MPLS—Multiprotocol Label Switching. MPLS is a switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

RSA—Rivest, Shamir, and Adelman are the inventors of the RSA technique. The RSA technique is a public-key cryptographic system that can be used for encryption and authentication.

SA—Security Association. SA is an instance of security policy and keying material applied to a data flow.

VPN—Virtual Private Network. A VPN enables IP traffic to travel securely over a public TCP or IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

VRF—Virtual Route Forwarding. VRF is A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

XAUTH—Extended authentication. XAUTH is an optional exchange between IKE Phase 1 and IKE Phase 2, in which the router demands additional authentication information in an attempt to authenticate the actual user (as opposed to authenticating the peer).

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2009 Cisco Systems, Inc. All rights reserved.



IKE: Initiate Aggressive Mode

Feature History

Release	Modification
12.2(8)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This document describes the IKE: Initiate Aggressive Mode feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 7](#)

Feature Overview

The IKE: Initiate Aggressive Mode feature allows you to configure Internet Key Exchange (IKE) preshared keys as RADIUS tunnel attributes for IP Security (IPSec) peers. Thus, you can scale your IKE preshared keys in a hub-and-spoke topology.

Although IKE preshared keys are simple to understand and easy to deploy, they do not scale well with an increasing number of users and are therefore prone to security threats. Instead of keeping your preshared keys on the hub router, this feature allows you to scale your preshared keys by storing and retrieving them from an authentication, authorization, and accounting (AAA) server. The preshared keys are stored in the AAA server as Internet Engineering Task Force (IETF) RADIUS tunnel attributes and are retrieved when a user tries to “speak” to the hub router. The hub router retrieves the preshared key



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

from the AAA server and the spokes (the users) initiate aggressive mode to the hub by using the preshared key that is specified in the Internet Security Association Key Management Policy (ISAKMP) peer policy as a RADIUS tunnel attribute.

RADIUS Tunnel Attributes

To initiate an IKE aggressive mode negotiation, the Tunnel-Client-Endpoint (66) and Tunnel-Password (69) attributes must be configured in the ISAKMP peer policy. The Tunnel-Client-Endpoint attribute will be communicated to the server by encoding it in the appropriate IKE identity payload; the Tunnel-Password attribute will be used as the IKE preshared key for the aggressive mode negotiation.

Benefits

The IKE: Initiate Aggressive Mode feature allows you to specify RADIUS tunnel attributes for an IPSec peer and to initiate an IKE aggressive mode negotiation with the tunnel attributes. This feature is best implemented in a crypto hub-and-spoke scenario, by which the spokes initiate IKE aggressive mode negotiation with the hub by using the preshared keys that are specified as tunnel attributes and stored on the AAA server. This scenario is scalable because the preshared keys are kept at a central repository (the AAA server) and more than one hub router and one application can use the information.

Restrictions

TED Restriction

This feature is not intended to be used with a dynamic crypto map that uses Tunnel Endpoint Discovery (TED) to initiate tunnel setup. TED is useful in configuring a full mesh setup, which requires an AAA server at each site to store the preshared keys for the peers; this configuration is not practical for use with this feature.

Tunnel-Client-Endpoint ID Types

Only the following ID types can be used in this feature:

- ID_IPV4 (IPV4 address)
- ID_FQDN (fully qualified domain name, for example “foo.cisco.com”)
- ID_USER_FQDN (e-mail address)

Related Documents

- [Cisco IOS Security Command Reference](#)

Supported Platforms

This feature runs on all platforms that support IPSec and public key infrastructure (PKI).

- Cisco 800 series
- Cisco 805

- Cisco 806
- Cisco 828
- Cisco 1400 series
- Cisco 1600 series
- Cisco 1600-R series
- Cisco 1710
- Cisco 1720
- Cisco 1750
- Cisco 1751
- Cisco 2400 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco 7700 series
- Cisco MC3810
- Route Processor Module (RPM)
- Universal Route Module (URM)

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

- RFC 2409, *The Internet Key Exchange*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

Prerequisites

Before configuring the Initiate Aggressive Mode IKE feature, you must perform the following tasks:

- Configure AAA
- Configure an IPSec Transform
- Configure a Static Crypto Map
- Configure an ISAKMP Policy
- Configure a Dynamic Crypto Map

For information on completing these tasks, refer to the chapters “Configuring Authentication,” “Configuring IPSec Network Security,” and “Configuring Internet Key Exchange Security Protocol” in the *Cisco IOS Security Configuration Guide*, Release 12.2.

Configuration Tasks

See the following sections for configuration tasks for the IKE: Initiate Aggressive Mode feature. Each task in the list is identified as either required or optional.

- [Configuring RADIUS Tunnel Attributes](#) (required)
- [Verifying RADIUS Tunnel Attribute Configurations](#) (optional)

Configuring RADIUS Tunnel Attributes

To configure the Tunnel-Client-Endpoint and Tunnel-Password attributes within the ISAKMP peer configuration, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto map <i>map-name</i> isakmp authorization list <i>list-name</i>	Enables IKE querying of AAA for tunnel attributes in aggressive mode.
Step 2	Router(config)# crypto isakmp peer { ip-address <i>ip-address</i> fqdn <i>fqdn</i> }	Enables an IPSec peer for IKE querying of AAA for tunnel attributes in aggressive mode and enters ISAKMP policy configuration mode.
Step 3	Router(config-isakmp)# set aggressive-mode client-endpoint <i>client-endpoint</i>	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.
Step 4	Router(config-isakmp)# set aggressive-mode password <i>password</i>	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

Verifying RADIUS Tunnel Attribute Configurations

To verify that the Tunnel-Client-Endpoint and Tunnel-Password attributes have been configured within the ISAKMP peer policy, use the **show running-config** global configuration command.

Troubleshooting Tips

To troubleshoot the IKE: Initiate Aggressive Mode feature, use the following debug commands in EXEC mode:

Command	Purpose
Router# debug aaa authorization	Displays information on AAA authorization.
Router# debug crypto isakmp	Displays messages about IKE events.
Router# debug radius	Displays information associated with the RADIUS.

Configuration Examples

This section provides the following configuration examples:

- [Hub Configuration Example](#)
- [Spoke Configuration Example](#)
- [RADIUS User Profile Example](#)

Hub Configuration Example

The following example shows how to configure a hub for a hub-and-spoke topology that supports aggressive mode using RADIUS tunnel attributes:

```
!The AAA configurations are as follows:
aaa new-model
aaa authorization network ike group radius
aaa authentication login default group radius
```

```

!
! The Radius configurations are as follows:
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server key rad123
!
! The IKE configurations are as follows:
crypto isakmp policy 1
 authentication pre-share
!
! The IPSec configurations are as follows:
crypto ipsec transform-set trans1 esp-3des esp-sha-hmac
!
crypto dynamic-map Dmap 10
 set transform-set trans1
!
crypto map Testtag isakmp authorization list ike
crypto map Testtag 10 ipsec-isakmp dynamic Dmap
!
interface Ethernet0
 ip address 4.4.4.1 255.255.255.0
 crypto map Testtag
!
interface Ethernet1
 ip address 2.2.2.1 255.255.255.0

```

Spoke Configuration Example

The following example shows how to configure a spoke for a hub-and-spoke topology that supports aggressive mode using RADIUS tunnel attributes:

```

!The IKE configurations are as follows:
crypto isakmp policy 1
 authentication pre-share
!
! The IPSec configurations are as follows:
crypto ipsec transform-set trans1 esp-3des esp-sha-hmac
 access-list 101 permit ip 3.3.3.0 0.0.0.255 2.2.2.0 0.0.0.255
!
! Initiate aggressive mode using Radius tunnel attributes
crypto isakmp peer address 4.4.4.1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
!
crypto map Testtag 10 ipsec-isakmp
 set peer 4.4.4.1
 set transform-set trans1
 match address 101
!
interface Ethernet0
 ip address 5.5.5.1 255.255.255.0
 crypto map Testtag
!
interface Ethernet1
 ip address 3.3.3.1 255.255.255.0

```

RADIUS User Profile Example

The following is an example of a user profile on a RADIUS server that supports the Tunnel-Client-Endpoint and Tunnel-Password attributes:

```
user@cisco.com Password = "cisco", Service-Type = Outbound
Tunnel-Medium-Type = :1:IP,
Tunnel-Type = :1:ESP,
Cisco:Avpair = "ipsec:tunnel-password=cisco123",
Cisco:Avpair = "ipsec:key-exchange=ike"
```

Command Reference

The following commands are introduced or modified in the feature or features

- **crypto isakmp peer**
- **set aggressive-mode client-endpoint**
- **set aggressive-mode password**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



Security for VPNs with IPsec



Configuring Security for VPNs with IPsec

First Published: May 2, 2005

Last Updated: February 6, 2009

This module describes how to configure basic IP Security (IPsec) virtual private networks (VPNs). IPsec is a framework of open standards developed by the Internet Engineering Task Force (IETF). It provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (“peers”), such as Cisco routers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Security for VPNs with IPsec” section on page 35](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Catalyst OS, and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Configuring Security for VPNs with IPsec, page 2](#)
- [Restrictions for Configuring Security for VPNs with IPsec, page 2](#)
- [Information About Configuring Security for VPNs with IPsec, page 2](#)
- [How to Configure IPsec VPNs, page 8](#)
- [Configuration Examples for Configuring an IPsec VPN, page 32](#)
- [Additional References, page 33](#)
- [Glossary, page 37](#)
- [Feature Information for Security for VPNs with IPsec, page 35](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2005–2009 Cisco Systems, Inc. All rights reserved.

Prerequisites for Configuring Security for VPNs with IPsec

IKE Configuration

You must configure Internet Key Exchange (IKE) as described in the module “Configuring Internet Key Exchange Security for IPsec VPNs.”

Even if you decide to not use IKE, you still must disable it as described in the module “Configuring Internet Key Exchange for IPsec VPNs.”

Ensure Access Lists Are Compatible with IPsec

IKE uses UDP port 500. The IPsec Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols use protocol numbers 50 and 51. Ensure that your access lists are configured so that protocol 50, 51, and User Datagram Protocol (UDP) port 500 traffic is not blocked at interfaces used by IPsec. In some cases you might need to add a statement to your access lists to explicitly permit this traffic.

Restrictions for Configuring Security for VPNs with IPsec

Unicast IP Datagram Application Only

At this time, IPsec can be applied to unicast IP datagrams only. Because the IPsec Working Group has not yet addressed the issue of group key distribution, IPsec does not currently work with multicasts or broadcast IP datagrams.

NAT Configuration

If you use Network Address Translation (NAT), you should configure static NAT translations so that IPsec works properly. In general, NAT translation should occur before the router performs IPsec encapsulation; in other words, IPsec should be working with global addresses.

Nested IPsec Tunnels

Cisco IOS IPsec supports nested tunnels that terminate on the same router. Double encryption of locally generated IKE packets and IPsec packets is supported only when a static virtual tunnel interface (sVTI) is configured. Double encryption is supported on releases up to and including Cisco IOS Release 12.4(15)T, but it is not supported on later releases.

Information About Configuring Security for VPNs with IPsec

To configure basic IPsec VPNs, you should understand the following concepts:

- [Supported Standards, page 2](#)
- [Supported Hardware, Switching Paths, and Encapsulation, page 4](#)
- [IPsec Functionality Overview, page 6](#)
- [IPsec Traffic Nested to Multiple Peers, page 8](#)

Supported Standards

Cisco implements the following standards with this feature:

- **IPsec**—IP Security Protocol. IPsec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.



Note The term IPsec is sometimes used to describe the entire protocol of IPsec data services and IKE security protocols and is also sometimes used to describe only the data services.

IPsec is documented in a series of Internet Drafts, all available at <http://www.ietf.org/html.charters/ipsec-charter.html>.

- **IKE**—A hybrid protocol that implements Oakley and SKEME key exchanges inside the ISAKMP framework. While IKE can be used with other protocols, its initial implementation is with the IPsec protocol. IKE provides authentication of the IPsec peers, negotiates IPsec security associations, and establishes IPsec keys.

The component technologies implemented for IPsec include:

- **AES**—Advanced Encryption Standard. A cryptographic algorithm that protects sensitive, unclassified information. AES is privacy transform for IPsec and IKE and has been developed to replace the DES. AES is designed to be more secure than DES: AES offers a larger key size, while ensuring that the only known approach to decrypt a message is for an intruder to try every possible key. AES has a variable key length—the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.
- **DES**—Data Encryption Standard. An algorithm that is used to encrypt packet data. Cisco IOS implements the mandatory 56-bit DES-CBC with Explicit IV. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPsec packet. For backwards compatibility, Cisco IOS IPsec also implements the RFC 1829 version of ESP DES-CBC.

Cisco IOS also implements Triple DES (168-bit) encryption, depending on the software versions available for a specific platform. Triple DES (3DES) is a strong form of encryption that allows sensitive information to be transmitted over untrusted networks. It enables customers to utilize network layer encryption.



Note Cisco IOS images with strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to United States government export controls, and have a limited distribution. Images to be installed outside the United States require an export license. Customer orders might be denied or subject to delay due to United States government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

- **SEAL**—Software Encryption Algorithm. An alternative algorithm to software-based DES, 3DES, and AES. SEAL encryption uses a 160-bit encryption key and has a lower impact to the CPU when compared to other software-based algorithms.
- **MD5 (HMAC variant)**—MD5 (Message Digest 5) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.
- **SHA (HMAC variant)**—SHA (Secure Hash Algorithm) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.

IPsec as implemented in Cisco IOS software supports the following additional standards:

- AH—Authentication Header. A security protocol which provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).
- ESP—Encapsulating Security Payload. A security protocol which provides data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

Supported Hardware, Switching Paths, and Encapsulation

IPsec has certain requirements for hardware, switching paths, and encapsulation methods as follows:

- [Supported Hardware](#)
- [Supported Switching Paths](#)
- [Supported Encapsulation](#)

Supported Hardware

This section contains the following subsections:

- [VPN Accelerator Module \(VAM\) Support](#)
- [AIMs and NM Support](#)

VPN Accelerator Module (VAM) Support

The VAM is a single-width acceleration module. It provides high-performance, hardware-assisted tunneling and encryption services suitable for VPN remote access, site-to-site intranet, and extranet applications. It also provides platform scalability and security while working with all services necessary for successful VPN deployments—security, quality of service (QoS), firewall and intrusion detection, service-level validation, and management. The VAM off-loads IPsec processing from the main processor, thus freeing resources on the processor engines for other tasks.

The VAM provides hardware-accelerated support for the following multiple encryption functions:

- 56-bit DES standard mode: CBC
- 3-Key Triple DES (168-bit)
- SHA-1 and MD5
- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman key exchange RC4-40

For more information on VAMs, see the document “VPN Acceleration Module (VAM).”

AIMs and NM Support

The data encryption Advanced Integration Module (AIM) and Network Module (NM) provide hardware-based encryption.

The data encryption AIMs and NM are hardware Layer 3 (IPsec) encryption modules and provide DES and Triple DES IPsec encryption for multiple T1s or E1s of bandwidth. These products also have hardware support for Diffie-Hellman, RSA, and DSA key generation.

Before using either module, note that RSA manual keying is not supported.

See [Table 44](#) to determine which VPN encryption module to use.

IPPCP Software for Use with AIMS and NMs in Cisco 2600 and Cisco 3600 Series Routers

Software IPPCP with AIMS and NMs allow customers to use Lempel-Ziv-Stac (LZS) software compression with IPsec when a VPN module is in Cisco 2600 and Cisco 3600 series routers, allowing users to effectively increase the bandwidth on their interfaces.

Without IPPCP software, compression is not supported with the VPN encryption hardware AIM and NM; that is, a user had to remove the VPN module from the router and run software encryption with software compression. IPPCP enables all VPN modules to support LZS compression in software when the VPN module is in the router, thereby, allowing users to configure data compression and increase their bandwidth, which is useful for a low data link.

Without IPPCP, compression occurs at Layer 2, and encryption occurs at Layer 3. After a data stream is encrypted, it is passed on for compression services. When the compression engine receives the encrypted data streams, the data expands and does not compress. This feature enables both compression and encryption of the data to occur at Layer 3 by selecting LZS with the IPsec transform set; that is, LZS compression occurs before encryption, and it is able to get better compression ratio.

Table 44 AIM/VPN Encryption Module Support by Cisco IOS Release

	Encryption Module Support by Cisco IOS Release				
Platform	12.2(13)T	12.3(4)T	12.3(5)	12.3(6)	12.3(7)T
Cisco 831	Software-based AES				
Cisco 1710	Software-based AES				
Cisco 1711					
Cisco 1721					
Cisco 1751					
Cisco 1760					
Cisco 2600 XM	—			AIM-VPN/BPII-Plus Hardware Encryption Module	
Cisco 2611 XM	—	AIM-VPN/BPII Hardware Encryption Module			AIM-VPN/BPII-Plus Hardware Encryption Module
Cisco 2621 XM					
Cisco 2651 XM					
Cisco 2691 XM	AIM-VPN/EPII Hardware Encryption Module				AIM-VPN/EPII-Plus Hardware Encryption Module
Cisco 3735	AIM-VPN/EPII Hardware Encryption Module		AIM-VPN/EPII-Plus Hardware Encryption Module		
Cisco 3660	AIM-VPN/HPPII Hardware Encryption Module		AIM-VPN/HPPII-Plus Hardware Encryption Module		
Cisco 3745					

For more information on AIMS and NM, see [Installing Advanced Integration Modules in Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers](#).

Supported Switching Paths

Table 45 lists the supported switching paths that work with IPsec.

Table 45 **Supported Switching Paths for IPsec**

Switching Paths	Examples
Process switching	<pre>interface ethernet0/0 no ip route-cache</pre>
Fast switching	<pre>interface ethernet0/0 ip route-cache ! Ensure that you will not hit flow switching. no ip route-cache flow ! Disable CEF for the interface, which supercedes global CEF. no ip route-cache cef</pre>
Cisco Express Forwarding (CEF)	<pre>ip cef interface ethernet0/0 ip route-cache ! Ensure that you will not hit flow switching. no ip route-cache flow</pre>
Fast-flow switching	<pre>interface ethernet0/0 ip route-cache ! Enable flow switching p route-cache flow ! Disable CEF for the interface. no ip route-cache cef</pre>
CEF-flow switching	<pre>! Enable global CEF. ip cef interface ethernet0/0 ip route-cache ip route-cache flow ! Enable CEF for the interface ip route-cache cef</pre>

Supported Encapsulation

IPsec works with the following serial encapsulations: High-Level Data-Links Control (HDLC), PPP, and Frame Relay.

IPsec also works with the Generic Routing Encapsulation (GRE) and IPinIP Layer 3, Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP), Data Link Switching+ (DLSw+), and SRB tunneling protocols; however, multipoint tunnels are not supported. Other Layer 3 tunneling protocols may not be supported for use with IPsec.

Because the IPsec Working Group has not yet addressed the issue of group key distribution, IPsec currently cannot be used to protect group traffic (such as broadcast or multicast traffic).

IPsec Functionality Overview

IPsec provides the following network security services. (In general, local security policy dictates the use of one or more of these services.)

- **Data Confidentiality**—The IPsec sender can encrypt packets before transmitting them across a network.
- **Data Integrity**—The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.

- **Data Origin Authentication**—The IPsec receiver can authenticate the source of the IPsec packets sent. This service is dependent upon the data integrity service.
- **Anti-Replay**—The IPsec receiver can detect and reject replayed packets.

IPsec provides secure *tunnels* between two peers, such as two routers. You define which packets are considered sensitive and should be sent through these secure tunnels, and you define the parameters that should be used to protect these sensitive packets, by specifying characteristics of these tunnels. Then, when the IPsec peer recognizes such a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer. (The use of the term *tunnel* in this chapter does not refer to using IPsec in tunnel mode.)

More accurately, these *tunnels* are sets of security associations (SAs) that are established between two IPsec peers. The SAs define which protocols and algorithms should be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per security protocol (AH or ESP).

With IPsec you define what traffic should be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces by way of crypto map sets. Therefore, traffic may be selected on the basis of source and destination address, and optionally Layer 4 protocol, and port. (The access lists used for IPsec are used only to determine which traffic should be protected by IPsec, not which traffic should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.)

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in order—the router attempts to match the packet to the access list specified in that entry.

When a packet matches a **permit** entry in a particular access list, and the corresponding crypto map entry is tagged as **cisco**, connections are established if necessary. If the crypto map entry is tagged as **ipsec-isakmp**, IPsec is triggered. If no SA exists that IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry. (The behavior is different for dynamic crypto map entries. See the section “[Creating Dynamic Crypto Maps](#)” section later in this module.)

If the crypto map entry is tagged as **ipsec-manual**, IPsec is triggered. If no SA exists that IPsec can use to protect this traffic to the peer, the traffic is dropped. In this case, the SAs are installed via the configuration, without the intervention of IKE. If the SAs did not exist, IPsec did not have all of the necessary pieces configured.

Once established, the set of SAs (outbound, to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the router. “Applicable” packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

Multiple IPsec tunnels can exist between two peers to secure different data streams, with each tunnel using a separate set of SAs. For example, some data streams might be authenticated only while other data streams must both be encrypted and authenticated.

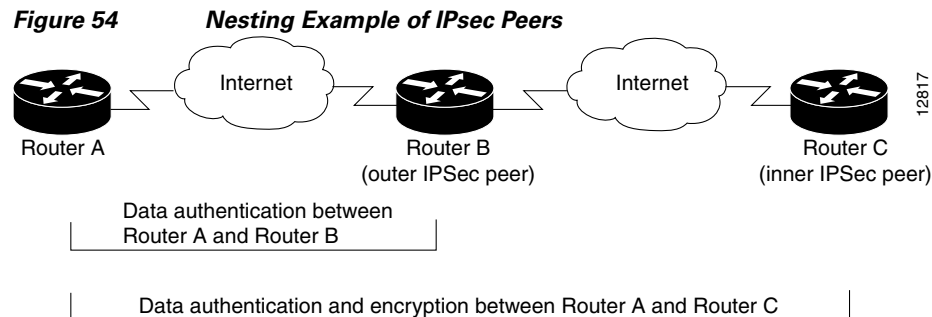
Access lists associated with IPsec crypto map entries also represent which traffic the router requires to be protected by IPsec. Inbound traffic is processed against the crypto map entries—if an unprotected packet matches a **permit** entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet.

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec protected traffic. During the IPsec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

IPsec Traffic Nested to Multiple Peers

You can nest IPsec traffic to a series of IPsec peers. For example, in order for traffic to traverse multiple firewalls (these firewalls have a policy of not letting through traffic that they have not authenticated), the router must establish IPsec tunnels with each firewall in turn. The “nearer” firewall becomes the “outer” IPsec peer.

In the example shown in [Figure 54](#), Router A encapsulates the traffic destined for Router C in IPsec (Router C is the inner IPsec peer). However, before Router A can send this traffic, it must first reencapsulate this traffic in IPsec in order to send it to Router B (Router B is the “outer” IPsec peer).



It is possible for the traffic between the “outer” peers to have one kind of protection (such as data authentication) and for traffic between the “inner” peers to have different protection (such as both data authentication and encryption).

How to Configure IPsec VPNs

Perform the tasks in the following sections to create IPsec VPNs:

- [Creating Crypto Access Lists, page 8](#)
- [Defining Transform Sets: A Combination of Security Protocols and Algorithms, page 14](#)
- [Creating Crypto Map Sets, page 17](#)
- [Applying Crypto Map Sets to Interfaces, page 30](#)

Creating Crypto Access Lists

To create crypto access lists that define which traffic is protected via IPsec tunnels, you should understand the following concepts:

- [Crypto Access List Overview](#)
- [When to Use the permit and deny Keywords in Crypto Access Lists](#)
- [Mirror Image Crypto Access Lists at Each IPsec Peer](#)
- [When to Use the any Keyword in Crypto Access Lists](#)

Crypto Access List Overview

Crypto access lists are used to define which IP traffic is protected by crypto and which traffic is not protected by crypto. (These access lists are *not* the same as regular access lists, which determine what traffic to forward or block at an interface.) For example, access lists can be created to protect all IP traffic between Subnet A and Subnet Y or Telnet traffic between Host A and Host B.

The access lists themselves are not specific to IPsec. It is the crypto map entry referencing the specific access list that defines whether IPsec processing is applied to the traffic matching a **permit** in the access list.

Crypto access lists associated with IPsec crypto map entries have four primary functions:

- Select outbound traffic to be protected by IPsec (permit = protect).
- Indicate the data flow to be protected by the new SAs (specified by a single **permit** entry) when initiating negotiations for IPsec security associations.
- Process inbound traffic in order to filter out and discard traffic that should have been protected by IPsec.
- Determine whether or not to accept requests for IPsec security associations on behalf of the requested data flows when processing IKE negotiation from the IPsec peer.
- Negotiation is performed only for **ipsec-isakmp** crypto map entries. In order to be accepted, if the peer initiates the IPsec negotiation, it must specify a data flow that is “permitted” by a crypto access list associated with an **ipsec-isakmp** crypto map entry.

If you want certain traffic to receive one combination of IPsec protection (for example, authentication only) and other traffic to receive a different combination of IPsec protection (for example, both authentication and encryption), you need to create two different crypto access lists to define the two different types of traffic. These different access lists are then used in different crypto map entries which specify different IPsec policies.

When to Use the permit and deny Keywords in Crypto Access Lists

Crypto protection can be permitted or denied for certain IP traffic in a crypto access list as follows:

- To protect IP traffic that matches the specified policy conditions in its corresponding crypto map entry, use the **permit** keyword in an access list.
- To refuse protection for IP traffic that matches the specified policy conditions in its corresponding crypto map entry, use the **deny** keyword in an access list.



Note

IP traffic is not protected by crypto if it is refused protection in all of the crypto map entries for an interface.

After the corresponding crypto map entry is defined and the crypto map set is applied to the interface, the defined crypto access list is applied to an interface the defined crypto access list is applied to an interface. Different access lists must be used in different entries of the same crypto map set. However, both inbound and outbound traffic is evaluated against the same “outbound” IPsec access list. Therefore, the access list’s criteria is applied in the forward direction to traffic exiting your router and in the reverse direction to traffic entering your router.

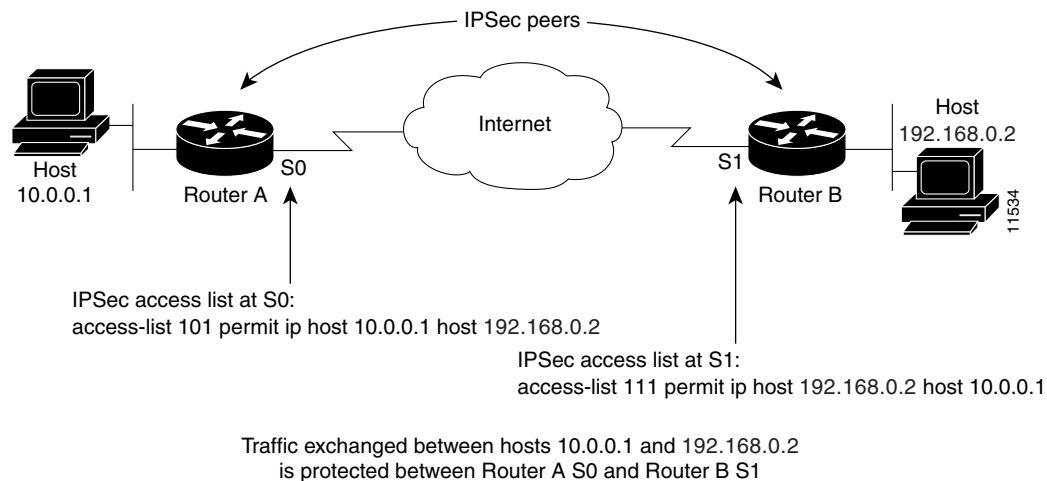
In [Figure 55](#), IPsec protection is applied to traffic between Host 10.0.0.1 and Host 192.168.0.2 as the data exits Router A’s S0 interface en route to Host 192.168.0.2. For traffic from Host 10.0.0.1 to Host 192.168.0.2, the access list entry on Router A is evaluated as follows:

```
source = host 10.0.0.1
dest = host 192.168.0.2
```

For traffic from Host 192.168.0.2 to Host 10.0.0.1, that same access list entry on Router A is evaluated as follows:

```
source = host 192.168.0.2
dest = host 10.0.0.1
```

Figure 55 How Crypto Access Lists Are Applied for Processing IPsec



If you configure multiple statements for a given crypto access list that is used for IPsec, in general the first **permit** statement that is matched is the statement used to determine the scope of the IPsec SA. That is, the IPsec SA is set up to protect traffic that meets the criteria of the matched statement only. Later, if traffic matches a different **permit** statement of the crypto access list, a new, separate IPsec SA is negotiated to protect traffic matching the newly matched access list statement.

Any unprotected inbound traffic that matches a **permit** entry in the crypto access list for a crypto map entry flagged as IPsec is dropped, because this traffic was expected to be protected by IPsec.



Note

If you view your router's access lists by using a command such as **show ip access-lists**, *all* extended IP access lists are shown in the command output. This display output includes extended IP access lists that are used for traffic filtering purposes and those that are used for crypto. The **show** command output does not differentiate between the different uses of the extended access lists.

The following example shows that if overlapping networks are used, then the most specific networks are defined in crypto sequence numbers before less specific networks are defined. In this example, the more specific network is covered by the crypto map sequence number 10, followed by the less specific network in the crypto map, which is sequence number 20.

```
crypto map mymap 10 ipsec-isakmp
  set peer 192.168.1.1
  set transform-set test
  match address 101
crypto map mymap 20 ipsec-isakmp
  set peer 192.168.1.2
  set transform-set test
  match address 102
```

```
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255  
access-list 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255
```

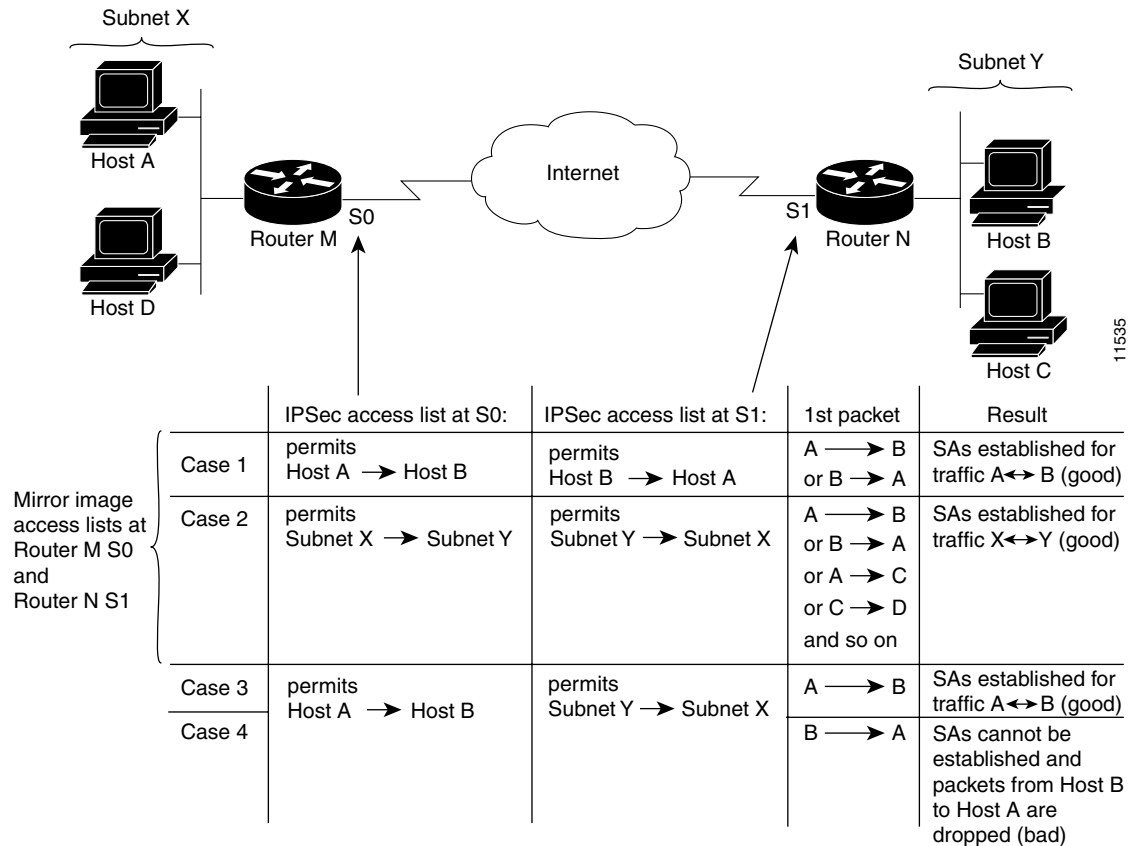
The following example shows how having a **deny** keyword in one crypto map sequence number and having a **permit** keyword for the same subnet and IP range in another crypto map sequence number is not supported.

```
crypto map mymap 10 ipsec-isakmp  
  set peer 192.168.1.1  
  set transform-set test  
  match address 101  
crypto map mymap 20 ipsec-isakmp  
  set peer 192.168.1.2  
  set transform-set test  
  match address 102  
  
access-list 101 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255  
access-list 101 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255  
  
access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

Mirror Image Crypto Access Lists at Each IPsec Peer

Cisco recommends that for every crypto access list specified for a static crypto map entry that you define at the local peer, you define a “mirror image” crypto access list at the remote peer. This ensures that traffic that has IPsec protection applied locally can be processed correctly at the remote peer. (The crypto map entries themselves must also support common transforms and must refer to the other system as a peer.)

[Figure 56](#) shows some sample scenarios when you have mirror image access lists and when you do not have mirror image access lists.

Figure 56 Mirror Image vs. Nonmirror Image Crypto Access Lists (for IPsec)

As Figure 56 indicates, IPsec SAs can be established as expected whenever the two peers' crypto access lists are mirror images of each other. However, an IPsec SA can be established only some of the time when the access lists are not mirror images of each other. This can happen in the case where an entry in one peer's access list is a subset of an entry in the other peer's access list, such as shown in Cases 3 and 4 of Figure 56. IPsec SA establishment is critical to IPsec—without SAs, IPsec does not work, causing any packets matching the crypto access list criteria to be silently dropped instead of being forwarded with IPsec.

In Figure 56, an SA cannot be established in Case 4. This is because SAs are always requested according to the crypto access lists at the initiating packet's end. In Case 4, Router N requests that all traffic between Subnet X and Subnet Y be protected, but this is a superset of the specific flows permitted by the crypto access list at Router M so the request is therefore not permitted. Case 3 works because Router M's request is a subset of the specific flows permitted by the crypto access list at Router N.

Because of the complexities introduced when crypto access lists are not configured as mirror images at peer IPsec devices, Cisco strongly encourages you to use mirror image crypto access lists.

When to Use the **any** Keyword in Crypto Access Lists

When you create crypto access lists, using the **any** keyword could cause problems. Cisco discourages the use of the **any** keyword to specify source or destination addresses.

The **any** keyword in a **permit** statement is discouraged when you have multicast traffic flowing through the IPsec interface; the **any** keyword can cause multicast traffic to fail.

The **permit any any** statement is strongly discouraged, because this causes all outbound traffic to be protected (and all protected traffic sent to the peer specified in the corresponding crypto map entry) and requires protection for all inbound traffic. Then, all inbound packets that lack IPsec protection are silently dropped, including packets for routing protocols, Network Time Protocol (NTP), echo, echo response, and so on.

You need to be sure you define which packets to protect. If you *must* use the **any** keyword in a **permit** statement, you must preface that statement with a series of **deny** statements to filter out any traffic (that would otherwise fall within that **permit** statement) that you do not want to be protected.

Also, use of **any** keyword in access control lists (ACLs) with reverse route injection (RRI) is not supported. (For more information on RRI, see the section “[Creating Crypto Map Sets](#).”)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]
or
ip access-list extended *name*
4. Repeat Step 3 for each crypto access list you want to create.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	access-list <i>access-list-number</i> { deny permit } <i>protocol source source-wildcard destination destination-wildcard</i> [log] Example: Router(config)# access-list 100 permit ip 10.0.68.0 0.0.0.255 10.1.1.0 0.0.0.255 or ip access-list extended <i>name</i> Example: Router(config)# ip access-list extended vpn-tunnel	Specifies conditions to determine which IP packets are protected. ¹ Enable or disable crypto for traffic that matches these conditions. Tip Cisco recommends that you configure “mirror image” crypto access lists for use by IPsec and that you avoid using the any keyword.
Step 4	—	Repeat Step 3 for each crypto access list you want to create.

1. You specify conditions using an IP access list designated by either a number or a name. The **access-list** command designates a numbered extended access list; the **ip access-list extended** command designates a named access list.

What to Do Next

After at least one crypto access list is created, a transform set needs to be defined as described in the section [“Defining Transform Sets: A Combination of Security Protocols and Algorithms.”](#)

Next the crypto access lists need to be associated to particular interfaces when you configure and apply crypto map sets to the interfaces are configured and applied (following instructions in the sections [“Creating Crypto Map Sets”](#) and [“Applying Crypto Map Sets to Interfaces”](#)).

Defining Transform Sets: A Combination of Security Protocols and Algorithms

Perform this task to define a transform set that is to be used by the IPsec peers during IPsec security association negotiations with IKE.

Restrictions

If you are specifying SEAL encryption, note the following restrictions:

- Your router and the other peer must not have hardware IPsec encryption.
- Your router and the other peer must support IPsec.
- Your router and the other peer must support the k9 subsystem.
- SEAL encryption is available only on Cisco equipment. Therefore, interoperability is not possible.

About Transform Sets

A transform set represents a certain combination of security protocols and algorithms. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

You can specify multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPsec SA negotiation to protect the data flows specified by that crypto map entry’s access list.

During IPsec security association negotiations with IKE, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and is applied to the protected traffic as part of both peers’ IPsec SAs. (With manually established SAs, there is no negotiation with the peer, so both sides must specify the same transform set.)

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change is not applied to existing security associations, but is used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2* [*transform3*]]

4. **mode** [**tunnel** | **transport**]
5. **exit**
6. **clear crypto sa** [**peer** {*ip-address* | *peer-name*} | **sa map** *map-name* | **sa entry** *destination-address protocol spi*]
7. **show crypto ipsec transform-set** [**tag** *transform-set-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec transform-set <i>transform-set-name transform1</i> [<i>transform2</i> [<i>transform3</i>]] Example: Router(config)# crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac	Defines a transform set and enters crypto transform configuration mode. There are complex rules defining which entries you can use for the transform arguments. These rules are explained in the command description for the crypto ipsec transform-set command, and Table 46 provides a list of allowed transform combinations.
Step 4	mode [tunnel transport] Example: Router(cfg-crypto-tran)# mode transport	(Optional) Changes the mode associated with the transform set. The mode setting is applicable only to traffic whose source and destination addresses are the IPsec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.)
Step 5	exit Example: Router(config)# exit	Exits global configuration mode.

	Command or Action	Purpose
Step 6	<pre>clear crypto sa [peer {ip-address peer-name} sa map map-name sa entry destination-address protocol spi]</pre> <p>Example: Router# clear crypto sa</p>	<p>(Optional) Clears existing IPsec security associations so that any changes to a transform set takes effect on subsequently established security associations.</p> <p>Manually established SAs are reestablished immediately.</p> <ul style="list-style-type: none"> Using the clear crypto sa command without parameters clear out the full SA database, which clears out active security sessions. You may also specify the peer, map, or entry keywords to clear out only a subset of the SA database.
Step 7	<pre>show crypto ipsec transform-set [tag transform-set-name]</pre> <p>Example: Router# show crypto ipsec transform-set</p>	<p>(Optional) Displays the configured transform sets.</p>

Table 46 shows allowed transform combinations.

Table 46 Allowed Transform Combinations

Transform Type	Transform	Description
AH Transform	ah-md5-hmac	AH with the MD5 (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm
	ah-sha-hmac	AH with the SHA (an HMAC variant) authentication algorithm
ESP Encryption Transform	esp-aes	ESP with the 128-bit AES encryption algorithm
	esp-aes 192	ESP with the 192-bit AES encryption algorithm
	esp-aes 256	ESP with the 256-bit AES encryption algorithm
	esp-des	ESP with the 56-bit DES encryption algorithm
	esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
	esp-null	Null encryption algorithm
	esp-seal	ESP with the 160-bit SEAL encryption algorithm.

Table 46 *Allowed Transform Combinations (continued)*

Transform Type	Transform	Description
ESP Authentication Transform	esp-md5-hmac	ESP with the MD5 (HMAC variant) authentication algorithm
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm
IP Compression Transform	comp-lzs	IP compression with the LZS algorithm

What to Do Next

After you have defined a transform set, you should create a crypto map as specified in the section [“Creating Crypto Map Sets.”](#)

Creating Crypto Map Sets

See one of the following sections, as appropriate, to help create crypto map sets:

- [Creating Static Crypto Maps](#)
- [Creating Dynamic Crypto Maps](#)
- [Creating Crypto Map Entries to Establish Manual SAs](#)

Prerequisites

Before you create crypto map entries, you should determine which type of crypto map—static, dynamic, or manual—best addresses the needs of your network. You should also understand the following concepts:

- [About Crypto Maps](#)
- [Load Sharing Among Crypto Maps](#)
- [Crypto Map Guidelines](#)

About Crypto Maps

Crypto map entries created for IPsec pull together the various parts used to set up IPsec SAs, including:

- Which traffic should be protected by IPsec (per a crypto access list)
- The granularity of the flow to be protected by a set of SAs
- Where IPsec-protected traffic should be sent (who the remote IPsec peer is)
- The local address to be used for the IPsec traffic (See the section [“Applying Crypto Map Sets to Interfaces”](#) for more details.)
- What IPsec SA should be applied to this traffic (selecting from a list of one or more transform sets)
- Whether SAs are manually established or are established via IKE
- Other parameters that might be necessary to define an IPsec SA

How Crypto Maps Work

Crypto map entries with the same crypto map name (but different map sequence numbers) are grouped into a crypto map set. Later, you apply these crypto map sets to interfaces; then, all IP traffic passing through the interface is evaluated against the applied crypto map set. If a crypto map entry sees outbound IP traffic that should be protected and the crypto map specifies the use of IKE, a SA is negotiated with the remote peer according to the parameters included in the crypto map entry; otherwise, if the crypto map entry specifies the use of manual SAs, an SA should have already been established via configuration. (If a dynamic crypto map entry sees outbound traffic that should be protected and no security association exists, the packet is dropped.)

The policy described in the crypto map entries is used during the negotiation of SAs. If the local router initiates the negotiation, it uses the policy specified in the static crypto map entries to create the offer to be sent to the specified IPsec peer. If the IPsec peer initiates the negotiation, the local router checks the policy from the static crypto map entries, as well as any referenced dynamic crypto map entries to decide whether to accept or reject the peer's request (offer).

For IPsec to succeed between two IPsec peers, both peers' crypto map entries must contain compatible configuration statements.

Compatible Crypto Maps: Establishing an SA

When two peers try to establish a SA, they must each have at least one crypto map entry that is compatible with one of the other peer's crypto map entries. For two crypto map entries to be compatible, they must at least meet the following criteria:

- The crypto map entries must contain compatible crypto access lists (for example, mirror image access lists). In the case where the responding peer is using dynamic crypto maps, the entries in the local crypto access list must be "permitted" by the peer's crypto access list.
- The crypto map entries must each identify the other peer (unless the responding peer is using dynamic crypto maps).
- The crypto map entries must have at least one transform set in common.

Load Sharing Among Crypto Maps

You can define multiple remote peers using crypto maps to allow for load sharing. Load sharing is useful because if one peer fails, there continues to be a protected path. The peer that packets are actually sent to is determined by the last peer that the router heard from (received either traffic or a negotiation request from) for a given data flow. If the attempt fails with the first peer, IKE tries the next peer on the crypto map list.

If you are not sure how to configure each crypto map parameter to guarantee compatibility with other peers, you might consider configuring dynamic crypto maps as described in the section "[Creating Dynamic Crypto Maps](#)." Dynamic crypto maps are useful when the establishment of the IPsec tunnels is initiated by the remote peer (such as in the case of an IPsec router fronting a server). They are not useful if the establishment of the IPsec tunnels is locally initiated, because the dynamic crypto maps are policy templates, not complete statements of policy. (Although the access lists in any referenced dynamic crypto map entry are used for crypto packet filtering.)

Crypto Map Guidelines

You can apply only one crypto map set to a single interface. The crypto map set can include a combination of IPsec/IKE and IPsec/manual entries. Multiple interfaces can share the same crypto map set if you want to apply the same policy to multiple interfaces.

If you create more than one crypto map entry for a given interface, use the *seq-num* argument of each map entry to rank the map entries: the lower the *seq-num* argument, the higher the priority. At the interface that has the crypto map set, traffic is evaluated against higher priority map entries first.

You must create multiple crypto map entries for a given interface if any of the following conditions exist:

- If different data flows are to be handled by separate IPsec peers.
- If you want to apply different IPsec security to different types of traffic (to the same or separate IPsec peers); for example, if you want traffic between one set of subnets to be authenticated, and traffic between another set of subnets to be both authenticated and encrypted. In this case the different types of traffic should have been defined in two separate access lists, and you must create a separate crypto map entry for each crypto access list.
- If you are not using IKE to establish a particular set of security associations, and want to specify multiple access list entries, you must create separate access lists (one per **permit** entry) and specify a separate crypto map entry for each access list.

Creating Static Crypto Maps


When IKE is used to establish SAs, the IPsec peers can negotiate the settings they use for the new security associations. This means that you can specify lists (such as lists of acceptable transforms) within the crypto map entry.

Perform this task to create crypto map entries that use IKE to establish the SAs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num ipsec-isakmp*
4. **match address** *access-list-id*
5. **set peer** {*hostname* | *ip-address*}
6. **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]
7. **set security-association lifetime** {*seconds seconds* | *kilobytes kilobytes*}
8. **set security-association level per-host**
9. **set pfs** [*group1* | *group2* | *group5*]
10. **exit**
11. **exit**
12. **show crypto map** [*interface interface* | *tag map-name*]

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-num ipsec-isakmp</i> Example: Router(config)# crypto map static-map 1 ipsec-isakmp	Names the crypto map entry to create (or modify), and enters crypto map configuration mode.
Step 4	match address <i>access-list-id</i> Example: Router(config-crypto-m)# match address vpn-tunnel	Names an extended access list. This access list determines which traffic should be protected by IPsec and which traffic should not be protected by IPsec security in the context of this crypto map entry.
Step 5	set peer { <i>hostname</i> <i>ip-address</i> } Example: Router(config-crypto-m)# set-peer 192.168.101.1	Specifies a remote IPsec peer, the peer to which IPsec protected traffic can be forwarded. Repeat for multiple remote peers.
Step 6	set transform-set <i>transform-set-name1</i> [<i>transform-set-name2</i> ... <i>transform-set-name6</i>] Example: Router(config-crypto-m)# set transform-set aasset	Specifies which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).
Step 7	set security-association lifetime { seconds <i>seconds</i> kilobytes <i>kilobytes</i> } Example: Router (config-crypto-m)# set security-association lifetime seconds 2700	(Optional) Specifies a SA lifetime for the crypto map entry. By default, the SAs of the crypto map are negotiated according to the global lifetimes.
Step 8	set security-association level per-host Example: Router(config-crypto-m)# set security-association level per-host	(Optional) Specifies that separate SAs should be established for each source and destination host pair. By default, a single IPsec “tunnel” can carry traffic for multiple source hosts and multiple destination hosts.
		 Caution Use this command with care, because multiple streams between given subnets can rapidly consume resources.

	Command	Purpose
Step 9	set pfs [group1 group2 group 5] Example: Router(config-crypto-m)# set pfs group2	(Optional) Specifies that IPsec either should ask for perfect forward secrecy (PFS) when requesting new SAs for this crypto map entry or should demand PFS in requests received from the IPsec peer. By default, PFS is not requested. If no group is specified with this command, group1 is used as the default.
Step 10	exit Example: Router(config-crypto-m)# exit	Exits crypto-map configuration mode.
Step 11	exit Example: Router(config)# exit	Exits global configuration mode.
Step 12	show crypto map [interface <i>interface</i> tag <i>map-name</i>] Example: Router# show crypto map	Displays your crypto map configuration.

Troubleshooting Tips

Certain configuration changes take effect only when negotiating subsequent SAs. If you want the new settings to take immediate effect, you must clear the existing SAs so that they are re-established with the changed configuration. If the router is actively processing IPsec traffic, it is desirable to clear only the portion of the SA database that would be affected by the configuration changes (that is, clear only the SAs established by a given crypto map set). Clearing the full SA database should be reserved for large-scale changes, or when the router is processing very little other IPsec traffic.

To clear IPsec SAs, use the **clear crypto sa** command with appropriate parameters. (Omitting all parameters clears out the full SA database, which clears active security sessions.)

What to Do Next

After you have successfully created a static crypto map, you must apply the crypto map set to each interface through which IPsec traffic flows. To complete this task, see the section “[Applying Crypto Map Sets to Interfaces](#).”

Creating Dynamic Crypto Maps

Dynamic crypto maps can ease IPsec configuration and are recommended for use with networks where the peers are not always predetermined. To create dynamic crypto maps, you should understand the following concepts:

- [Dynamic Crypto Maps Overview](#)
- [Tunnel Endpoint Discovery \(TED\)](#)

Dynamic Crypto Maps Overview

Dynamic crypto maps are only available for use by IKE.

A dynamic crypto map entry is essentially a static crypto map entry without all the parameters configured. It acts as a policy template where the missing parameters are later dynamically configured (as the result of an IPsec negotiation) to match a remote peer's requirements. This allows remote peers to exchange IPsec traffic with the router even if the router does not have a crypto map entry specifically configured to meet all of the remote peer's requirements.

Dynamic crypto maps are not used by the router to initiate new IPsec security associations with remote peers. Dynamic crypto maps are used when a remote peer tries to initiate an IPsec security association with the router. Dynamic crypto maps are also used in evaluating traffic.

A dynamic crypto map set is included by reference as part of a crypto map set. Any crypto map entries that reference dynamic crypto map sets should be the lowest priority crypto map entries in the crypto map set (that is, have the highest sequence numbers) so that the other crypto map entries are evaluated first; that way, the dynamic crypto map set is examined only when the other (static) map entries are not successfully matched.

If the router accepts the peer's request, at the point that it installs the new IPsec security associations it also installs a temporary crypto map entry. This entry is filled in with the results of the negotiation. At this point, the router performs normal processing, using this temporary crypto map entry as a normal entry, even requesting new security associations if the current ones are expiring (based upon the policy specified in the temporary crypto map entry). Once the flow expires (that is, all of the corresponding security associations expire), the temporary crypto map entry is then removed.

For both static and dynamic crypto maps, if unprotected inbound traffic matches a **permit** statement in an access list, and the corresponding crypto map entry is tagged as "IPsec," then the traffic is dropped because it is not IPsec-protected. (This is because the security policy as specified by the crypto map entry states that this traffic must be IPsec-protected.)

For static crypto map entries, if outbound traffic matches a **permit** statement in an access list and the corresponding SA is not yet established, the router initiates new SAs with the remote peer. In the case of dynamic crypto map entries, if no SA existed, the traffic would simply be dropped (because dynamic crypto maps are not used for initiating new SAs).



Note

Use care when using the **any** keyword in **permit** entries in dynamic crypto maps. If it is possible for the traffic covered by such a **permit** entry to include multicast or broadcast traffic, the access list should include **deny** entries for the appropriate address range. Access lists should also include **deny** entries for network and subnet broadcast traffic, and for any other traffic that should not be IPsec protected.

Restrictions for Dynamic Crypto Maps

Dynamic crypto map entries specify crypto access lists that limit traffic for which IPsec SAs can be established. A dynamic crypto map entry that does not specify an access list is ignored during traffic filtering. A dynamic crypto map entry with an empty access list causes traffic to be dropped. If there is only one dynamic crypto map entry in the crypto map set, it must specify acceptable transform sets.

Tunnel Endpoint Discovery (TED)

Defining a dynamic crypto map allows only the receiving router to dynamically determine an IPsec peer. TED allows the initiating router to dynamically determine an IPsec peer for secure IPsec communications.

Dynamic TED helps to simplify IPsec configuration on the individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the required IPsec transforms.

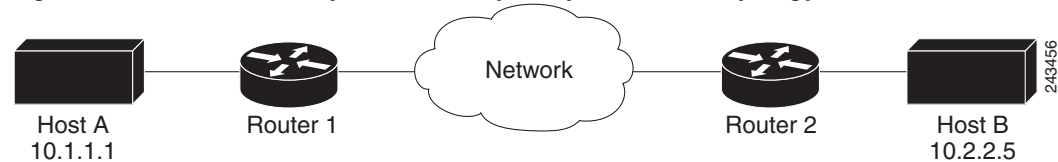
To have a large, fully-meshed network *without* TED, each peer needs to have static crypto maps to every other peer in the network. For example, if there are 100 peers in a large, fully-meshed network, each router needs 99 static crypto maps for each of its peers. With TED, only a single dynamic crypto map with TED enabled is needed because the peer is discovered dynamically. Thus, static crypto maps do not need to be configured for each peer.

**Note**

TED helps only in discovering peers; otherwise, TED does not function any differently than normal IPsec. TED does not improve the scalability of IPsec (in terms of performance or the number of peers or tunnels).

Figure 57 and the corresponding steps explain a sample TED network topology.

Figure 57 Tunnel Endpoint Discovery Sample Network Topology



-
- Step 1** Host A sends a packet that is destined for Host B.
- Step 2** Router 1 intercepts and reads the packet. According to the IKE policy, Router 1 contains the following information: the packet must be encrypted, there are no SAs for the packet, and TED is enabled. Thus, Router 1 drops the packet and sends a TED probe into the network. (The TED probe contains the IP address of Host A (as the source IP address) and the IP address of Host B (as the destination IP address) embedded in the payload.
- Step 3** Router 2 intercepts the TED probe and checks the probe against the ACLs that it protects; after the probe matches an ACL, it is recognized as a TED probe for proxies that the router protects. It then sends a TED reply with the IP address of Host B (as the source IP address) and the IP address of Host A (as the destination IP address) embedded in the payload.
- Step 4** Router 1 intercepts the TED reply and checks the payloads for the IP address and half proxy of Router 2. It then combines the source side of its proxy with the proxy found in the second payload and initiates an IKE session with Router 2; thereafter, Router 1 initiates an IPsec session with Router 2.

**Note**

IKE cannot occur until the peer is identified.

TED Versions

The following table lists the available TED versions:

Version	First Available Release	Description
TEDv1	12.0(5)T	Performs basic TED functionality on nonredundant networks.
TEDv2	12.1M	Enhanced to work with redundant networks with paths through multiple security gateways between the source and the destination.
TEDv3	12.2M	Enhanced to allow non-IP-related entries to be used in the access list.

TED Restrictions

TED has the following restrictions:

- It is Cisco proprietary.
- It is available only on dynamic crypto maps. (The dynamic crypto map template is based on the dynamic crypto map performing peer discovery. Although there are no access-list restrictions on the dynamic crypto map template, the dynamic crypto map template should cover data sourced from the protected traffic and the receiving router using the **any** keyword. When using the **any** keyword, include explicit **deny** statements to exempt routing protocol traffic prior to entering the **permit any** command.)
- TED works only in tunnel mode; that is, it does not work in transport mode.
- It is limited by the performance and scalability of limitation of IPsec on each individual platform.



Note

Enabling TED slightly decreases the general scalability of IPsec because of the set-up overhead of peer discovery, which involves an additional “round-trip” of IKE messages (TED probe and reply). Although minimal, the additional memory used to store data structures during the peer discovery stage adversely affects the general scalability of IPsec.

- The IP addresses must be able to be routed within the network.
- The access list used in the crypto map for TED can only contain IP-related entries—TCP, UDP, or any other protocol cannot be used in the access list.



Note

This restriction is no longer applicable in TEDv3.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name* *dynamic-seq-num*
4. **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]
5. **match address** *access-list-id*
6. **set peer** {*hostname* | *ip-address*}
7. **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

8. **set pfs** [group1 | group2 | group5]
9. **exit**
10. **exit**
11. **show crypto dynamic-map** [tag *map-name*]
12. **configure terminal**
13. **crypto map** *map-name seq-num ipsec-isakmp dynamic dynamic-map-name* [discover]

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto dynamic-map <i>dynamic-map-name dynamic-seq-num</i> Example: Router(config)# crypto dynamic-map test-map 1	Creates a dynamic crypto map entry and enters crypto map configuration mode.
Step 4	set transform-set <i>transform-set-name1</i> [<i>transform-set-name2...transform-set-name6</i>] Example: Router(config-crypto-m)# set transform-set aasset	Specifies which transform sets are allowed for the crypto map entry. List multiple transform sets in order of priority (highest priority first). This is the only configuration statement required in dynamic crypto map entries.

	Command	Purpose
Step 5	<p>match address <i>access-list-id</i></p> <p>Example: Router(config-crypto-m)# match address 101</p>	<p>(Optional) Accesses list number or name of an extended access list.</p> <p>This access list determines which traffic should be protected by IPsec and which traffic should not be protected by IPsec security in the context of this crypto map entry.</p> <p>Note Although access-lists are optional for dynamic crypto maps, they are highly recommended.</p> <p>If this is configured, the data flow identity proposed by the IPsec peer must fall within a permit statement for this crypto access list.</p> <p>If this is not configured, the router accepts any data flow identity proposed by the IPsec peer. However, if this is configured but the specified access list does not exist or is empty, the router drops all packets. This is similar to static crypto maps because they also require that an access list be specified.</p> <p>Care must be taken if the any keyword is used in the access list, because the access list is used for packet filtering as well as for negotiation.</p> <p>You must configure a match address; otherwise, the behavior is not secure, and you cannot enable TED because packets are sent in the clear (unencrypted.)</p>
Step 6	<p>set peer {<i>hostname</i> <i>ip-address</i>}</p> <p>Example: Router(config-crypto-m)# set peer 192.168.101.1</p>	<p>(Optional) Specifies a remote IPsec peer. Repeat for multiple remote peers.</p> <p>Note This is rarely configured in dynamic crypto map entries. Dynamic crypto map entries are often used for unknown remote peers.</p>
Step 7	<p>set security-association lifetime {seconds <i>seconds</i> kilobytes <i>kilobytes</i>}</p> <p>Example: Router (config-crypto-m)# set security-association lifetime seconds 7200</p>	<p>(Optional) Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IP Security SAs.</p>
Step 8	<p>set pfs [group1 group2 group5]</p> <p>Example: Router(config-crypto-m)# set pfs group2</p>	<p>(Optional) Specifies that IPsec should ask for PFS when requesting new security associations for this crypto map entry or should demand PFS in requests received from the IPsec peer.</p> <p>By default, PFS is not requested. If no group is specified with this command, group1 is used as the default.</p>
Step 9	<p>exit</p> <p>Example: Router(config-crypto-m)# exit</p>	<p>Exits crypto-map configuration mode and returns to global configuration mode.</p>

	Command	Purpose
Step 10	exit Example: Router(config)# exit	Exits global configuration mode.
Step 11	show crypto dynamic-map [tag <i>map-name</i>] Example: Router# show crypto dynamic-map	(Optional) Displays information about dynamic crypto maps.
Step 12	configure terminal Example: Router# configure terminal	Returns to global configuration mode.
Step 13	crypto map <i>map-name</i> <i>seq-num</i> ipsec-isakmp dynamic <i>dynamic-map-name</i> [discover] Example: Router(config)# crypto map static-map 1 ipsec-isakmp dynamic test-map discover	(Optional) Adds a dynamic crypto map to a crypto map set. You should set the crypto map entries referencing dynamic maps to the lowest priority entries in a crypto map set. Note You must issue the discover keyword to enable TED.

Troubleshooting Tips

Certain configuration changes take effect only when negotiating subsequent SAs. If you want the new settings to take immediate effect, you must clear the existing SAs so that they are reestablished with the changed configuration. If the router is actively processing IPsec traffic, it is desirable to clear only the portion of the SA database that would be affected by the configuration changes (that is, clear only the SAs established by a given crypto map set). Clearing the full SA database should be reserved for large-scale changes, or when the router is processing very little other IPsec traffic.

To clear IPsec SAs, use the **clear crypto sa** command with appropriate parameters. (Omitting all parameters clears the full SA database, which clears active security sessions.)

What to Do Next

After you have successfully created a crypto map set, you must apply the crypto map set to each interface through which IPsec traffic flows. To complete this task, see the section “[Applying Crypto Map Sets to Interfaces](#).”

Creating Crypto Map Entries to Establish Manual SAs

The use of manual security associations is a result of a prior arrangement between the users of the local router and the IPsec peer. The two parties may begin with manual SAs and then move to using SAs established via IKE, or the remote party’s system may not support IKE. If IKE is not used for establishing the SAs, there is no negotiation of SAs, so the configuration information in both systems must be the same in order for traffic to be processed successfully by IPsec.

The local router can simultaneously support manual and IKE-established SAs, even within a single crypto map set.

There is very little reason to disable IKE on the local router (unless the router only supports manual SAs, which is unlikely).

**Note**

Access lists for crypto map entries tagged as **ipsec-manual** are restricted to a single **permit** entry and subsequent entries are ignored. In other words, the SAs established by that particular crypto map entry are only for a single data flow. To be able to support multiple manually established SAs for different kinds of traffic, define multiple crypto access lists, and then apply each one to a separate **ipsec-manual** crypto map entry. Each access list should include one **permit** statement defining what traffic to protect.

To create crypto map entries to establish manual SAs (that is, when IKE is not used to establish the SAs), perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num ipsec-manual*
4. **match address** *access-list-id*
5. **set peer** {*hostname* | *ip-address*}
6. **set transform-set** *transform-set-name*
7. **set session-key inbound ah spi hex-key-string**
or
set session-key outbound ah spi hex-key-string
8. **set session-key inbound esp spi cipher hex-key-string [authenticator hex-key-string]**
or
set session-key outbound esp spi cipher hex-key-string [authenticator hex-key-string]
9. **exit**
10. **exit**
11. **show crypto map** [*interface interface* | *tag map-name*]

DETAILED STEPS

	Command	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
	Example: Router> enable	
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command	Purpose
Step 3	crypto map <i>map-name seq-num ipsec-manual</i> Example: Router(config)# crypto map mymap 10 ipsec-manual	Specifies the crypto map entry to create or modify and enters crypto map configuration mode.
Step 4	match address <i>access-list-id</i> Example: Router(config-crypto-m)# match address 102	Names an IPsec access list that determines which traffic should be protected by IPsec and which traffic should not be protected by IPsec in the context of this crypto map entry. (The access list can specify only one permit entry when IKE is not used.)
Step 5	set peer { <i>hostname</i> <i>ip-address</i> } Example: Router(config-crypto-m)# set peer 10.0.0.5	Specifies the remote IPsec peer. This is the peer to which IPsec protected traffic should be forwarded. (Only one peer can be specified when IKE is not used.)
Step 6	set transform-set <i>transform-set-name</i> Example: Router(config-crypto-m)# set transform-set someset	Specifies which transform set should be used. This must be the same transform set that is specified in the remote peer's corresponding crypto map entry. Note Only one transform set can be specified when IKE is not used.
Step 7	set session-key inbound ah <i>spi hex-key-string</i> Example: Router(config-crypto-m)# set session-key inbound ah 256 98765432109876549876543210987654 and set session-key outbound ah <i>spi hex-key-string</i> Example: Router(config-crypto-m)# set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc	Sets the AH security parameter indexes (SPIs) and keys to apply to inbound and outbound protected traffic if the specified transform set includes the AH protocol. (This manually specifies the AH security association to be used with protected traffic.)
Step 8	set session-key inbound esp <i>spi cipher hex-key-string</i> [authenticator <i>hex-key-string</i>] Example: Router(config-crypto-m)# set session-key inbound esp 256 cipher 0123456789012345 and set session-key outbound esp <i>spi cipher hex-key-string</i> [authenticator <i>hex-key-string</i>] Example: Router(config-crypto-m)# set session-key outbound esp 256 cipher abcdefabcdefabcd	Sets the ESP SPIs and keys to apply to inbound and outbound protected traffic if the specified transform set includes the ESP protocol. Specifies the cipher keys if the transform set includes an ESP cipher algorithm. Specifies the authenticator keys if the transform set includes an ESP authenticator algorithm. (This manually specifies the ESP security association to be used with protected traffic.)

	Command	Purpose
Step 9	exit Example: Router(config-crypto-m)# exit	Exits crypto-map configuration mode and returns to global configuration mode.
Step 10	exit Example: Router(config)# exit	Exits global configuration mode.
Step 11	show crypto map [interface <i>interface</i> tag <i>map-name</i>] Example: Router# show crypto map	Displays your crypto map configuration.

Troubleshooting Tips

For manually established SAs, you must clear and reinitialize the SAs for the changes to take effect. To clear IPsec SAs, use the **clear crypto sa** command with appropriate parameters. (Omitting all parameters clears the full SA database, which clears active security sessions.)

What to Do Next

After you have successfully created a crypto map set, you must apply the crypto map set to each interface through which IPsec traffic flows. To complete this task, see the section “[Applying Crypto Map Sets to Interfaces](#).”

Applying Crypto Map Sets to Interfaces

You need to apply a crypto map set to each interface through which IPsec traffic flows. Applying the crypto map set to an interface instructs the router to evaluate all the interface’s traffic against the crypto map set and to use the specified policy during connection or security association negotiation on behalf of traffic to be protected by crypto.

Perform this task to apply a crypto map to an interface.

Redundant Interfaces Sharing the Same Crypto Map

For redundancy, you could apply the same crypto map set to more than one interface. The default behavior is as follows:

- Each interface has its own piece of the security association database.
- The IP address of the local interface is used as the local address for IPsec traffic originating from or destined to that interface.

If you apply the same crypto map set to multiple interfaces for redundancy purposes, you need to specify an identifying interface. One suggestion is to use a loopback interface as the identifying interface. This has the following effects:

- The per-interface portion of the IPsec security association database is established one time and shared for traffic through all the interfaces that share the same crypto map.

- The IP address of the identifying interface is used as the local address for IPsec traffic originating from or destined to those interfaces sharing the same crypto map set.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **crypto map** *map-name*
5. **exit**
6. **crypto map** *map-name* **local-address** *interface-id*
7. **exit**
8. **show crypto map** [**interface** *interface*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# Interface FastEthernet 0/0	Configures an interface and enters interface configuration mode.
Step 4	crypto map <i>map-name</i> Example: Router(config-if)# crypto map mymap	Applies a crypto map set to an interface.
Step 5	exit Example: Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 6	crypto map <i>map-name</i> local-address <i>interface-id</i> Example: Router(config)# crypto map mymap local-address loopback0	(Optional) Permits redundant interfaces to share the same crypto map using the same local identity.

	Command or Action	Purpose
Step 7	exit Example: Router(config)# exit	(Optional) Exits global configuration mode.
Step 8	show crypto map [interface <i>interface</i>] Example: Router# show crypto map	(Optional) Displays your crypto map configuration

Configuration Examples for Configuring an IPsec VPN

This section contains the following configuration example:

- [AES-Based Static Crypto Map: Example, page 32](#)

AES-Based Static Crypto Map: Example

The following example is a portion of the **show running-config** command. This example shows how to configure a static crypto map and define AES as the encryption method.

```
crypto isakmp policy 10
  encryption aes 256
  authentication pre-share
  lifetime 180

crypto isakmp key cisco123 address 10.0.110.1
!
!
crypto ipsec transform-set aasset esp-aes 256 esp-sha-hmac
mode transport
!
crypto map aesmap 10 ipsec-isakmp
  set peer 10.0.110.1
  set transform-set aasset
  match address 120
!
!
!
voice call carrier capacity active
!
!
mta receive maximum-recipients 0
!
!
interface FastEthernet0/0
  ip address 10.0.110.2 255.255.255.0
  ip nat outside
  no ip route-cache
  no ip mroute-cache
  duplex auto
  speed auto
  crypto map aesmap
!
interface Serial0/0
```

```

no ip address
shutdown
!
interface FastEthernet0/1
 ip address 10.0.110.1 255.255.255.0
 ip nat inside
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
!
ip nat inside source list 110 interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.5.1.1
ip route 10.0.110.0 255.255.255.0 FastEthernet0/0
ip route 172.18.124.0 255.255.255.0 10.5.1.1
ip route 172.18.125.3 255.255.255.255 10.5.1.1
ip http server
!
!
access-list 110 deny ip 10.0.110.0 0.0.0.255 10.0.110.0 0.0.0.255
access-list 110 permit ip 10.0.110.0 0.0.0.255 any
access-list 120 permit ip 10.0.110.0 0.0.0.255 10.0.110.0 0.0.0.255
!

```

Additional References

The following sections provide references related to IPsec VPN configuration.

Related Documents

Related Topic	Document Title
IKE configuration	“Configuring IKE for IPsec VPNs” module
IKE, IPsec, and PKI configuration commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Security Command Reference

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> CISCO-IPSEC-FLOW-MONITOR- MIB CISCO-IPSEC-MIB CISCO-IPSEC-POLICY-MAP-MIB 	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFCs	Title
RFC 2401	Security Architecture for the Internet Protocol
RFC 2402	<i>IP Authentication Header</i>
RFC 2403	The Use of HMAC-MD5-96 within ESP and AH
RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC 2406	<i>IP Encapsulating Security Payload (ESP)</i>
RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Security for VPNs with IPsec

Table 47 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Cisco IOS Carrier Ethernet Features Roadmap](#).”

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, Catalyst OS, and Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 47 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 47 Feature Information for Configuring Security for IPsec VPNs

Feature Name	Software Releases	Feature Configuration Information
Advanced Encryption Standard (AES)	12.2(8)T	<p>This feature adds support for the new encryption standard AES, which is a privacy transform for IPsec and IKE and has been developed to replace DES.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Supported Standards Defining Transform Sets: A Combination of Security Protocols and Algorithms <p>The following commands were modified by this feature: crypto ipsec transform-set, encryption (IKE policy), show crypto ipsec transform-set, show crypto isakmp policy</p>
DES/3DES/AES VPN Encryption Module (AIM-VPN/EP1, AIM-VPN/HP1, AIM-VPN/BP1 Family)	12.3(7)T	<p>This feature describes which VPN encryption hardware AI and NM are supported in certain Cisco IOS software releases.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> AIMs and NM Support

Table 47 *Feature Information for Configuring Security for IPsec VPNs (continued)*

Feature Name	Software Releases	Feature Configuration Information
SEAL Encryption	12.3(7)T	<p>This feature adds support for SEAL encryption in IPsec.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> Supported Standards Defining Transform Sets: A Combination of Security Protocols and Algorithms <p>The following command was modified by this feature: crypto ipsec transform-set</p>
Software IPPCP (LZS) with Hardware Encryption	12.2(13)T	<p>This feature allows customers to use LZS software compression with IPsec when a VPN module is in Cisco 2600 and Cisco 3600 series routers.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> AIMs and NM Support
IKE Shared Secret Using AAA Server	Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.

Glossary

anti-replay—Security service where the receiver can reject old or duplicate packets to protect itself against replay attacks. IPsec provides this optional service by use of a sequence number combined with the use of data authentication. Cisco IOS IPsec provides this service whenever it provides the data authentication service, except for manually established SAs (that is, SAs established by configuration and not by IKE).

data authentication—Verification of the integrity and origin of the data.

Data authentication can refer either to integrity alone or to both of these concepts (although data origin authentication is dependent upon data integrity).

data confidentiality—Security service in which the protected data cannot be observed.

data flow—Grouping of traffic, identified by a combination of source address or mask; destination address or mask; IP next protocol field, and source and destination ports, where the protocol and port fields can have the values of **any**. IPsec protection is applied to data flows.

peer—In the context of this module, a “peer” is a router or other device that participates in IPsec.

PFS—perfect forward secrecy. Cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.

SA—security association. Description of how two or more entities use security services in the context of a particular security protocol (AH or ESP) to communicate securely on behalf of a particular data flow. The transform and the shared secret keys are used for protecting the traffic.

SPI—security parameter index. A number which, together with a destination IP address and security protocol, uniquely identifies a particular security association. Without IKE, the SPI is manually specified for each security association.

transform—List of operations performed on a dataflow to provide data authentication, data confidentiality, and data compression. For example, one transform is the ESP protocol with the HMAC-MD5 authentication algorithm; another transform is the AH protocol with the 56-bit DES encryption algorithm and the ESP protocol with the HMAC-SHA authentication algorithm.

tunnel—In the context of this module, “tunnel” is a secure communication path between two peers, such as two routers. It does not refer to using IPsec in tunnel mode.



Note

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005–2009 Cisco Systems, Inc. All rights reserved.



IPsec Virtual Tunnel Interface

First Published: October 18, 2004

Last Updated: June 11, 2008

IP security (IPsec) virtual tunnel interfaces (VTIs) provide a routable interface type for terminating IPsec tunnels and an easy way to define protection between sites to form an overlay network. IPsec VTIs simplify configuration of IPsec for protection of remote links, support multicast, and simplify network management and load balancing.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for IPsec Virtual Tunnel Interface” section on page 24](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Catalyst OS, and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Restrictions for IPsec Virtual Tunnel Interface, page 2](#)
- [Information About IPsec Virtual Tunnel Interface, page 3](#)
- [How to Configure IPsec Virtual Tunnel Interface, page 7](#)
- [Configuration Examples for IPsec Virtual Tunnel Interface, page 10](#)
- [Additional References, page 21](#)
- [Command Reference, page 23](#)
- [Feature Information for IPsec Virtual Tunnel Interface, page 24](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for IPsec Virtual Tunnel Interface

IPsec Transform Set

The IPsec transform set must be configured in tunnel mode only.

IKE Security Association

The Internet Key Exchange (IKE) security association (SA) is bound to the VTI. Because IKE SA is bound to the VTI, the same IKE SA cannot be used for a crypto map.

IPsec SA Traffic Selectors

Static VTIs (SVTIs) support only a single IPsec SA that is attached to the VTI interface. The traffic selector for the IPsec SA is always “IP any any.”

A dynamic VTI (DVTIs) also is a point-point interface that supports only a single IPsec SA, but the DVTI is flexible in that it can accept the IPsec selectors that are proposed by the initiator.

IPv4 and IPv6 Packets

This feature supports SVTIs that are configured to encapsulate IPv4 packets or IPv6 packets, but IPv4 packets cannot carry IPv6 packets, and IPv6 packets cannot carry IPv4 packets.

Proxy

SVTIs support only the “IP any any” proxy.

DVTIs support only one proxy, which can be “IP any any” or any subset of it.

QoS Traffic Shaping

The shaped traffic is process switched.

Stateful Failover

IPsec stateful failover is not supported with IPsec VTIs.

Tunnel Protection

The **shared** keyword is not required and must not be configured when using the **tunnel mode ipsec ipv4** command for IPsec IPv4 mode.

Static VTIs Versus GRE Tunnels

The IPsec VTI is limited to IP unicast and multicast traffic only, as opposed to GRE tunnels, which have a wider application for IPsec implementation.

VRF-Aware IPsec Configuration

In VRF-aware IPsec configurations with either SVTIs or DVTIs, the VRF must *not* be configured in the Internet Security Association and Key Management Protocol (ISAKMP) profile. Instead, the VRF must be configured on the tunnel interface for SVTIs. For DVTIs, you must apply VRF to the vtemplate using the **ip vrf forwarding** command.

Information About IPsec Virtual Tunnel Interface

The use of IPsec VTIs both greatly simplifies the configuration process when you need to provide protection for remote access and provides a simpler alternative to using generic routing encapsulation (GRE) or Layer 2 Tunneling Protocol (L2TP) tunnels for encapsulation and crypto maps with IPsec. A major benefit associated with IPsec VTIs is that the configuration does not require a static mapping of IPsec sessions to a physical interface. The IPsec tunnel endpoint is associated with an actual (virtual) interface. Because there is a routable interface at the tunnel endpoint, many common interface capabilities can be applied to the IPsec tunnel.

The IPsec VTI allows for the flexibility of sending and receiving both IP unicast and multicast encrypted traffic on any physical interface, such as in the case of multiple paths. Traffic is encrypted or decrypted when it is forwarded from or to the tunnel interface and is managed by the IP routing table. Using IP routing to forward the traffic to the tunnel interface simplifies the IPsec VPN configuration compared to the more complex process of using access control lists (ACLs) with the crypto map in native IPsec configurations. DVTIs function like any other real interface so that you can apply quality of service (QoS), firewall, and other security services as soon as the tunnel is active.

Without Virtual Private Network (VPN) Acceleration Module2+ (VAM2+) accelerating virtual interfaces, the packet traversing an IPsec virtual interface is directed to the router processor (RP) for encapsulation. This method tends to be slow and has limited scalability. In hardware crypto mode, all the IPsec VTIs are accelerated by the VAM2+ crypto engine, and all traffic going through the tunnel is encrypted and decrypted by the VAM2+.

The following sections provide details about the IPsec VTI:

- [Benefits of Using IPsec Virtual Tunnel Interfaces, page 3](#)
- [Routing with IPsec Virtual Tunnel Interfaces, page 5](#)
- [Static Virtual Tunnel Interfaces, page 3](#)
- [Dynamic Virtual Tunnel Interfaces, page 4](#)
- [Dynamic Virtual Tunnel Interface Life Cycle, page 5](#)
- [Traffic Encryption with the IPsec Virtual Tunnel Interface, page 6](#)

Benefits of Using IPsec Virtual Tunnel Interfaces

IPsec VTIs allow you to configure a virtual interface to which you can apply features. Features for clear-text packets are configured on the VTI. Features for encrypted packets are applied on the physical outside interface. When IPsec VTIs are used, you can separate the application of features such as NAT, ACLs, and QoS and apply them to clear-text or encrypted text, or both. When crypto maps are used, there is no simple way to apply encryption features to the IPsec tunnel.

There are two types of VTI interfaces: static VTIs (SVTIs) and dynamic VTIs (DVTIs).

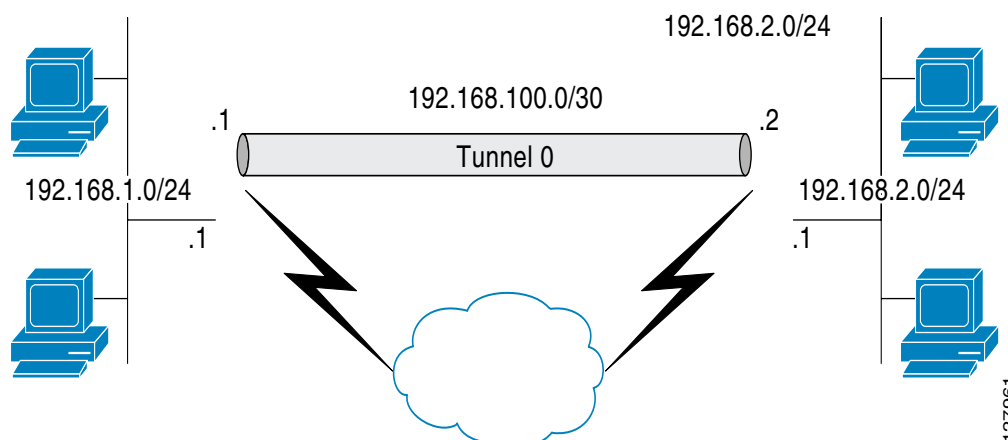
Static Virtual Tunnel Interfaces

SVTI configurations can be used for site-to-site connectivity in which a tunnel provides always-on access between two sites. The advantage of using SVTIs as opposed to crypto map configurations is that users can enable dynamic routing protocols on the tunnel interface without the extra 24 bytes required for GRE headers, thus reducing the bandwidth for sending encrypted data.

Additionally, multiple Cisco IOS software features can be configured directly on the tunnel interface and on the physical egress interface of the tunnel interface. This direct configuration allows users to have solid control on the application of the features in the pre- or post-encryption path.

Figure 1 illustrates how a SVTI is used.

Figure 1 *IPsec SVTI*



The IPsec VTI supports native IPsec tunneling and exhibits most of the properties of a physical interface.

Dynamic Virtual Tunnel Interfaces

DVTIs can provide highly secure and scalable connectivity for remote-access VPNs. The DVTI technology replaces dynamic crypto maps and the dynamic hub-and-spoke method for establishing tunnels.

DVTIs can be used for both the server and remote configuration. The tunnels provide an on-demand separate virtual access interface for each VPN session. The configuration of the virtual access interfaces is cloned from a virtual template configuration, which includes the IPsec configuration and any Cisco IOS software feature configured on the virtual template interface, such as QoS, NetFlow, or ACLs.

DVTIs function like any other real interface so that you can apply QoS, firewall, other security services as soon as the tunnel is active. QoS features can be used to improve the performance of various applications across the network. Any combination of QoS features offered in Cisco IOS software can be used to support voice, video, or data applications.

DVTIs provide efficiency in the use of IP addresses and provide secure connectivity. DVTIs allow dynamically downloadable per-group and per-user policies to be configured on a RADIUS server. The per-group or per-user definition can be created using extended authentication (Xauth) User or Unity group, or it can be derived from a certificate. DVTIs are standards based, so interoperability in a multiple-vendor environment is supported. IPsec DVTIs allow you to create highly secure connectivity for remote access VPNs and can be combined with Cisco Architecture for Voice, Video, and Integrated Data (AVVID) to deliver converged voice, video, and data over IP networks. The DVTI simplifies Virtual Private Network (VRF) routing and forwarding- (VRF-) aware IPsec deployment. The VRF is configured on the interface.

A DVTI requires minimal configuration on the router. A single virtual template can be configured and cloned.

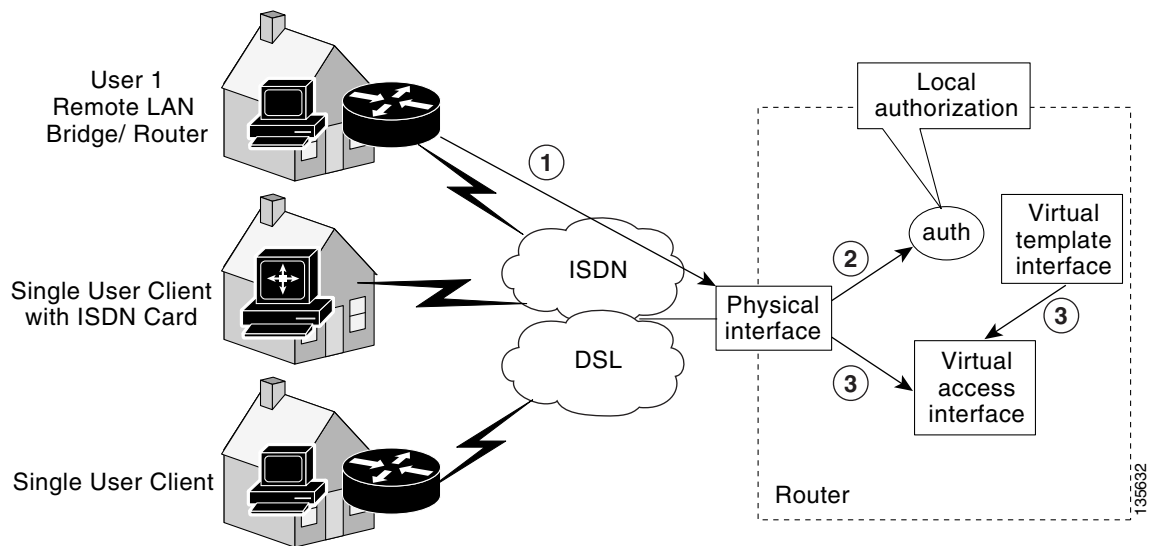
The DVTI creates an interface for IPsec sessions and uses the virtual template infrastructure for dynamic instantiation and management of dynamic IPsec VTIs. The virtual template infrastructure is extended to create dynamic virtual-access tunnel interfaces. DVTI is used in hub-and-spoke configurations. A single DVTI can support several static VTIs.

**Note**

DVTI is supported only in Easy VPNs. That is, the DVTI end must be configured as an Easy VPN server.

Figure 2 illustrates the DVTI authentication path.

Figure 2 *Dynamic IPsec VTI*



The authentication shown in Figure 2 follows this path:

1. User 1 calls the router.
2. Router 1 authenticates User 1.
3. IPsec clones virtual access interface from virtual template interface.

Dynamic Virtual Tunnel Interface Life Cycle

IPsec profiles define policy for DVTI. The dynamic interface is created at the end of IKE Phase 1 and IKE Phase 1.5. The interface is deleted when the IPsec session to the peer is closed. The IPsec session is closed when both IKE and IPsec SAs to the peer are deleted.

Routing with IPsec Virtual Tunnel Interfaces

Because VTIs are routable interfaces, routing plays an important role in the encryption process. Traffic is encrypted only if it is forwarded out of the VTI, and traffic arriving on the VTI is decrypted and routed accordingly. VTIs allow you to establish an encryption tunnel using a real interface as the tunnel endpoint. You can route to the interface or apply services such as QoS, firewalls, network address

translation, and Netflow statistics as you would to any other interface. You can monitor the interface, route to it, and it has an advantage over crypto maps because it is a real interface and provides the benefits of any other regular Cisco IOS interface.

**Note**

Dynamic routing can be used with SVTIs. Routing with DVTIs is *not* supported or recommended.

**Note**

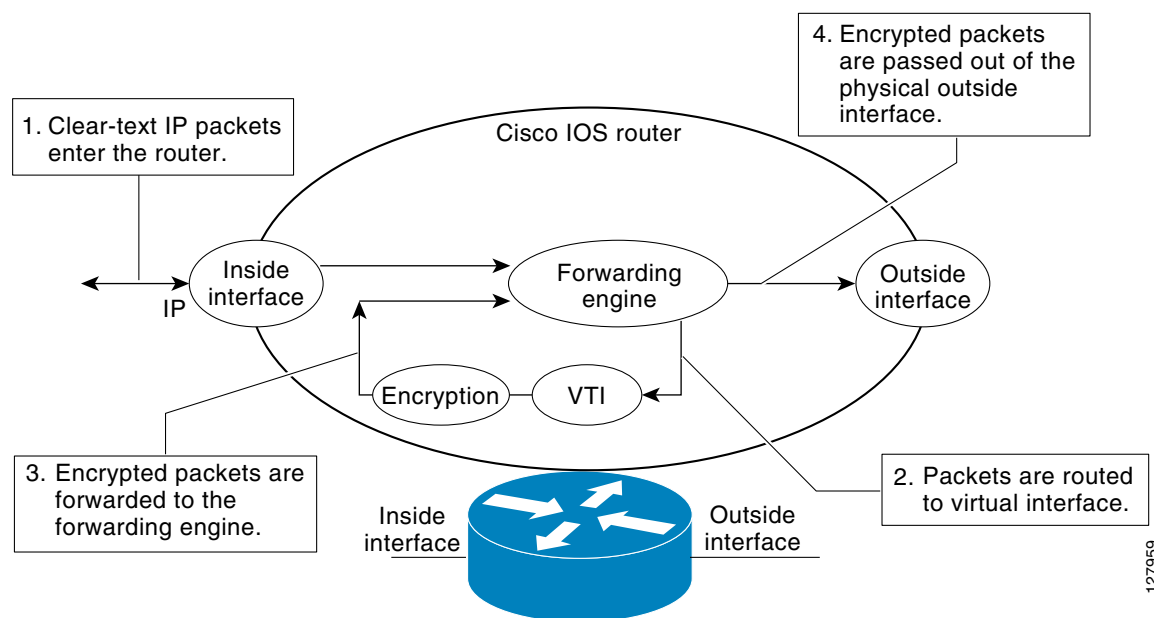
SVTI remote to DVTI interfaces are not supported.

Traffic Encryption with the IPsec Virtual Tunnel Interface

When an IPsec VTI is configured, encryption occurs in the tunnel. Traffic is encrypted when it is forwarded to the tunnel interface. Traffic forwarding is handled by the IP routing table, and dynamic or static routing can be used to route traffic to the SVTI. DVTI uses reverse route injection to further simplify the routing configurations. Using IP routing to forward the traffic to encryption simplifies the IPsec VPN configuration because the use of ACLs with a crypto map in native IPsec configurations is not required. The IPsec virtual tunnel also allows you to encrypt multicast traffic with IPsec.

IPsec packet flow into the IPsec tunnel is illustrated in [Figure 3](#).

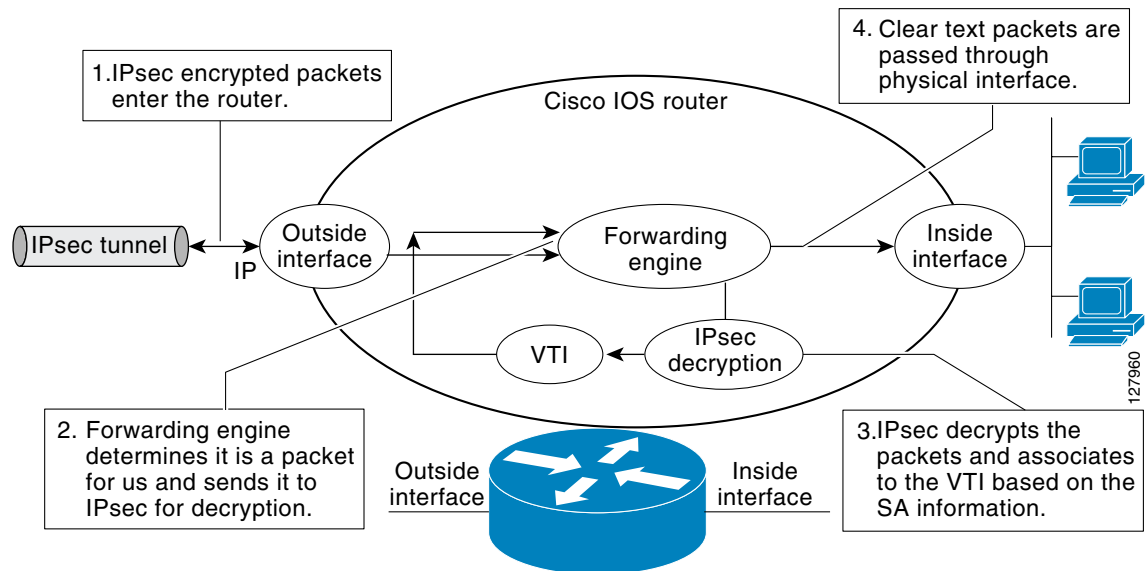
Figure 3 Packet Flow into the IPsec Tunnel



After packets arrive on the inside interface, the forwarding engine switches the packets to the VTI, where they are encrypted. The encrypted packets are handed back to the forwarding engine, where they are switched through the outside interface.

[Figure 4](#) shows the packet flow out of the IPsec tunnel.

Figure 4 Packet Flow out of the IPsec Tunnel



How to Configure IPsec Virtual Tunnel Interface

- [Configuring Static IPsec Virtual Tunnel Interfaces, page 7](#)
- [Configuring Dynamic IPsec Virtual Tunnel Interfaces, page 9](#)

Configuring Static IPsec Virtual Tunnel Interfaces

This configuration shows how to configure a static IPsec VTI.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile** *profile-name*
4. **set transform-set** *transform-set-name*
5. **interface** *type number*
6. **ip address** *address mask*
7. **tunnel mode ipsec ipv4**
8. **tunnel source** *interface*
9. **tunnel destination** *ip-address*
10. **tunnel protection IPsec profile** *profile-name* [**shared**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto IPsec profile <i>profile-name</i> Example: Router(config)# crypto IPsec profile PROF	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers.
Step 4	set transform-set <i>transform-set-name</i> [<i>transform-set-name2</i> ... <i>transform-set-name6</i>] Example: Router(config)# set transform-set tset	Specifies which transform sets can be used with the crypto map entry.
Step 5	interface <i>type number</i> Example: Router(config)# interface tunnel0	Specifies the interface on which the tunnel will be configured and enters interface configuration mode.
Step 6	ip address <i>address mask</i> Example: Router(config-if)# ip address 10.1.1.1 255.255.255.0	Specifies the IP address and mask.
Step 7	tunnel mode ipsec ipv4 Example: Router(config-if)# tunnel mode ipsec ipv4	Defines the mode for the tunnel.
Step 8	tunnel source <i>interface</i> Example: Router(config-if)# tunnel source loopback0	Specifies the tunnel source as a loopback interface.

	Command or Action	Purpose
Step 9	tunnel destination <i>ip-address</i> Example: Router(config-if)# tunnel destination 172.16.1.1	Identifies the IP address of the tunnel destination.
Step 10	tunnel protection IPsec profile <i>profile-name</i> [shared] Example: Router(config-if)# tunnel protection IPsec profile PROF	Associates a tunnel interface with an IPsec profile.

Configuring Dynamic IPsec Virtual Tunnel Interfaces

This task shows how to configure a dynamic IPsec VTI.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile** *profile-name*
4. **set transform-set** *transform-set-name*
5. **interface virtual-template** *number*
6. **tunnel mode** *mode*
7. **tunnel protection IPsec profile** *profile-name* [**shared**]
8. **exit**
9. **crypto isakamp profile** *profile-name*
10. **virtual-template** *template-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	crypto IPsec profile <i>profile-name</i> Example: Router(config)# crypto IPsec profile PROF	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers.
Step 4	set transform-set <i>transform-set-name</i> [<i>transform-set-name2</i> ... <i>transform-set-name6</i>] Example: Router(config)# set transform-set tset	Specifies which transform sets can be used with the crypto map entry.
Step 5	interface virtual-template <i>number</i> Example: Router(config)# interface virtual-template 2	Defines a virtual-template tunnel interface and enters interface configuration mode.
Step 6	tunnel mode ipsec ipv4 Example: Router(config-if)# tunnel mode ipsec ipv4	Defines the mode for the tunnel.
Step 7	tunnel protection IPsec profile <i>profile-name</i> [<i>shared</i>] Example: Router(config-if)# tunnel protection IPsec profile PROF	Associates a tunnel interface with an IPsec profile.
Step 8	exit Example: Router(config-if)# exit	Exits interface configuration mode.
Step 9	crypto isakamp profile <i>profile-name</i> Example: Router(config)# crypto isakamp profile red	Defines the ISAKAMP profile to be used for the virtual template.
Step 10	virtual-template <i>template-number</i> Example: Router(config)# virtual-template 1	Specifies the virtual template attached to the ISAKAMP profile.

Configuration Examples for IPsec Virtual Tunnel Interface

The following examples are provided to illustrate configuration scenarios for IPsec VTIs:

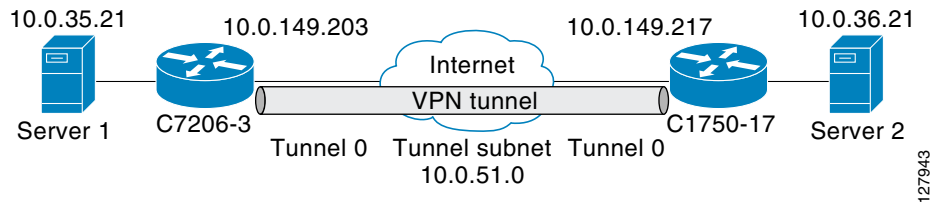
- [Static Virtual Tunnel Interface with IPsec: Example, page 11](#)
- [VRF-Aware Static Virtual Tunnel Interface: Example, page 14](#)
- [Static Virtual Tunnel Interface with QoS: Example, page 14](#)
- [Static Virtual Tunnel Interface with Virtual Firewall: Example, page 15](#)

- [Dynamic Virtual Tunnel Interface Easy VPN Server: Example, page 16](#)
- [Dynamic Virtual Tunnel Interface Easy VPN Client: Example, page 18](#)
- [VRF-Aware IPsec with Dynamic VTI: Example, page 20](#)
- [Dynamic Virtual Tunnel Interface with Virtual Firewall: Example, page 20](#)
- [Dynamic Virtual Tunnel Interface with QoS: Example, page 21](#)

Static Virtual Tunnel Interface with IPsec: Example

The following example configuration uses a preshared key for authentication between peers. VPN traffic is forwarded to the IPsec VTI for encryption and then sent out the physical interface. The tunnel on subnet 10 checks packets for IPsec policy and passes them to the Crypto Engine (CE) for IPsec encapsulation. [Figure 5](#) illustrates the IPsec VTI configuration.

Figure 5 VTI with IPsec



C7206 Router Configuration

```

version 12.3

service timestamps debug datetime
service timestamps log datetime
hostname 7200-3
no aaa new-model
ip subnet-zero
ip cef
controller ISA 6/1
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
group 2
crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto IPsec transform-set T1 esp-3des esp-sha-hmac
crypto IPsec profile P1
set transform-set T1
!

interface Tunnel0
  ip address 10.0.51.203 255.255.255.0
  ip ospf mtu-ignore
  load-interval 30
  tunnel source 10.0.149.203
  tunnel destination 10.0.149.217
  tunnel mode IPsec ipv4
  tunnel protection IPsec profile P1

```

```

!
interface Ethernet3/0
 ip address 10.0.149.203 255.255.255.0
 duplex full
!
interface Ethernet3/3
 ip address 10.0.35.203 255.255.255.0
 duplex full
!
ip classless
ip route 10.0.36.0 255.255.255.0 Tunnel0
line con 0
line aux 0
line vty 0 4
end

```

C1750 Router Configuration

```

version 12.3

hostname c1750-17
no aaa new-model
ip subnet-zero
ip cef
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2

crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto IPsec transform-set T1 esp-3des esp-sha-hmac
crypto IPsec profile P1
 set transform-set T1
!
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0
 ip ospf mtu-ignore
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
!
interface FastEthernet0/0
 ip address 10.0.149.217 255.255.255.0
 speed 100
 full-duplex
!
interface Ethernet1/0
 ip address 10.0.36.217 255.255.255.0
 load-interval 30
 full-duplex
!

ip classless
ip route 10.0.35.0 255.255.255.0 Tunnel0
line con 0
line aux 0
line vty 0 4
end

```

Verifying the Results for the IPsec Static Virtual Tunnel Interface: Example

This section provides information that you can use to confirm that your configuration is working properly. In this display, Tunnel 0 is “up,” and the line protocol is “up.” If the line protocol is “down,” the session is not active.

Verifying the C7206 Status

```
Router# show interface tunnel 0
```

```
Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 10.0.51.203/24
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
reliability 255/255, txload 103/255, rxload 110/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.0.149.203, destination 10.0.149.217
Tunnel protocol/transport IPsec/IP, key disabled, sequencing disabled
Tunnel TTL 255

Checksumming of packets disabled, fast tunneling enabled
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPsec (profile "P1")
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
30 second input rate 13000 bits/sec, 34 packets/sec
30 second output rate 36000 bits/sec, 34 packets/sec
191320 packets input, 30129126 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
59968 packets output, 15369696 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

```
Router# show crypto session
```

```
Crypto session current status
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.149.217 port 500
IKE SA: local 10.0.149.203/500 remote 10.0.149.217/500 Active
IPsec FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 4, origin: crypto map
```

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.35.0/24 is directly connected, Ethernet3/3
S 10.0.36.0/24 is directly connected, Tunnel0
```

```
C 10.0.51.0/24 is directly connected, Tunnel0
C 10.0.149.0/24 is directly connected, Ethernet3/0
```

VRF-Aware Static Virtual Tunnel Interface: Example

To add VRF to the static VTI example, include the **ip vrf** and **ip vrf forwarding** commands to the configuration as shown in the following example.

C7206 Router Configuration

```
hostname c7206
.
.
ip vrf sample-vti1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
.
.
interface Tunnel0
  ip vrf forwarding sample-vti1
  ip address 10.0.51.217 255.255.255.0
  tunnel source 10.0.149.217
  tunnel destination 10.0.149.203
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile P1
.
.
!
end
```

Static Virtual Tunnel Interface with QoS: Example

You can apply any QoS policy to the tunnel endpoint by including the **service-policy** statement under the tunnel interface. The following example is policing traffic out the tunnel interface.

C7206 Router Configuration

```
hostname c7206
.
.
class-map match-all VTI
  match any
!
policy-map VTI
  class VTI
    police cir 2000000
      conform-action transmit
      exceed-action drop
!
.
.
interface Tunnel0
  ip address 10.0.51.217 255.255.255.0
  tunnel source 10.0.149.217
  tunnel destination 10.0.149.203
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile P1
```

```

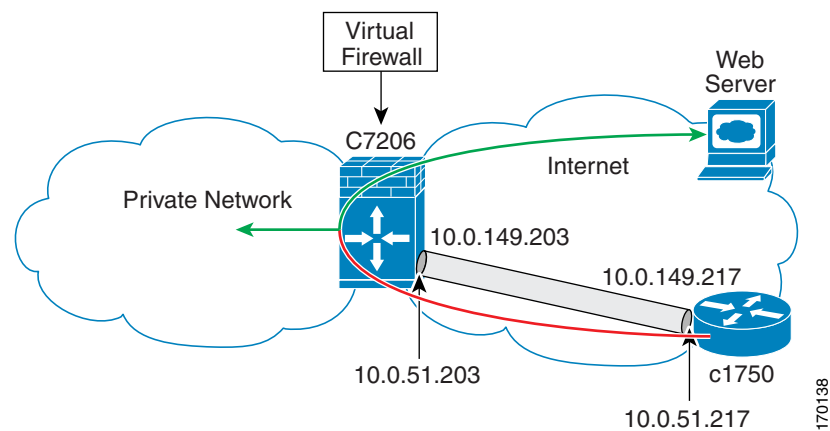
service-policy output VTI
!
.
.
!
end

```

Static Virtual Tunnel Interface with Virtual Firewall: Example

Applying the virtual firewall to the SVTI tunnel allows traffic from the spoke to pass through the hub to reach the internet. [Figure 6](#) illustrates a SVTI with the spoke protected inherently by the corporate firewall.

Figure 6 Static VTI with Virtual Firewall



The basic SVTI configuration has been modified to include the virtual firewall definition.

C7206 Router Configuration

```

hostname c7206
.
.
ip inspect max-incomplete high 1000000
ip inspect max-incomplete low 800000
ip inspect one-minute high 1000000
ip inspect one-minute low 800000
ip inspect tcp synwait-time 60
ip inspect tcp max-incomplete host 100000 block-time 2
ip inspect name IOSFW1 tcp timeout 300
ip inspect name IOSFW1 udp
!
.
.
interface GigabitEthernet0/1
description Internet Connection
ip address 172.18.143.246 255.255.255.0
ip access-group 100 in
ip nat outside
!
interface Tunnel0
ip address 10.0.51.217 255.255.255.0
ip nat inside

```

```

ip inspect IOSFW1 in
tunnel source 10.0.149.217
tunnel destination 10.0.149.203
tunnel mode ipsec ipv4
tunnel protection ipsec profile P1
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
ip nat translation timeout 120
ip nat translation finrst-timeout 2
ip nat translation max-entries 300000
ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0
ip nat inside source list 110 pool test1 vrf test-vti1 overload
!
access-list 100 permit esp any any
access-list 100 permit udp any eq isakmp any
access-list 100 permit udp any eq non500-isakmp any
access-list 100 permit icmp any any
access-list 110 deny esp any any
access-list 110 deny udp any eq isakmp any
access-list 110 permit ip any any
access-list 110 deny udp any eq non500-isakmp any
!
end

```

Dynamic Virtual Tunnel Interface Easy VPN Server: Example

The following example illustrates the use of the DVTI Easy VPN server, which serves as an IPsec remote access aggregator. The client can be a home user running a Cisco VPN client or it can be a Cisco IOS router configured as an Easy VPN client.

C7206 Router Configuration

```

hostname c7206
!
aaa new-model
aaa authentication login local_list local
aaa authorization network local_list local
aaa session-id common
!
ip subnet-zero
ip cef
!
username cisco password 0 cisco123
!
controller ISA 1/1
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp client configuration group group1
  key cisco123
  pool group1pool
  save-password
!
crypto isakmp profile vpn1-ra
  match identity group group1
  client authentication list local_list

```



```

isakmp authorization list local_list
client configuration address respond
virtual-template 1
!
crypto ipsec transform-set VTI-TS esp-3des esp-sha-hmac
!
crypto ipsec profile test-vti1
set transform-set VTI-TS
!
interface GigabitEthernet0/1
description Internet Connection
ip address 172.18.143.246 255.255.255.0
!
interface GigabitEthernet0/2
description Internal Network
ip address 10.2.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
ip unnumbered GigabitEthernet0/1
ip virtual-reassembly
tunnel mode ipsec ipv4
tunnel protection ipsec profile test-vti1
!
ip local pool group1pool 192.168.1.1 192.168.1.4
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
end

```

Verifying the Results for the Dynamic Virtual Tunnel Interface Easy VPN Server: Example

The following examples show that a DVTI has been configured for an Easy VPN server.

Router# **show running-config interface Virtual-Access2**

Building configuration...

```

Current configuration : 250 bytes
!
interface Virtual-Access2
ip unnumbered GigabitEthernet0/1
ip virtual-reassembly
tunnel source 172.18.143.246
tunnel destination 172.18.143.208
tunnel mode ipsec ipv4
tunnel protection ipsec profile test-vti1
no tunnel protection ipsec initiate
end

```

Router# **show ip route**

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

```

Gateway of last resort is 10.2.1.10 to network 0.0.0.0

```

      172.18.0.0/24 is subnetted, 1 subnets
C       172.18.143.0 is directly connected, GigabitEthernet0/1

```

```

    192.168.1.0/32 is subnetted, 1 subnets
S       192.168.1.1 [1/0] via 0.0.0.0, Virtual-Access2
    10.0.0.0/24 is subnetted, 1 subnets
C       10.2.1.0 is directly connected, GigabitEthernet0/2
S*    0.0.0.0/0 [1/0] via 172.18.143.1

```

Dynamic Virtual Tunnel Interface Easy VPN Client: Example

The following example shows how you can set up a router as the Easy VPN client. This example uses basically the same idea as the Easy VPN client that you can run from a PC to connect. In fact, the configuration of the Easy VPN server will work for the software client or the Cisco IOS client.

```

hostname c1841
!
no aaa new-model
!
ip cef
!
username cisco password 0 cisco123
!
crypto ipsec client ezvpn CLIENT
  connect manual
  group group1 key cisco123
  mode client
  peer 172.18.143.246
  virtual-interface 1
  username cisco password cisco123
  xauth userid mode local
!
interface Loopback0
  ip address 10.1.1.1 255.255.255.255
!
interface FastEthernet0/0
  description Internet Connection
  ip address 172.18.143.208 255.255.255.0
  crypto ipsec client ezvpn CLIENT
!
interface FastEthernet0/1
  ip address 10.1.1.252 255.255.255.0
  crypto ipsec client ezvpn CLIENT inside
!
interface Virtual-Template1 type tunnel
  ip unnumbered Loopback0
!
ip route 0.0.0.0 0.0.0.0 172.18.143.1 254
!
end

```

The client definition can be set up in many different ways. The mode specified with the **connect** command can be automatic or manual. If the connect mode is set to manual, the IPsec tunnel has to be initiated manually by a user.

Also note use of the **mode** command. The mode can be client, network-extension, or network-extension-plus. This example indicates client mode, which means that the client is given a private address from the server. Network-extension mode is different from client mode in that the client specifies for the server its attached private subnet. Depending on the mode, the routing table on either end will be slightly different. The basic operation of the IPsec tunnel remains the same, regardless of the specified mode.

Verifying the Results for the Dynamic Virtual Tunnel Interface Easy VPN Client: Example

The following examples illustrate different ways to display the status of the DVTI.

```
Router# show running-config interface Virtual-Access2
```

```
Building configuration...
```

```
Current configuration : 148 bytes
!
interface Virtual-Access2
 ip unnumbered Loopback1
 tunnel source FastEthernet0/0
 tunnel destination 172.18.143.246
 tunnel mode ipsec ipv4
end
```

```
Router# show running-config interface Loopback1
```

```
Building configuration...
```

```
Current configuration : 65 bytes
!
interface Loopback1
 ip address 192.168.1.1 255.255.255.255
end
```

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 172.18.143.1 to network 0.0.0.0
```

```
    10.0.0.0/32 is subnetted, 1 subnets
C       10.1.1.1 is directly connected, Loopback0
    172.18.0.0/24 is subnetted, 1 subnets
C       172.18.143.0 is directly connected, FastEthernet0/0
    192.168.1.0/32 is subnetted, 1 subnets
C       192.168.1.1 is directly connected, Loopback1
S*    0.0.0.0/0 [1/0] via 0.0.0.0, Virtual-Access2
```

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 6
```

```
Tunnel name : CLIENT
Inside interface list: FastEthernet0/1
Outside interface: Virtual-Access2 (bound to FastEthernet0/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.1.1
Mask: 255.255.255.255
Save Password: Allowed
Current EzVPN Peer: 172.18.143.246
```

VRF-Aware IPsec with Dynamic VTI: Example

This example shows how to configure VRF-Aware IPsec to take advantage of the DVTI:

```
hostname c7206
.
.
ip vrf test-vti1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
.
.
interface Virtual-Template1 type tunnel
  ip vrf forwarding test-vti1
  ip unnumbered Loopback0
  ip virtual-reassembly
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile test-vti1
!
.
.
end
```

Dynamic Virtual Tunnel Interface with Virtual Firewall: Example

The DVTI Easy VPN server can be configured behind a virtual firewall. Behind-the-firewall configuration allows users to enter the network, while the network firewall is protected from unauthorized access. The virtual firewall uses Context-Based Access Control (CBAC) and NAT applied to the Internet interface as well as to the virtual template.

```
hostname c7206
.
.
ip inspect max-incomplete high 1000000
ip inspect max-incomplete low 800000
ip inspect one-minute high 1000000
ip inspect one-minute low 800000
ip inspect tcp synwait-time 60
ip inspect tcp max-incomplete host 100000 block-time 2
ip inspect name IOSFW1 tcp timeout 300
ip inspect name IOSFW1 udp
!
.
.
interface GigabitEthernet0/1
  description Internet Connection
  ip address 172.18.143.246 255.255.255.0
  ip access-group 100 in
  ip nat outside
!
interface GigabitEthernet0/2
  description Internal Network
  ip address 10.2.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
  ip unnumbered Loopback0
  ip nat inside
  ip inspect IOSFW1 in
```

```

tunnel mode ipsec ipv4
tunnel protection ipsec profile test-vti1
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
ip nat translation timeout 120
ip nat translation finrst-timeout 2
ip nat translation max-entries 300000
ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0
ip nat inside source list 110 pool test1 vrf test-vti1 overload
!
access-list 100 permit esp any any
access-list 100 permit udp any eq isakmp any
access-list 100 permit udp any eq non500-isakmp any
access-list 100 permit icmp any any
access-list 110 deny esp any any
access-list 110 deny udp any eq isakmp any
access-list 110 permit ip any any
access-list 110 deny udp any eq non500-isakmp any
!
end

```

Dynamic Virtual Tunnel Interface with QoS: Example

You can add QoS to the DVTI tunnel by applying the service policy to the virtual template. When the template is cloned to make the virtual-access interface, the service policy will be applied there. The following example shows the basic DVTI configuration with QoS added.

```

hostname c7206
.
.
class-map match-all VTI
match any
!
policy-map VTI
class VTI
police cir 2000000
conform-action transmit
exceed-action drop
!
.
.
interface Virtual-Templat1 type tunnel
ip vrf forwarding test-vti1
ip unnumbered Loopback0
ip virtual-reassembly
tunnel mode ipsec ipv4
tunnel protection ipsec profile test-vti1
service-policy output VTI
!
.
.
!
end

```

Additional References

The following sections provide references related to IPsec virtual tunnel interface.

Related Documents

Related Topic	Document Title
IPsec, security issues	Configuring Security for VPNs with IPsec
QoS, configuring	Cisco IOS Quality of Service Solutions Configuration Guide on Cisco.com
Security commands	Cisco IOS Security Command Reference
VPN configuration	<ul style="list-style-type: none"> • Cisco Easy VPN Remote • Easy VPN Server

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFC	Title
RFC 2401	Security Architecture for the Internet Protocol
RFC 2408	Internet Security Association and Key Management Protocol
RFC 2409	The Internet Key Exchange (IKE)

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

- **crypto isakmp profile**
- **interface virtual-template**
- **show vtemplate**
- **tunnel mode**
- **virtual-template**

Feature Information for IPsec Virtual Tunnel Interface

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for IPsec Virtual Tunnel Interface

Feature Name	Releases	Feature Configuration Information
Static IPsec VTIs	12.3(7)T 12.3(14)T 12.2(33)SRA 12.2(33)SXH	IPsec VTIs (VTIs) provide a routable interface type for terminating IPsec tunnels and an easy way to define protection between sites to form an overlay network. IPsec VTIs simplify configuration of IPsec for protection of remote links, support multicast, and simplify network management and load balancing.
Dynamic IPsec VTIs	12.3(7)T 12.3(14)T	Dynamic VTIs provide efficiency in the use of IP addresses and provide secure connectivity. Dynamic VTIs allow dynamically downloadable per-group and per-user policies to be configured on a RADIUS server. The per-group or per-user definition can be created using Xauth User or Unity group, or it can be derived from a certificate. Dynamic VTIs are standards based, so interoperability in a multiple-vendor environment is supported. IPsec dynamic VTIs allow you to create highly secure connectivity for remote access VPNs and can be combined with Cisco Architecture for Voice, Video, and Integrated Data (AVVID) to deliver converged voice, video, and data over IP networks. The dynamic VTI simplifies VRF-aware IPsec deployment. The VRF is configured on the interface.
IPSec Virtual Tunnel Interface	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2004–2009 Cisco Systems, Inc. All rights reserved.



SafeNet IPsec VPN Client Support

The SafeNet IPsec VPN Client Support feature allows you to limit the scope of an Internet Security Association and Key Management Protocol (ISAKMP) profile or ISAKMP keyring configuration to a local termination address or interface. The benefit of this feature is that different customers can use the same peer identities and ISAKMP keys by using different local termination addresses.

History for the SafeNet IPsec VPN Client Support Feature

Release	Modification
12.3(14)T	This feature was introduced.
12.2(18)SXE	This feature was integrated into Cisco IOS Release 12.2(18)SXE.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for SafeNet IPsec VPN Client Support, page 2](#)
- [Restrictions for SafeNet IPsec VPN Client Support, page 2](#)
- [Information About SafeNet IPsec VPN Client Support, page 2](#)
- [How to Configure SafeNet IPsec VPN Client Support, page 3](#)
- [Configuration Examples for SafeNet IPsec VPN Client Support, page 7](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for SafeNet IPsec VPN Client Support

- You must understand how to configure ISAKMP profiles and ISAKMP keyrings.

Restrictions for SafeNet IPsec VPN Client Support

- The local address option works only for the primary address of an interface.
- If an IP address is provided, the administrator has to ensure that the connection of the peer terminates to the address that is provided.
- If the IP address does not exist on the device, or if the interface does not have an IP address, the ISAKMP profile or ISAKMP keyring will be effectively disabled.

Information About SafeNet IPsec VPN Client Support

Before configuring SafeNet IPsec VPN Client Support, you should understand the following concepts:

- [ISAKMP Profile and ISAKMP Keyring Configurations: Background, page 2](#)
- [Local Termination Address or Interface, page 2](#)

ISAKMP Profile and ISAKMP Keyring Configurations: Background

Prior to Cisco IOS Release 12.3(14)T, ISAKMP-profile and ISAKMP-keyring configurations could be only global, meaning that the scope of these configurations could not be limited by any locally defined parameters (VRF instances were an exception). For example, if an ISAKMP keyring contained a preshared key for address 10.11.12.13, the same key would be used if the peer had the address 10.11.12.13, irrespective of the interface or local address to which the peer was connected. There are situations, however, in which users prefer that associate keyrings be bound not only with virtual route forwarding (VRF) instances but also to a particular interface. For example, if instead of VRF instances, there are virtual LANS, and the Internet Key Exchange (IKE) is negotiated with a group of peers using one fixed virtual LAN (VLAN) interface. Such a group of peers uses a single preshared key, so if keyrings could be bound to an interface, it would be easy to define a wildcard key without risking that the keys would also be used for other customers.

Sometimes the identities of the peer are not in the control of the administrator, and even if the same peer negotiates for different customers, the local termination address is the only way to distinguish the peer. After such a distinction is made, if the traffic is sent to different VRF instances, configuring an ISAKMP profile is the only way to distinguish the peer. Unfortunately, when the peer uses an identical identity for all such situations, the ISAKMP profile cannot distinguish among the negotiations. For such scenarios, it would be beneficial to bind ISAKMP profiles to a local termination address. If a local termination address could be assigned, identical identities from the peer would not be a problem.

Local Termination Address or Interface

Effective with Cisco IOS Release 12.3(14)T, the SafeNet IPsec VPN Client Support feature allows you to limit the scope of ISAKMP profiles and ISAKMP keyrings to a local termination address or interface.

Benefit of SafeNet IPsec VPN Client Support

The benefit of this feature is that different customers can use the same peer identities and ISAKMP keys by using different local termination addresses.

How to Configure SafeNet IPsec VPN Client Support

This section contains the following procedures. The first two configurations are independent of each other.

- [Limiting an ISAKMP Profile to a Local Termination Address or Interface, page 3](#) (required)
- [Limiting a Keyring to a Local Termination Address or Interface, page 4](#) (required)
- [Monitoring and Maintaining SafeNet IPsec VPN Client Support, page 5](#) (optional)
- [Examples, page 6](#) (optional)

Limiting an ISAKMP Profile to a Local Termination Address or Interface

To configure an ISAKMP profile and limit it to a local termination address or interface, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **keyring** *keyring-name*
5. **match identity address** *address*
6. **local-address** { *interface-name* | *ip-address* [*vrf-tag*] }

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	crypto isakmp profile <i>profile-name</i> Example: Router (config)# crypto isakmp profile profile1	Defines an ISAKMP profile and enters ISAKMP profile configuration mode.
Step 4	keyring <i>keyring-name</i> Example: Router (conf-isa-profile)# keyring keyring1	(Optional) Configures a keyring with an ISAKMP profile. <ul style="list-style-type: none"> A keyring is not needed inside an ISAKMP profile for local termination to work. Local termination works even if Rivest, Shamir, and Adelman (RSA) certificates are used.
Step 5	match identity address <i>address</i> Example: Router (conf-isa-profile)# match identity address 10.0.0.0 255.0.0.0	Matches an identity from a peer in an ISAKMP profile.
Step 6	local-address { <i>interface-name</i> <i>ip-address</i> [<i>vrf-tag</i>]} Example: Router (conf-isa-profile)# local-address serial2/0	Limits the scope of an ISAKMP profile or an ISAKMP keyring configuration to a local termination address or interface.

Limiting a Keyring to a Local Termination Address or Interface

To configure an ISAKMP keyring and limit its scope to a local termination address or interface, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto keyring** *keyring-name*
4. **local-address** {*interface-name* | *ip-address* [*vrf-tag*]}
5. **pre-shared-key** *address address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto keyring <i>keyring-name</i> Example: Router (config)# crypto keyring keyring1	Defines a crypto keyring to be used during IKE authentication and enters keyring configuration mode.
Step 4	local-address { <i>interface-name</i> <i>ip-address</i> [<i>vrf-tag</i>]} Example: Router (conf-keyring)# local-address serial2/0	Limits the scope of an ISAKMP profile or an ISAKMP keyring configuration to a local termination address or interface.
Step 5	pre-shared-key address <i>address</i> Example: Router (conf-keyring)# pre-shared-key address 10.0.0.1	Defines a preshared key to be used for IKE authentication.

Monitoring and Maintaining SafeNet IPsec VPN Client Support

The following **debug** and **show** commands may be used to monitor and maintain the configuration in which you limited the scope of an ISAKMP profile or ISAKMP keyring to a local termination address or interface.

SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp**
3. **show crypto isakmp profile**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug crypto isakmp Example: Router# debug crypto isakmp	Displays messages about IKE events.
Step 3	show crypto isakmp profile Example: Router# show crypto isakmp profile	Lists all the ISAKMP profiles that are defined on a router.

Examples

debug crypto isakmp Command Output for an ISAKMP Keyring That Is Bound to Local Termination Addresses: Example

You have an ISAKMP configuration as follows (the address of serial2/0 is 10.0.0.1, and the address of serial2/1 is 10.0.0.2),

```
crypto keyring keyring1
! Scope of the keyring is limited to interface serial2/0.
local-address serial2/0
! The following is the key string used by the peer.
pre-shared-key address 10.0.0.3 key somerandomkeystring
crypto keyring keyring2
local-address serial2/1
! The following is the keystring used by the peer coming into serial2/1.
pre-shared-key address 10.0.0.3 key someotherkeystring
```

and if the connection is coming into serial2/0, keyring1 is chosen as the source of the preshared key (and keyring2 is ignored because it is bound to serial2/1), you would see the following output:

```
Router# debug crypto isakmp

*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0):Keyring keyring2 is bound to
10.0.0.0, skipping
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0):Looking for a matching key for
10.0.0.3 in keyring1
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0): : success
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0):found peer pre-shared key
matching 10.0.0.3
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0): local preshared key found
```

debug crypto isakmp Command Output for an ISAKMP Profile That Is Bound to a Local Termination Address: Example

If you have the following configuration,

```
crypto isakmp profile profile1
```



```
keyring keyring1
match identity address 10.0.0.0 255.0.0.0
local-address serial2/0
crypto isakmp profile profile2
keyring keyring1
keyring keyring2
self-identity fqdn
match identity address 10.0.0.1 255.255.255.255
local-address serial2/1
```

and the connection is coming through the local terminal address serial2/0, you will see the following output:

```
Router# debug crypto isakmp
```

```
*Feb 11 15:01:29.935: ISAKMP: (0:0:N/A:0):
```

```
Profile profile2 bound to 10.0.0.0 skipped
```

```
*Feb 11 15:01:29.935: ISAKMP: (0:1:SW:1):: peer matches profile1 profile
```

show crypto isakmp profile Command Output: Example

The following is an example of typical **show** command output for an ISAKMP profile that is bound to serial2/0:

```
Router# show crypto isakmp profile
```

```
ISAKMP PROFILE profile1
Identities matched are:
  ip-address 10.0.0.0 255.0.0.0
Certificate maps matched are:
keyring(s): keyring1
trustpoint(s): <all>
Interface binding: serial2/0 (10.20.0.1:global)
```

Troubleshooting SafeNet IPsec VPN Client Support

If an ISAKMP profile or ISAKMP keyring fails to be selected, you should double-check the local-address binding in the ISAKMP profile or ISAKMP keyring configuration and follow the output of the IKE debugs to determine whether the peer is correctly terminating on the address. You may remove the local-address binding (to make the scope of the profile or keyring global) and check to determine whether the profile or keyring is selected to confirm the situation.

Configuration Examples for SafeNet IPsec VPN Client Support

This section contains the following configuration, **debug** command, and **show** command examples.

- [ISAKMP Profile Bound to a Local Interface: Example, page 8](#)
- [ISAKMP Keyring Bound to a Local Interface: Example, page 8](#)
- [ISAKMP Keyring Bound to a Local IP Address: Example, page 8](#)
- [ISAKMP Keyring Bound to an IP Address and Limited to a VRF: Example, page 8](#)

ISAKMP Profile Bound to a Local Interface: Example

The following example shows that the ISAKMP profile is bound to a local interface:

```
crypto isakmp profile profile1
  keyring keyring1
  match identity address 10.0.0.0 255.0.0.0
  local-address serial2/0
```

ISAKMP Keyring Bound to a Local Interface: Example

The following example shows that the ISAKMP keyring is bound only to interface serial2/0:

```
crypto keyring
  local-address serial2/0
  pre-shared-key address 10.0.0.1
```

ISAKMP Keyring Bound to a Local IP Address: Example

The following example shows that the ISAKMP keyring is bound only to IP address 10.0.0.2:

```
crypto keyring keyring1
  local-address 10.0.0.2
  pre-shared-key address 10.0.0.2 key
```

ISAKMP Keyring Bound to an IP Address and Limited to a VRF: Example

The following example shows that an ISAKMP keyring is bound to IP address 10.34.35.36 and that the scope is limited to VRF examplevrf1:

```
ip vrf examplevrf1
  rd 12:3456
crypto keyring ring1
  local-address 10.34.35.36 examplevrf1
interface ethernet2/0
  ip vrf forwarding examplevrf1
  ip address 10.34.35.36 255.255.0.0
```

Additional References

The following sections provide references related to SafeNet IPsec VPN Client Support.

Related DocumentsStandards

Related Topic	Document Title
Configuring ISAKMP profiles and ISAKMP keyrings	VRF-Aware IPsec
Security commands	Cisco IOS Security Command Reference

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features

- **local-address**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream,

Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2009 Cisco Systems, Inc. All rights reserved.



Crypto Conditional Debug Support

The Crypto Conditional Debug Support feature introduces three new command-line interfaces (CLIs) that allow users to debug an IP Security (IPSec) tunnel on the basis of predefined crypto conditions such as the peer IP address, connection-ID of a crypto engine, and security parameter index (SPI). By limiting debug messages to specific IPSec operations and reducing the amount of debug output, users can better troubleshoot a router with a large number of tunnels.

Feature History for Crypto Conditional Debug Support

Feature History	
Release	Modification
12.3(2)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Crypto Conditional Debug Support, page 2](#)
- [Restrictions for Crypto Conditional Debug Support, page 2](#)
- [Information About Crypto Conditional Debug Support, page 2](#)
- [How to Enable Crypto Conditional Debug Support, page 3](#)
- [Configuration Examples for the Crypto Conditional Debug CLIs, page 6](#)
- [Additional References, page 8](#)
- [Command Reference, page 8](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Crypto Conditional Debug Support

To use the new crypto CLIs, you must be using a crypto image, such as the k8 or k9 subsystem.

Restrictions for Crypto Conditional Debug Support

- This feature does not support debug message filtering for hardware crypto engines.
- Although conditional debugging is useful for troubleshooting peer-specific or functionality related Internet Key Exchange (IKE) and IPSec problems, conditional debugging may not be able to define and check large numbers of debug conditions.

Because extra space is needed to store the debug condition values, additional processing overhead is added to the CPU and memory usage is increased. Thus, enabling crypto conditional debugging on a router with heavy traffic should be used with caution.

Information About Crypto Conditional Debug Support

To enable the conditional crypto debug commands, you should understand the following concept:

- [Supported Condition Types, page 2](#)

Supported Condition Types

The new crypto conditional debug CLIs—**debug crypto condition**, **debug crypto condition unmatched**, and **show crypto debug-condition**—allow you to specify conditions (filter values) in which to generate and display debug messages related only to the specified conditions. [Table 1](#) lists the supported condition types.

Table 1 *Supported Condition Types for Crypto Debug CLI*

Condition Type (Keyword)	Description
connid ¹	An integer between 1–32766. Relevant debug messages will be shown if the current IPSec operation uses this value as the connection ID to interface with the crypto engine.
flowid ¹	An integer between 1–32766. Relevant debug messages will be shown if the current IPSec operation uses this value as the flow-ID to interface with the crypto engine.
FVRF	The name string of a virtual private network (VPN) routing and forwarding (VRF) instance. Relevant debug messages will be shown if the current IPSec operation uses this VRF instance as its front-door VRF (FVRF).

Table 1 **Supported Condition Types for Crypto Debug CLI (continued)**

Condition Type (Keyword)	Description
IVRF	The name string of a VRF instance. Relevant debug messages will be shown if the current IPsec operation uses this VRF instance as its inside VRF (IVRF).
peer group	A Unity group-name string. Relevant debug messages will be shown if the peer is using this group name as its identity.
peer hostname	A fully qualified domain name (FQDN) string. Relevant debug messages will be shown if the peer is using this string as its identity; for example, if the peer is enabling IKE Xauth with this FQDN string.
peer ipaddress	A single IP address. Relevant debug messages will be shown if the current IPsec operation is related to the IP address of this peer.
peer subnet	A subnet and a subnet mask that specify a range of peer IP addresses. Relevant debug messages will be shown if the IP address of the current IPsec peer falls into the specified subnet range.
peer username	A username string. Relevant debug messages will be shown if the peer is using this username as its identity; for example, if the peer is enabling IKE Extended Authentication (Xauth) with this username.
SPI ¹	A 32-bit unsigned integer. Relevant debug messages will be shown if the current IPsec operation uses this value as the SPI.

1. If an IPsec connid, flowid, or SPI is used as a debug condition, the debug messages for a related IPsec flow are generated. An IPsec flow has two connids, flowids, and SPIs—one inbound and one outbound. Both two connids, flowids, and SPIs can be used as the debug condition that triggers debug messages for the IPsec flow.

How to Enable Crypto Conditional Debug Support

This section contains the following procedures:

- [Enabling Crypto Conditional Debug Messages, page 3](#)
- [Enabling Crypto Error Debug Messages, page 5](#)

Enabling Crypto Conditional Debug Messages

To enable crypto conditional debug filtering, you must perform the following tasks.

Performance Considerations

- Before enabling crypto conditional debugging, you must decide what debug condition types (also known as debug filters) and values will be used. The volume of debug messages is dependent on the number of conditions you define.



Note Specifying numerous debug conditions may consume CPU cycles and negatively affect router performance.

- Your router will perform conditional debugging only after at least one of the global crypto debug commands—**debug crypto isakmp**, **debug crypto ipsec**, and **debug crypto engine**—has been enabled. This requirement helps to ensure that the performance of the router will not be impacted when conditional debugging is not being used.

Disable Crypto Debug Conditions

If you choose to disable crypto conditional debugging, you must first disable any crypto global debug CLIs you have issued; thereafter, you can disable conditional debugging.



Note The **reset** keyword can be used to disable all configured conditions at one time.

SUMMARY STEPS

1. **enable**
2. **debug crypto condition** [*connid integer engine-id integer*] [*flowid integer engine-id integer*] [*fvrfl string*] [*ivrf string*] [*peer [group string] [hostname string] [ipv4 ipaddress] [subnet subnet mask] [username string]] [spi integer] [reset]*
3. **show crypto debug-condition** {[*peer*] [*connid*] [*spi*] [*fvrfl*] [*ivrf*] [*unmatched*]}
4. **debug crypto isakmp**
5. **debug crypto ipsec**
6. **debug crypto engine**
7. **debug crypto condition unmatched** [*isakmp | ipsec | engine*] (optional)

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug crypto condition [connid <i>integer</i>] [engine-id <i>integer</i>] [flowid <i>integer</i>] [engine-id <i>integer</i>] [fvrf <i>string</i>] [ivrf <i>string</i>] [peer [group <i>string</i>] [hostname <i>string</i>] [ipv4 <i>ipaddress</i>] [subnet <i>subnet mask</i>] [username <i>string</i>]] [spi <i>integer</i>] [reset]	Defines conditional debug filters.
Step 3	Example: Router# debug crypto condition connid 2000 engine-id 1	
Step 3	show crypto debug-condition {[peer] [connid] [spi] [fvrf] [ivrf] [unmatched]}	Displays crypto debug conditions that have already been enabled in the router.
Step 4	Example: Router# show crypto debug-condition spi	
Step 4	debug crypto isakmp Example: Router# debug crypto isakmp	Enables global IKE debugging.
Step 5	debug crypto ipsec Example: Router# debug crypto ipsec	Enables global IPSec debugging.
Step 6	debug crypto engine Example: Router# debug crypto engine	Enables global crypto engine debugging.
Step 7	debug crypto condition unmatched [isakmp ipsec engine]	(Optional) Displays debug conditional crypto messages when no context information is available to check against debug conditions.
	Example: Router# debug crypto condition unmatched ipsec	If none of the optional keywords are specified, all crypto-related information will be shown.

Enabling Crypto Error Debug Messages

To enable crypto error debug messages, you must perform the following tasks.

debug crypto error CLI

Enabling the **debug crypto error** command displays only error-related debug messages, thereby, allowing you to easily determine why a crypto operation, such as an IKE negotiation, has failed within your system.



Note

When enabling this command, ensure that global crypto debug commands are not enabled; otherwise, the global commands will override any possible error-related debug messages.

SUMMARY STEPS

1. **enable**
2. **debug crypto {isakmp | ipsec | engine} error**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug crypto {isakmp ipsec engine} error Example: Router# debug crypto ipsec error	Enables only error debugging messages for a crypto area.

Configuration Examples for the Crypto Conditional Debug CLIs

This section includes the following examples:

- [Enabling Crypto Conditional Debugging: Example, page 6](#)
- [Disabling Crypto Conditional Debugging: Example, page 7](#)

Enabling Crypto Conditional Debugging: Example

The following example shows how to display debug messages when the peer IP address is 10.1.1.1, 10.1.1.2, or 10.1.1.3, and when the connection-ID 2000 of crypto engine 0 is used. This example also shows how to enable global debug crypto CLIs and enable the **show crypto debug-condition** command to verify conditional settings.

```
Router# debug crypto condition connid 2000 engine-id 1
Router# debug crypto condition peer ipv4 10.1.1.1
Router# debug crypto condition peer ipv4 10.1.1.2
Router# debug crypto condition peer ipv4 10.1.1.3
Router# debug crypto condition unmatched
! Verify crypto conditional settings.
Router# show crypto debug-condition
```

```
Crypto conditional debug currently is turned ON
IKE debug context unmatched flag:ON
IPsec debug context unmatched flag:ON
Crypto Engine debug context unmatched flag:ON

IKE peer IP address filters:
10.1.1.1 10.1.1.2 10.1.1.3

Connection-id filters:[connid:engine_id]2000:1,
! Enable global crypto CLIs to start conditional debugging.
Router# debug crypto isakmp
Router# debug crypto ipsec
Router# debug crypto engine
```

Disabling Crypto Conditional Debugging: Example

The following example shows how to disable all crypto conditional settings and verify that those settings have been disabled:

```
Router# debug crypto condition reset
! Verify that all crypto conditional settings have been disabled.
Router# show crypto debug-condition

Crypto conditional debug currently is turned OFF
IKE debug context unmatched flag:OFF
IPsec debug context unmatched flag:OFF
Crypto Engine debug context unmatched flag:OFF
```

Additional References

The following sections provide references to the Crypto Conditional Debug Support feature.

Related Documents

Related Topic	Document Title
IPSec and IKE configuration tasks	“Internet Key Exchange for IPsec VPNs” section of <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
IPSec and IKE commands	Cisco IOS Security Command Reference

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features

- **debug crypto condition**
- **debug crypto condition unmatched**
- **debug crypto error**
- **show crypto debug-condition**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



VPN Acceleration Module (VAM)

Feature History

Release	Modification
12.1(9)E	This feature was introduced on the Cisco 7200 series routers on NPE-225, NPE-400, and NSE-1
12.1(14)E	This feature was integrated into Cisco IOS Release 12.1(14)E and support for dual VAMs ¹ on the Cisco 7200 series with NPE-G1 was added
12.2(9)YE	Support for this feature was added to the Cisco 7401ASR router ²
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T
12.2(15)T	This feature was integrated into Cisco IOS Release 12.2(15)T
12.3(1)Mainline	This feature was integrated into Cisco IOS Release 12.3(1) Mainline
12.2(14)SU	This feature was integrated into Cisco IOS Release 12.2(14)SU

1. Support for dual VAMs is available on a Cisco 7200 series router with NPE-G1 on Cisco IOS Release 12.2(15)T, 12.1(14)E, and 12.3 Mainline only.
2. The Cisco 7401ASR router is no longer sold.

This feature module describes the VPN Acceleration Module (VAM) feature. It includes the following sections:

- [Feature Overview, page 2](#)
- [Supported Platforms, page 5](#)
- [Supported Standards, MIBs, and RFCs, page 6](#)
- [Prerequisites, page 6](#)
- [Configuration Tasks, page 6](#)
- [Monitoring and Maintaining the VPN Acceleration Module, page 12](#)
- [Configuration Examples, page 13](#)
- [Command Reference, page 15](#)
- [Glossary, page 15](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Feature Overview

The VPN Acceleration Module (VAM) is a single-width acceleration module. It provides high-performance, hardware-assisted tunneling and encryption services suitable for Virtual Private Network (VPN) remote access, site-to-site intranet, and extranet applications. It also provides platform scalability and security while working with all services necessary for successful VPN deployments — security, quality of service (QoS), firewall and intrusion detection, service-level validation, and management. The VAM off-loads IPSec processing from the main processor, thus freeing resources on the processor engines for other tasks.

The VAM provides hardware-accelerated support for the following multiple encryption functions:

- 56-bit Data Encryption Standard (DES) standard mode: Cipher Block Chaining (CBC)
- 3-Key Triple DES (168-bit)
- Secure Hash Algorithm (SHA)-1 and Message Digest 5 (MD5)
- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman key exchange RC4-40

Benefits

The VAM provides the following benefits:

- 10 tunnels per second
- The following number of tunnels based on the corresponding memory of the NPE:
 - 800 tunnels for 64 MB
 - 1600 tunnels for 128 MB
 - 3200 tunnels for 256 MB
 - 5000 tunnels for 512 MB
- RSA encryption
- Accelerated Crypto performance
- Accelerated Internet Key Exchange (IKE)
- Certificate support for automatic authentication using digital certificates
- Dual VAM support

**Note**

Support for dual VAMs is available on a Cisco 7200 series router with an NPE-G1, on Cisco IOS Release 12.2(15)T, 12.1(14)E, and 12.3 Mainline.

- Encryption services to any port adapter installed in the router. The interface on the port adapter must be configured with a crypto map to support IPSec.
- Full-duplex data transmission of over 100 Mbps with various encryption and compression schemes for 300 byte packages
- Hardware-based IPComp LZS compression
- Network traffic compression that reduces bandwidth utilization
- Online Insertion and Removal (OIR)

- QoS, multiprotocol, and multicast feature interoperation
- Support for full Layer 3 routing, such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) across the IPsec VPN
- Up to 145 Mbps throughput using 3DES
- VPN initialization improvements

Performance Results for Single VAM

The following two tables provide performance results for a single VAM on a Cisco 7206VXR with an NPE-G1 processor, an onboard GE, and FE port adapters in slots 3 and 4.

clear_packet_size	crypto_packet_size	out_packet_size
64	96	114
300	336	354
1400	1432	1450
Mixed packet size - 344	378	396

pkt_size (bytes)	# of tunnels	measured_pps (pps)	meas_clear_ndr (Mbps)	meas_crypto_ndr (Mbps)	meas_out_ndr (Mbps)
64	4	65,224	33.39	50.09	59.48
	500	41,888	21.44	32.17	38.20
	1,000	40,480	20.73	31.09	36.92
	5,000	39,408	20.18	30.27	35.94
300	4	38,032	91.28	102.23	107.71
	500	37,184	89.24	99.95	105.31
	1,000	36,064	86.55	96.94	102.13
	5,000	36,016	86.44	96.81	101.99
1400	4	9,984	111.82	114.38	115.81
	500	9,848	110.29	112.82	114.24
	1,000	9,648	108.06	110.53	111.92
	5,000	9,616	107.70	110.16	111.55
Mixed packet size	4	31,472	86.61	95.17	99.70
	500	31,056	85.47	93.91	98.39
	1,000	30,128	82.91	91.11	95.45
	5,000	29,264	80.53	88.49	92.71

Performance Results for Dual VAMs

The following two tables provide performance results for dual VAMs on a Cisco 7206VXR with an NPE-G1 processor, an onboard GE, and FE port adapters in slots 3 and 4.

clear_packet_size	crypto_packet_size	out_packet_size
64	96	114
300	336	354
1400	1432	1450
Mixed packet size - 344	378	396

pkt_size (bytes)	# of tunnels	measured_pps (pps)	meas_clear_ndr (Mbps)	meas_crypto_ndr (Mbps)	meas_out_ndr (Mbps)
64	4	135,544	69.40	104.10	123.61
	500	61,520	31.50	47.25	56.11
	1,000	56,928	29.15	43.72	51.92
	5,000	43,744	22.40	33.60	39.89
300	4	71,336	171.21	191.75	202.02
	500	60,416	145.00	162.40	171.10
	1,000	56,016	134.44	150.57	158.64
	5,000	42,496	101.99	114.23	120.35
1400	4	18,736	209.84	214.64	217.34
	500	18,424	206.35	211.07	213.72
	1000	18,352	205.54	210.24	212.88
	5,000	18,352	205.54	210.24	212.88
Mixed packet size	4	60,416	166.26	182.70	191.40
	500	57,888	159.31	175.05	183.40
	1,000	55,488	152.70	167.80	175.79
	5,000	34,272	94.32	103.64	108.57

Related Features and Technologies

The following features and technologies are related to the VAM:

- Internet Key Exchange (IKE)
- IP Security (IPSec)

Related Documents

The following document describes the VAM hardware:

- [VPN Acceleration Module Installation and Configuration](#)

Supported Platforms

The VAM feature is supported on the following platforms:

- Cisco 7200 series routers with NPE-225, NPE-400, NSE-1, and NPE-G1
- Dual VAM support is available on a Cisco 7200 series router with an NPE-G1, on Cisco IOS Release 12.2(15)T, 12.1(14)E, and 12.3M.
- Cisco 7401ASR router

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

- No new or modified standards are supported by this feature.

MIBs

The following MIBs were introduced or modified in this feature:

- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

- IPPCP: RFC 2393, 2395
- IPSec/IKE: RFCs 2401-2411, 2451

Prerequisites

You must configure IPSec and IKE on the router and a crypto map to all interfaces that require encryption service from the VAM. See the “[Configuration Examples](#)” section on [page 13](#) for configuration procedures.

Configuration Tasks


On power up if the enabled LED is on, the VAM is fully functional and does not require any configuration commands. However, for the VAM to provide encryption services, you must complete the following tasks:

- [Configuring an IKE Policy](#) (required)
- [Configuring IPSec](#) (required)

Configuring an IKE Policy

If you do not specify a value for a parameter, the default value is assigned. For information on default values, refer to the “IP Security and Encryption” chapter of the *Security Command Reference* publication.

To configure an IKE policy, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto isakmp policy <i>priority</i>	Defines an IKE policy and enters Internet Security Association Key Management Protocol (ISAKMP) policy configuration (config-isakmp) mode.
Step 2	Router(config-isakmp)# encryption {des 3des aes aes 192 aes 256}	Specifies the encryption algorithm within an IKE policy. <ul style="list-style-type: none"> des—Specifies 56-bit DES as the encryption algorithm. 3des—Specifies 168-bit DES as the encryption algorithm. aes—Specifies 128-bit AES as the encryption algorithm. aes 192—Specifies 192-bit AES as the encryption algorithm. aes 256—Specifies 256-bit AES as the encryption algorithm.
Step 3	Router(config-isakmp)# authentication {rsa-sig rsa-encr pre-share}	<p>(Optional) Specifies the authentication method within an IKE policy.</p> <ul style="list-style-type: none"> rsa-sig—Specifies Rivest, Shamir, and Adelman (RSA) signatures as the authentication method. rsa-encr—Specifies RSA encrypted nonces as the authentication method. <div>  <p>Note Beginning with Cisco IOS Release 12.3(10), rsa-encr is now enabled for VAM crypto cards.</p> </div> <ul style="list-style-type: none"> pre-share—Specifies preshared keys as the authentication method. <p>Note If this command is not enabled, the default value (rsa-sig) will be used.</p>
Step 4	Router(config-isakmp)# lifetime <i>seconds</i>	<p>(Optional) Specifies the lifetime of an IKE security association (SA).</p> <p><i>seconds</i>—Number of seconds that each SA should exist before expiring. Use an integer from 60 to 86,400 seconds.</p> <p>Note If this command is not enabled, the default value (86,400 seconds [one day]) will be used.</p>

	Command	Purpose
Step 5	Router(config-isakmp)# hash { sha md5 }	(Optional) Specifies the hash algorithm within an IKE policy. <ul style="list-style-type: none"> sha—Specifies SHA-1 (HMAC variant) as the hash algorithm. md5—Specifies MD5 (HMAC variant) as the hash algorithm. Note If this command is not enabled, the default value (sha) will be used.
Step 6	Router(config-isakmp)# group { 1 2 5 }	(Optional) Specifies the Diffie-Hellman (DH) group identifier within an IKE policy. <p>1—Specifies the 768-bit DH group.</p> <p>2—Specifies the 1024-bit DH group.</p> <p>5—Specifies the 1536-bit DH group.</p> Note If this command is not enabled, the default value (768-bit) will be used.

For detailed information on creating IKE policies, refer to the “[Configuring Internet Key Exchange Security Protocol](#)” chapter in the *Security Configuration Guide* publication.

Configuring IPSec

After you have completed IKE configuration, configure IPSec at each participating IPSec peer. This section contains basic steps to configure IPSec and includes the tasks discussed in the following sections:

- [Creating Crypto Access Lists, page 8](#)
- [Defining Transform Sets, page 9](#)

Creating Crypto Access Lists

To create crypto access lists, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# access-list <i>access-list-number</i> { deny permit } <i>protocol source source-wildcard destination destination-wildcard</i> [log] or ip access-list extended <i>name</i>	Specifies conditions to determine which IP packets are protected. ¹ (Enable or disable encryption for traffic that matches these conditions.) We recommend that you configure “mirror image” crypto access lists for use by IPSec and that you avoid using the any keyword.
Step 2	Router(config-if)# Add permit and deny statements as appropriate.	Adds permit or deny statements to access lists.
Step 3	Router(config-if)# end	Exits the configuration command mode.

1. You specify conditions using an IP access list designated by either a number or a name. The **access-list** command designates a numbered extended access list; the **ip access-list extended** command designates a named access list.

For detailed information on configuring access lists, refer to the “[Configuring IPSec Network Security](#)” chapter in the *Security Configuration Guide* publication.

Defining Transform Sets

To define a transform set, use the following commands, starting in global configuration mode:

Command	Purpose
Router# crypto ipsec transform-set <i>transform-set-name transform1 [transform2 [transform3]]</i>	Defines a transform set and enters crypto transform configuration mode.
Router# mode [tunnel transport]	Changes the mode associated with the transform set. The mode setting is applicable only to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.)
Router# end	Exits the crypto transform configuration mode to enabled mode.
Router# clear crypto sa or clear crypto sa peer { <i>ip-address</i> <i>peer-name</i> } or clear crypto sa map <i>map-name</i> or clear crypto sa spi <i>destination-address protocol spi</i>	Clears existing IPSec security associations so that any changes to a transform set take effect on subsequently established security associations (SAs). (Manually established SAs are reestablished immediately.) Using the clear crypto sa command without parameters clears out the full SA database, which clears out active security sessions. You might also specify the peer , map , or entry keywords to clear out only a subset of the SA database.

To create crypto map entries that use IKE to establish the security associations, use the following commands, starting in global configuration mode:

Command	Purpose
Router# crypto map <i>map-name seq-num ipsec-isakmp</i>	Creates the crypto map and enters crypto map configuration mode.
Router# match address <i>access-list-id</i>	Specifies an extended access list. This access list determines which traffic is protected by IPSec and which is not.
Router# set peer { <i>hostname</i> <i>ip-address</i> }	Specifies a remote IPSec peer. This is the peer to which IPSec-protected traffic can be forwarded. Repeat for multiple remote peers.
Router# set transform-set <i>transform-set-name1 [transform-set-name2...transform-set-name6]</i>	Specifies which transform sets are allowed for this crypto map entry. Lists multiple transform sets in order of priority (highest priority first).
Router# end	Exits crypto map configuration mode.

Repeat these steps to create additional crypto map entries as required.

For detailed information on configuring crypto maps, refer to the “[Configuring IPSec Network Security](#)” chapter in the *Security Configuration Guide* publication.

Verifying the Configuration

The following steps provide information on verifying your configurations:

Step 1 Enter the **show crypto ipsec transform-set** command to view your transform set configuration:

```
Router# show crypto ipsec transform-set
Transform set combined-des-md5: {esp-des esp-md5-hmac}
    will negotiate = {Tunnel,},
Transform set t1: {esp-des esp-md5-hmac}
    will negotiate = {Tunnel,},
Transform set t100: {ah-sha-hmac}
    will negotiate = {Transport,},
Transform set t2: {ah-sha-hmac}
    will negotiate = {Tunnel,},
    {esp-des}
    will negotiate = {Tunnel,},
```

Step 2 Enter the **show crypto map [interface interface | tag map-name]** command to view your crypto map configuration:

```
outer# show crypto map
Crypto Map: "router-alice" idb: Ethernet0 local address: 172.21.114.123
Crypto Map "router-alice" 10 ipsec-isakmp
    Peer = 172.21.114.67
    Extended IP access list 141
        access-list 141 permit ip
            source: addr = 172.21.114.123/0.0.0.0
            dest:   addr = 172.21.114.67/0.0.0.0
    Current peer: 172.21.114.67
    Security-association lifetime: 4608000 kilobytes/120 seconds
    PFS (Y/N): N
    Transform sets={t1,}
```

Step 3 Enter the **show crypto ipsec sa [map map-name | address | identity | detail | interface]** command to view information about IPSec security associations.

```
Router# show crypto ipsec sa
interface: Ethernet0
    Crypto map tag: router-alice, local addr. 172.21.114.123
    local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
    current_peer: 172.21.114.67
        PERMIT, flags={origin_is_acl,}
        #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
        #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
        #send errors 10, #recv errors 0
        local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
        path mtu 1500, media mtu 1500
        current outbound spi: 20890A6F
    inbound esp sas:
        spi: 0x257A1039(628756537)
            transform: esp-des esp-md5-hmac,
            in use settings = {Tunnel,}
            slot: 0, conn id: 26, crypto map: router-alice
            sa timing: remaining key lifetime (k/sec): (4607999/90)
            IV size: 8 bytes
            replay detection support: Y
    inbound ah sas:
    outbound esp sas:
```



```

spi: 0x20890A6F(545852015)
  transform: esp-des esp-md5-hmac,
  in use settings ={Tunnel,}
  slot: 0, conn id: 27, crypto map: router-alice
  sa timing: remaining key lifetime (k/sec): (4607999/90)
  IV size: 8 bytes
  replay detection support: Y
outbound ah sas:
interface: Tunnel0
  Crypto map tag: router-alice, local addr. 172.21.114.123
  local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
  current_peer: 172.21.114.67
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
    local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
    path mtu 1500, media mtu 1500
    current outbound spi: 20890A6F
  inbound esp sas:
    spi: 0x257A1039(628756537)
      transform: esp-des esp-md5-hmac,
      in use settings ={Tunnel,}
      slot: 0, conn id: 26, crypto map: router-alice
      sa timing: remaining key lifetime (k/sec): (4607999/90)
      IV size: 8 bytes
      replay detection support: Y
  inbound ah sas:
  outbound esp sas:
    spi: 0x20890A6F(545852015)
      transform: esp-des esp-md5-hmac,
      in use settings ={Tunnel,}
      slot: 0, conn id: 27, crypto map: router-alice
      sa timing: remaining key lifetime (k/sec): (4607999/90)
      IV size: 8 bytes
      replay detection support: Y
  outbound ah sas:

```

Troubleshooting Tips

To verify that Cisco IOS software has recognized VAM, enter the **show diag** command and check the output. For example, when the router has the VAM in slot 1, the following output appears:

```

Router# show diag 1
Slot 1:
  VAM Encryption/Compression engine. Port adapter
  Port adapter is analyzed
  Port adapter insertion time 00:04:45 ago
  EEPROM contents at hardware discovery:
  Hardware Revision      :1.0
  PCB Serial Number      :15485660
  Part Number            :73-5953-04
  Board Revision         :
  RMA Test History       :00
  RMA Number             :0-0-0-0
  RMA History            :00
  Deviation Number       :0-0
  Product Number         :CLEO

```

```

Top Assy. Part Number      :800-10496-04
CLEI Code                  :
EEPROM format version 4
EEPROM contents (hex):
0x00:04 FF 40 02 8A 41 01 00 C1 8B 31 35 34 38 35 36
0x10:36 30 00 00 00 82 49 17 41 04 42 FF FF 03 00 81
0x20:00 00 00 00 04 00 80 00 00 00 00 CB 94 43 4C 45
0x30:4F 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0x40:20 C0 46 03 20 00 29 00 04 C6 8A FF FF FF FF FF
0x50:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

```

To see if the VAM is currently processing crypto packets, enter the **show pas vam interface** command. The following is sample output:

```

Router# show pas vam interface

Interface VAM 1/1 :
ds:0x632770C8      idb:0x62813728
Statistics of packets and bytes that through this interface:
    18 packets in          18 packets out
   2268 bytes in          2268 bytes out
    0 paks/sec in          0 paks/sec out
    0 Kbits/sec in          0 Kbits/sec out
    83 commands out        83 commands acknowledged
ppq_full_err   :0          ppq_rx_err       :0
cmdq_full_err  :0          cmdq_rx_err      :0
no_buffer      :0          fallback         :0
dst_overflow   :0          nr_overflow      :0
sess_expired   :0          pkt_fragmented  :0
out_of_mem     :0          access_denied   :0
invalid_fc     :0          invalid_param   :0
invalid_handle :0          output_overrun  :0
input_underrun :0          input_overrun   :0
key_invalid    :0          packet_invalid  :0
decrypt_failed :0          verify_failed   :0
attr_invalid   :0          attr_val_invalid :0
attr_missing   :0          obj_not_wrap    :0
bad_imp_hash    :0          cant_fragment   :0
out_of_handles :0          compr_cancelled  :0
rng_st_fail    :0          other_errors     :0
633 seconds since last clear of counters

```

When the VAM processes packets, the “packet in” and “packet out” counters change. Counter “packets out” represents the number of packets directed to the VAM. Counter “packets in” represents the number of packets received from the VAM.



Note

In versions prior to Cisco IOS Release 12.2(5)T and Cisco IOS Release 12.1(10)E, upon reboot trap configurations are lost and need to be re-entered.

Monitoring and Maintaining the VPN Acceleration Module

Use the commands below to monitor and maintain the VPN Acceleration Module:

Command	Purpose
Router# show pas isa interface	Displays the ISA interface configuration.
Router# show pas isa controller	Displays the ISA controller configuration.
Router# show pas vam interface	Verifies the VAM is currently processing crypto packets.
Router# show pas vam controller	Displays the VAM controller configuration.
Router# Show version	Displays integrated service adapter as part of the interfaces.

Configuration Examples

This section provides the following configuration examples:

- [Configuring IKE Policies Example, page 13](#)
- [Configuring IPSec Configuration Example, page 13](#)

Configuring IKE Policies Example

In the following example, two IKE policies are created, with policy 15 as the highest priority, policy 20 as the next priority, and the existing default priority as the lowest priority. It also creates a preshared key to be used with policy 20 with the remote peer whose IP address is 192.168.224.33.

```
crypto isakmp policy 15
  encryption 3des
  hash md5
  authentication rsa-sig
  group 2
  lifetime 5000
crypto isakmp policy 20
  authentication pre-share
  lifetime 10000
crypto isakmp key 1234567890 address 192.168.224.33
```

Configuring IPSec Configuration Example

The following example shows a minimal IPSec configuration where the security associations will be established via IKE:

An IPSec access list defines which traffic to protect:

```
access-list 101 permit ip 10.0.0.0 0.0.0.255 10.2.2.0 0.0.0.255
```

A transform set defines how the traffic will be protected. In this example, transform set "myset1" uses DES encryption and SHA for data packet authentication:

```
crypto ipsec transform-set myset1 esp-des esp-sha
```

Another transform set example is "myset2," which uses Triple DES encryption and MD5 (HMAC variant) for data packet authentication:

```
crypto ipsec transform-set myset2 esp-3des esp-md5-hmac
```

A crypto map joins together the IPsec access list and transform set and specifies where the protected traffic is sent (the remote IPsec peer):

```
crypto map toRemoteSite 10 ipsec-isakmp
  match address 101
  set transform-set myset2
  set peer 10.2.2.5
```

The crypto map is applied to an interface:

```
interface Serial0
  ip address 10.0.0.2
  crypto map toRemoteSite
```

**Note**

In this example, IKE must be enabled.

Command Reference

The following commands are introduced or modified in the feature or features

- **show pas vam interface**
- **show pas vam controller**
- **crypto engine sw ipsec**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Glossary

VAM—VPN Acceleration Module.

IKE—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service.

IPSec—IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2009 Cisco Systems, Inc. All rights reserved.



VPN Availability



Reverse Route Injection

First Published: August 16, 2001
Last Updated: November 5, 2007

Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote Virtual Private Network (VPN) router as the next hop, the traffic is forced through the crypto process to be encrypted.

Enhancements to the default behavior of RRI, the addition of a route tag value, and enhancements to how RRI is configured were added to the Reverse Route Injection feature in Cisco IOS Release 12.3(14)T.

An enhancement was added in Cisco IOS Release 12.4(15)T that allows a distance metric to be set for routes that are created by a VPN process so that the dynamically learned route on a router can take precedence over a locally configured static route.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Reverse Route Injection](#)” section on [page 18](#).

Finding Support Information for Platforms and Cisco IOS Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Reverse Route Injection, page 2](#)
- [Restrictions for Reverse Route Injection, page 2](#)
- [Information About Reverse Route Injection, page 2](#)
- [How to Configure Reverse Route Injection, page 4](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for Reverse Route Injection, page 10](#)
- [Additional References, page 16](#)
- [Command Reference, page 17](#)
- [Feature Information for Reverse Route Injection, page 26](#)

Prerequisites for Reverse Route Injection

- IP routing should be enabled and static routes should be redistributed if dynamic routing protocols are to be used to propagate RRI-generated static routes.

Restrictions for Reverse Route Injection

- If RRI is applied to a crypto map, that map must be unique to one interface on the router. In other words, the same crypto map cannot be applied to multiple interfaces. If more than one crypto map is applied to multiple interfaces, routes may not be cleaned up correctly. If multiple interfaces require a crypto map, each must use a uniquely defined map. This restriction applies only to RRI before Cisco IOS Release 12.3(14)T.
- For static crypto maps, routes are always present if RRI is configured on an applied crypto map. In Cisco IOS Release 12.3(14)T, the default behavior—of routes always being present for a static map—will not apply unless the **static keyword** is added to the **reverse-route** command.

Information About Reverse Route Injection

To configure the Reverse Route Injection enhancements, you should understand the following concepts:

- [Reverse Route Injection, page 2](#)
- [Enhancements to Reverse Route Injection in Cisco IOS Release 12.4\(15\)T, page 3](#)

Reverse Route Injection

RRI is the ability for static routes to be automatically inserted into the routing process for those networks and hosts that are protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote VPN router as the next hop, the traffic is forced through the crypto process to be encrypted.

After the static route is created on the VPN router, this information is propagated to upstream devices, allowing them to determine the appropriate VPN router to which to send returning traffic in order to maintain IPsec state flows. Being able to determine the appropriate VPN router is particularly useful if multiple VPN routers are used at a site to provide load balancing or failover or if the remote VPN devices are not accessible via a default route. Routes are created in either the global routing table or the appropriate virtual route forwarding (VRF) table.

RRI is applied on a per-crypto map basis, whether this is via a static crypto map or a dynamic crypto map template. The default behavior for the two map types is as follows:

- In the case of a dynamic crypto map, routes are created upon the successful establishment of IPsec security associations (SAs) for those remote proxies. The next hop back to those remote proxies is via the remote VPN router whose address is learned and applied during the creation of the dynamic crypto map template. The routes are deleted after the SAs are deleted. In Cisco IOS Release 12.3(14)T, the creation of routes on the basis of IPsec source proxies on static crypto maps was added. This behavior became the default behavior on static maps and overrode the creation of routes on the basis of crypto ACLs (see the next bullet).
- For static crypto maps, routes are created on the basis of the destination information defined in the crypto access list. The next hop is taken from the first set peer statement that is attached to the crypto map. If at any time, RRI, the peer, or the access list is removed from the crypto map, routes will be deleted. This behavior changes with the addition of the RRI enhancements, as explained in the sections below.

Enhancements to Reverse Route Injection in Cisco IOS Release 12.4(15)T

The following enhancements have been added to the Reverse Route Injection feature in Cisco IOS Release 12.4(15)T:

- [RRI Distance Metric, page 3](#)
- [Gateway Option, page 3](#)
- [Support for RRI on IPsec Profiles, page 4](#)
- [Tag Option Configuration Changes, page 4](#)
- [show crypto route Command, page 4](#)

RRI Distance Metric

In general, a static route is created having an administrative distance of 1, which means that static routes always have precedence in the routing table. In some scenarios, however, it is required that dynamically learned routes take precedence over static routes, with the static route being used in the absence of a dynamically learned route. The addition of the **set reverse-route distance** command under either a crypto map or IPsec profile allows you to specify a different distance metric for VPN-created routes so that those routes will be in effect only if a dynamic or more favored route becomes unavailable.

Gateway Option

This RRI gateway option is relevant to the crypto map only.

This option allows you to configure unique next hops or gateways for remote tunnel endpoints. The option is identical to the way the **reverse-route remote-peer** {*ip-address*} command worked prior to Cisco IOS Release 12.3(14)T in that two routes are created for each VPN tunnel. The first route is to the destination-protected subnet via the remote tunnel endpoint. The second route specifies the next hop to be taken to reach this tunnel endpoint. This RRI gateway option allows specific default paths to be specified for specific groups of VPN connections on platforms that support recursive route lookups.



Note

In 12.4(15)T and later releases, the **gateway** keyword option replaces the **reverse-route remote-peer** command (with no *ip-address*). Due to changes to Cisco Express Forwarding (CEF), an interface as a next-hop cannot be used without also adding a next-hop IP address.

Support for RRI on IPsec Profiles

Previously RRI was available for crypto map configurations only. Cisco IOS Release 12.4(15)T introduces support for relevant RRI options on IPsec profiles that are predominantly used for virtual tunnel interfaces. On tunnel interfaces, only the distance metric and tag options are useful with the generic RRI capability.

**Note**

It is not necessary to specifically enable RRI on dynamic virtual interfaces for Easy VPN clients. Route support is enabled by default. It is necessary to specify tag or distance metric values if these are required.

Tag Option Configuration Changes

The tag option was introduced in 12.3(14)T for crypto maps. This option is now supported with IPsec profiles under the **set reverse-route tag** command syntax. The **set reverse-route tag** command is also available under the crypto map for uniformity although the legacy **reverse-route tag** command is no longer supported.

show crypto route Command

The **show crypto route** command displays routes that are created through IPsec via RRI or Easy VPN virtual tunnel interfaces (VTIs). The routes are displayed in one table. To see sample output for the **show crypto route** command, see the section “[show crypto route Command Output: Example](#).”

How to Configure Reverse Route Injection

The following sections show how to configure reverse route injection for Cisco IOS software before Release 12.4(15)T and for Release 12.4(15)T.

- [Configuring RRI on Crypto Maps for Cisco IOS Releases Prior to 12.4\(15\)T, page 4](#)
- [Configuring RRI with Enhancements Added in Cisco IOS Release 12.4\(15\)T, page 6](#)

Configuring RRI on Crypto Maps for Cisco IOS Releases Prior to 12.4(15)T

This section includes the following tasks:

- [Configuring RRI Under a Static Crypto Map, page 4](#)
- [Configuring RRI Under a Dynamic Map Template, page 5](#)

Configuring RRI Under a Static Crypto Map

To configure RRI under a static crypto map for Cisco IOS software prior to Release 12.4(15)T, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto map** {*map-name*} {*seq-name*} **ipsec-isakmp**
4. **reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map { <i>map-name</i> } { <i>seq-name</i> } ipsec-isakmp Example: Router (config)# crypto map mymap 1 ipsec-isakmp	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 4	reverse-route [static tag <i>tag-id</i> [static] remote-peer [static] remote-peer <i>ip-address</i> [static]] Example: Router (config-crypto-map)# reverse-route remote peer 10.1.1.1	Creates source proxy information for a crypto map entry.

Configuring RRI Under a Dynamic Map Template

To configure RRI under a dynamic map template for Cisco IOS software prior to Release 12.4(15)T, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name* *dynamic-seq-name*
4. **reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto dynamic-map <i>dynamic-map-name</i> <i>dynamic-seq-name</i> Example: Router (config)# crypto dynamic-map mymap 1	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
Step 4	reverse-route [static tag <i>tag-id</i> [static remote-peer [static remote-peer <i>ip-address</i> [static]]] Example: Router (config-crypto-map)# reverse-route remote peer 10.1.1.1	Creates source proxy information for a crypto map entry.

Configuring RRI with Enhancements Added in Cisco IOS Release 12.4(15)T

The following sections show how to configure RRI with the enhancements that were added in Cisco IOS Release 12.4(15)T:

- [Configuring RRI with Enhancements Under a Static Crypto Map, page 6](#)
- [Configuring RRI with Enhancements Under a Dynamic Map Template, page 7](#)
- [Configuring a RRI Distance Metric Under an IPsec Profile, page 8](#)
- [Verifying Routes That Are Created Through IPsec via RRI or Easy VPN VTIs, page 9](#)

Configuring RRI with Enhancements Under a Static Crypto Map

To configure RRI with enhancements under a static crypto map (for Cisco IOS Release 12.4(15)T and later releases), perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name* *seq-name* **ipsec-isakmp**
4. **reverse-route** [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]]
5. **set reverse-route** [**distance** *number* | **tag** *tag-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-name ipsec-isakmp</i> Example: Router (config)# crypto map mymap 1 ipsec-isakmp	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 4	reverse-route [static remote-peer <i>ip-address</i> [gateway] [static]] Example: Router (config-crypto-map)# reverse-route	Creates source proxy information for a crypto map entry. Note The gateway keyword can be added to enable the dual route functionality for default gateway support.
Step 5	set reverse-route [distance <i>number</i> tag <i>tag-id</i>] Example: Router (config-crypto-map)# set reverse-route distance 20	Specifies a distance metric to be used or a tag value to be associated with these routes.

Configuring RRI with Enhancements Under a Dynamic Map Template

To configure RRI with enhancements under a dynamic map template (for Cisco IOS Release 12.4(15)T and later releases), perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name dynamic-seq-name*
4. **reverse-route** [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]]
5. **set reverse-route** [**distance** *number* | **tag** *tag-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto dynamic-map <i>dynamic-map-name</i> <i>dynamic-seq-name</i> Example: Router (config)# crypto dynamic-map mymap 1	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
Step 4	reverse-route [static remote-peer <i>ip-address</i> [<i>gateway</i>] [static]] Example: Router (config-crypto-map)# reverse-route remote peer 10.1.1.1 gateway	Creates source proxy information for a crypto map entry.
Step 5	set reverse-route [distance <i>number</i> tag <i>tag-id</i>] Example: Router (config-crypto-map)# set reverse-route distance 20	Specifies a distance metric to be used or a tag value to be associated with these routes.

Configuring a RRI Distance Metric Under an IPsec Profile

To configure a RRI distance metric under an IPsec profile for Cisco IOS Release 12.4(15)T and later releases, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **set reverse-route** [**distance** *number* | **tag** *tag-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec profile name Example: Router (config)# crypto ipsec profile myprofile	Creates or modifies an IPsec profile and enters IPsec profile configuration mode.
Step 4	set reverse-route [distance number tag tag-id] Example: Router (config-crypto-profile)# set reverse-route distance 20	Defines a distance metric for each static route or tags a reverse route injection- (RRI-) created route. <ul style="list-style-type: none">distance—Defines a distance metric for each static route.tag—Sets a tag value that can be used as a “match” value for controlling distribution using route maps.

Verifying Routes That Are Created Through IPsec via RRI or Easy VPN VTIs

To display routes that are created through IPsec via RRI or Easy VPN VTIs, perform the following steps.

SUMMARY STEPS

1. enable
2. show crypto route

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	show crypto route Example: Router# show crypto route	Displays routes that are created through IPsec via RRI or Easy VPN VTIs.

Troubleshooting Tips

To observe the behavior of RRI and its relationship to the creation and deletion of an IPsec SA, you can use the **debug crypto ipsec** command (see the [Cisco IOS Debug Command Reference](#), Release 12.4T).

Configuration Examples for Reverse Route Injection

This section contains the following sections:

- [Configuring RRI Prior to Cisco IOS Release 12.3\(14\)T: Examples, page 10](#)
- [Configuring RRI with Enhancements Added in Cisco IOS Release 12.3\(14\)T: Examples, page 11](#)
- [Configuring RRI with Enhancements Added in Cisco IOS Release 12.4\(15\)T: Examples, page 12](#)

Configuring RRI Prior to Cisco IOS Release 12.3(14)T: Examples

The following are examples of RRI configurations and output before Cisco IOS Release 12.3(14)T:

- [Configuring RRI When Crypto ACLs Exist: Example, page 10](#)
- [Configuring RRI When Two Routes Are Created, One for the Remote Endpoint and One for Route Recursion: Example, page 11](#)

Configuring RRI When Crypto ACLs Exist: Example

The following example shows that all remote VPN gateways connect to the router via 192.168.0.3. RRI is added on the static crypto map, which creates routes on the basis of the source network and source netmask that are defined in the crypto access control list (ACL):

```
crypto map mymap 1 ipsec-isakmp
  set peer 10.1.1.1
  reverse-route
  set transform-set esp-3des-sha
  match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

In Cisco IOS Release 12.3(14)T and later releases, for the static map to retain this same behavior of creating routes on the basis of crypto ACL content, the **static** keyword is required, that is, **reverse-route static**.



Note

The **reverse-route** command in this situation creates routes that are analogous to the following static route command-line interface (CLI) commands (**ip route**):

Remote Tunnel Endpoint

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1
```

VPNSM

```
ip route 10.1.1.1 255.255.255.255 vlan0.1
```

Configuring RRI When Two Routes Are Created, One for the Remote Endpoint and One for Route Recursion: Example

In the following example, two routes are created, one for the remote endpoint and one for route recursion to the remote endpoint via the interface on which the crypto map is configured:

```
reverse-route remote-peer
```

Configuring RRI with Enhancements Added in Cisco IOS Release 12.3(14)T: Examples

The following are examples of configurations and output for RRI enhancements that were added in Cisco IOS Release 12.3(14)T.

- [Configuring RRI When Crypto ACLs Exist: Example, page 11](#)
- [Configuring RRI with Route Tags: Example, page 11](#)
- [Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop: Example, page 12](#)

Configuring RRI When Crypto ACLs Exist: Example

The following example shows that RRI has been configured for a situation in which there are existing ACLs:

```
crypto map mymap 1 ipsec-isakmp
  set peer 172.17.11.1
  reverse-route static
  set transform-set esp-3des-sha
  match address 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

Configuring RRI with Route Tags: Example

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
  reverse-route tag 5

router ospf 109
  redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
  match tag 5
  set metric 5
  set metric-type type1

Router# show ip ospf topology
```

```
P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop: Example

Note This option is applicable only to crypto maps.

The preceding example shows that one route has been created to the remote proxy via a user-defined next hop. This next hop should not require a recursive route lookup unless it will recurse to a default route.

```
reverse-route remote-peer 10.4.4.4
```

The preceding example yields the following prior to Cisco IOS Release 12.3(14)T:

```
10.0.0.0/24 via 10.1.1.1 (in the VRF table if VRFs are configured)
10.1.1.1/32 via 10.4.4.4 (in the global route table)
```

And this result occurs with RRI enhancements:

```
10.0.0.0/24 via 10.4.4.4 (in the VRF table if VRFs are configured, otherwise in the global
table)
```

Configuring RRI with Enhancements Added in Cisco IOS Release 12.4(15)T: Examples

The following are examples of configurations and output for RRI enhancements that were added in Cisco IOS Release 12.4(15)T.

- [Configuring a RRI Distance Metric Under a Crypto Map: Example, page 12](#)
- [Configuring RRI with Route Tags: Example, page 11](#)
- [debug and show Command Output for a RRI Distance Metric Configuration Under a Crypto Map: Example, page 13](#)
- [Configuring a RRI Distance Metric for a VTI: Example, page 14](#)
- [debug and show Command Output for a RRI Metric Configuration Having a VTI: Example, page 14](#)
- [show crypto route Command Output: Example, page 15](#)

Configuring a RRI Distance Metric Under a Crypto Map: Example

The following configuration shows a server and client configuration for which a RRI distance metric has been set under a crypto map:

Server

```
crypto dynamic-map mymap
  set security-association lifetime seconds 300
  set transform-set 3dessha
  set isakmp-profile profile1
  set reverse-route distance 20
reverse-route
```

Client

```
crypto ipsec client ezvpn ez
  connect auto
  group cisco key cisco
```

```

mode client
peer 10.0.0.119
username XXX password XXX
xauth userid mode local

```

Configuring RRI with Route Tags: Example

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```

crypto dynamic-map ospf-clients 1
  set reverse-route tag 5

router ospf 109
  redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
  match tag 5
  set metric 5
  set metric-type type1

Router# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1

```

debug and show Command Output for a RRI Distance Metric Configuration Under a Crypto Map: Example

The following are **debug** and **show** command output for a RRI distance metric configuration under a crypto map on a server:

```

Router# debug crypto ipsec

00:23:37: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.0.0.119, remote= 10.0.0.14,
  local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
  remote_proxy= 192.168.6.1/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
00:23:37: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:23:37: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for
  10.0.0.128
00:23:37: IPSEC(rte_mgr): VPN Route Refcount 1 FastEthernet0/0
00:23:37: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via 10.0.0.14 in IP
  DEFAULT TABLE with tag 0 distance 20
00:23:37: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0

Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.14 to network 0.0.0.0

```

```

C    192.200.200.0/24 is directly connected, Loopback0
    10.20.20.20/24 is subnetted, 1 subnets
C    10.30.30.30 is directly connected, Loopback4
C    192.168.5.0/24 is directly connected, Loopback3
    10.20.20.20/24 is subnetted, 2 subnets
S    10.3.1.0 [1/0] via 10.0.0.113
C    10.20.20.20 is directly connected, FastEthernet0/0
    192.168.6.0/32 is subnetted, 1 subnets
S    192.168.6.1 [20/0] via 10.0.0.14
C    192.168.3.0/24 is directly connected, Loopback2
    10.15.0.0/24 is subnetted, 1 subnets
C    10.15.0.0 is directly connected, Loopback6
S*   0.0.0.0/0 [1/0] via 10.0.0.14

```

Configuring a RRI Distance Metric for a VTI: Example

The following configuration shows a server and client configuration in which a RRI distance metric has been set for a VTI:

Server Configuration

```

crypto isakmp profile profile1
  keyring mykeyring
  match identity group cisco
  client authentication list authenlist
  isakmp authorization list autholist
  client configuration address respond
  virtual-template 1
crypto ipsec profile vi
  set transform-set 3dessa
  set reverse-route distance 20
  set isakmp-profile profile1
!
interface Virtual-Template1 type tunnel
  ip unnumbered
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile vi

```

Client Configuration

```

crypto ipsec client ezvpn ez
  connect auto
  group cisco key cisco
  mode client
  peer 10.0.0.119
  username XXX password XXX
  virtual-interface 1

```

debug and show Command Output for a RRI Metric Configuration Having a VTI: Example

The following are **debug** and **show** command output for a RRI metric configuration for a VTI on a server:

```

Router# debug crypto ipsec

00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:47:56: Crypto mapdb : proxy_match
          src addr      : 0.0.0.0
          dst addr      : 192.168.6.1
          protocol      : 0
          src port      : 0

```



```

dst port      : 0
00:47:56: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same pro
xies and peer 10.0.0.14
00:47:56: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for
10.0.0.14
00:47:56: IPSEC(rte_mgr): VPN Route Refcount 1 Virtual-Access2
00:47:56: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via Virtua
l-Access2 in IP DEFAULT TABLE with tag 0 distance 20
00:47:56: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0

00:47:56: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.0.0.110, sa_proto= 50,
sa_spi= 0x19E1175C(434181980),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 87
00:47:56: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.0.0.14, sa_proto= 50,
sa_spi= 0xADC90C5(182227141),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 88
00:47:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, chang
ed state to up
00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:47:56: IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP
00:47:56: IPSEC(key_engine_enable_outbound): enable SA with spi 182227141/50
00:47:56: IPSEC(update_current_outbound_sa): updated peer 10.0.0.14 current outb
ound sa to SPI ADC90C5

```

Router# **show ip route**

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

```

Gateway of last resort is 10.0.0.14 to network 0.0.0.0

```

C    192.200.200.0/24 is directly connected, Loopback0
    10.20.20.20/24 is subnetted, 1 subnets
C      10.30.30.30 is directly connected, Loopback4
C    192.168.5.0/24 is directly connected, Loopback3
    10.20.20.20/24 is subnetted, 2 subnets
S      10.3.1.0 [1/0] via 10.0.0.113
C      10.20.20.20 is directly connected, FastEthernet0/0
    192.168.6.0/32 is subnetted, 1 subnets
S      192.168.6.1 [20/0] via 0.0.0.0, Virtual-Access2
C    192.168.3.0/24 is directly connected, Loopback2
    10.15.0.0/24 is subnetted, 1 subnets
C      10.15.0.0 is directly connected, Loopback6
S*   0.0.0.0/0 [1/0] via 10.0.0.14

```

show crypto route Command Output: Example

The following output example displays routes, in one table, that are created through IPsec via RRI or Easy VPN VTIs:

Router# **show crypto route**

```

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
S - Static Map ACLs

```

```

Routes created in table GLOBAL DEFAULT
192.168.6.2/255.255.255.255 [0/0] via 10.0.0.133
                                on Virtual-Access3 RRI
10.1.1.0/255.255.255.0 [10/0] via Virtual-Access2 VTI
192.168.6.1/255.255.255.255 [0/0] via Virtual-Access2 VTI

```

Additional References

The following sections provide references related to Reverse Route Injection enhancements.

Related Documents

Related Topic	Document Title
Cisco IOS Security commands	Cisco IOS Security Command Reference
Other Cisco IOS commands	Cisco IOS Master Command List, Release 12.4T

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features

- **reverse-route**
- **set reverse-route**
- **show crypto route**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Feature Information for Reverse Route Injection

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Reverse Route Injection

Feature Name	Releases	Feature Information
Reverse Route Injection	12.1(9)E 12.2(8)T 12.2(8)YE	Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities. Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote Virtual Private Network (VPN) router as the next hop, the traffic is forced through the crypto process to be encrypted. The following sections provide information about this feature: <ul style="list-style-type: none"> “Reverse Route Injection” section on page 2 The following commands were introduced or modified by this feature: reverse-route .
Reverse Route Remote Peer Options	12.2(13)T 12.2(14)S	An enhancement was added to RRI to allow you to specify an interface or address as the explicit next hop to the remote VPN device. This functionality allows the overriding of a default route to properly direct outgoing encrypted packets. The following sections provide information about the remote peer options: <ul style="list-style-type: none"> “Enhancements to Reverse Route Injection in Cisco IOS Release 12.4(15)T” section on page 3.

Table 1 **Feature Information for Reverse Route Injection (continued)**

Feature Name	Releases	Feature Information
Reverse Route Injection Enhancements	12.3(14)T 12.2(33)SRA 12.2(33)SXH	<p>The following enhancements were added to the Reverse Route Injection feature:</p> <ul style="list-style-type: none"> • The default behavior of static crypto maps will be the same as that of dynamic crypto maps unless the reverse-route command and static keyword are used. • A route tag value was added for any routes that are created using RRI. • RRI can be configured on the same crypto map that is applied to multiple router interfaces. • RRI configured with the reverse-route remote-peer {ip-address} command, keyword, and argument will create one route instead of two. <p>The following sections provide information about the Reverse Route Injection enhancements:</p> <ul style="list-style-type: none"> • “Reverse Route Injection” section on page 2 • “Configuring RRI on Crypto Maps for Cisco IOS Releases Prior to 12.4(15)T” section on page 4 • “Configuring RRI with Enhancements Added in Cisco IOS Release 12.4(15)T” section on page 6 • “Configuring RRI When Crypto ACLs Exist: Example” section on page 10 • “Configuring RRI with Route Tags: Example” section on page 11 • “Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop: Example” section on page 12 <p>The following command was modified by these feature enhancements: reverse-route.</p>
Gateway Option	12.4(15)T	<p>This option allows you to configure unique next hops or gateways for remote tunnel endpoints.</p> <p>The following section provides information about the Gateway Option:</p> <ul style="list-style-type: none"> • “Gateway Option” section on page 3

Table 1 **Feature Information for Reverse Route Injection (continued)**

Feature Name	Releases	Feature Information
RRI Distance Metric	12.4(15)T	<p>This enhancement allows you to define a metric distance for each static route.</p> <p>The following sections provide information about the RRI distance metric enhancement.</p> <ul style="list-style-type: none"> • “RRI Distance Metric” section on page 3 • “Configuring a RRI Distance Metric Under an IPsec Profile” section on page 8 • “Configuring a RRI Distance Metric Under a Crypto Map: Example” section on page 12 • “debug and show Command Output for a RRI Metric Configuration Having a VTI: Example” section on page 14 <p>The following commands were introduced or modified by this feature: reverse-route, set reverse-route.</p>
show crypto route Command	12.4(15)T	This command displays routes that are created through IPsec via RRI or Easy VPN VTIs.
Support for RRI on IPsec Profiles	12.4(15)T	<p>This feature provides support for relevant RRI options on IPsec profiles that are predominantly used by VTIs.</p> <p>The following section provides information about the Support for RRI on IPsec Profiles feature:</p> <ul style="list-style-type: none"> • “Support for RRI on IPsec Profiles” section on page 4
Tag Option Configuration Changes	12.4(15)T	<p>The tag option is now supported with IPsec profiles under the set reverse-route tag command.</p> <p>The following section provides information about this feature enhancement:</p> <ul style="list-style-type: none"> • “Tag Option Configuration Changes” section on page 4
Reverse Route Injection (RRI)	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2009 Cisco Systems, Inc. All rights reserved.



IPsec VPN High Availability Enhancements

Feature History

Release	Modification
12.1(9)E	This feature was introduced in Cisco IOS Release 12.1(9)E.
12.2(8)T	This feature was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 and Cisco AS5800 platforms.
12.2(9)YE	This feature was integrated into Cisco IOS Release 12.2(9)YE.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

This feature module describes the IPsec VPN High Availability Enhancements. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 4](#)
- [Supported Standards, MIBs, and RFCs, page 5](#)
- [Configuration Tasks, page 6](#)
- [Configuration Examples, page 8](#)
- [Command Reference, page 10](#)

Feature Overview

The IPsec VPN High Availability Enhancements feature consists of two new features—[Reverse Route Injection](#) (RRI) and [Hot Standby Router Protocol and IPsec](#) (HSRP)—that work together to provide users with a simplified network design for VPNs, and reduced configuration complexity on remote peers with respect to defining gateway lists. When used together, RRI and HSRP provide a more reliable network design for VPNs and reduce configuration complexity on remote peers.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Reverse Route Injection

Reverse Route Injection (RRI) is a feature designed to simplify network design for Virtual Private Networks (VPNs) in which there is a requirement for redundancy or load balancing. RRI works with both dynamic and static crypto maps.

In the dynamic case, as remote peers establish IPsec security associations (SAs) with an RRI-enabled router, a static route is created for each subnet or host protected by that remote peer. For static crypto maps, a static route is created for each destination of an extended access list rule. When RRI is used on a static crypto map with an access control list (ACL), routes will always exist, even without the negotiation of IPsec SAs.



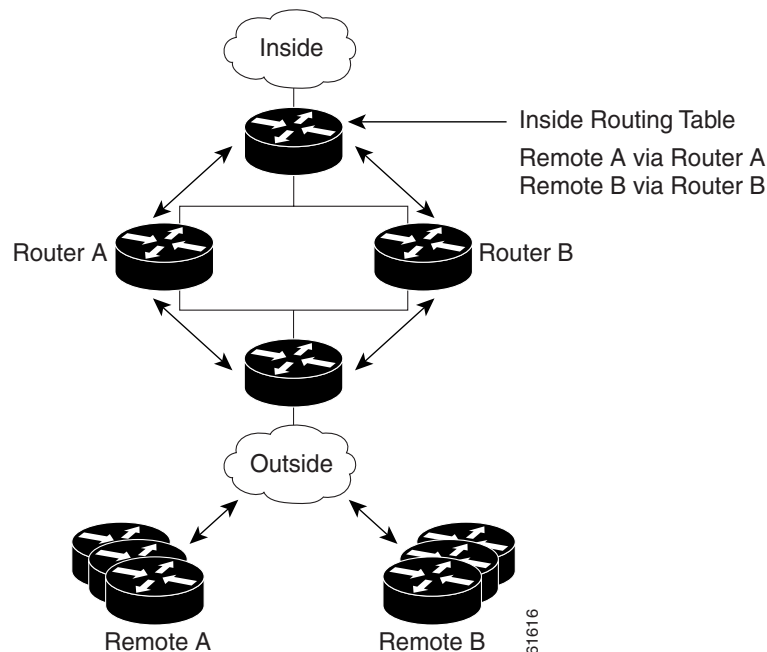
Note

Use of any keyword in ACLs with RRI is not supported.

When routes are created, they are injected into any dynamic routing protocol and distributed to surrounding devices. This traffic flows, requiring IPsec to be directed to the appropriate RRI router for transport across the correct SAs to avoid IPsec policy mismatches and possible packet loss.

Figure 87 shows a RRI configuration functionality topology. Remote A is being serviced by Router A and Remote B connected to Router B, providing load balancing across VPN gateways at the central site. RRI on the central site devices will ensure that the other router on the inside of the network can automatically make the correct forwarding decision. RRI also eliminates the need to administer static routes on the inside router.

Figure 87 **Topology Showing Reverse Route Injection Configuration Functionality**



Hot Standby Router Protocol and IPsec

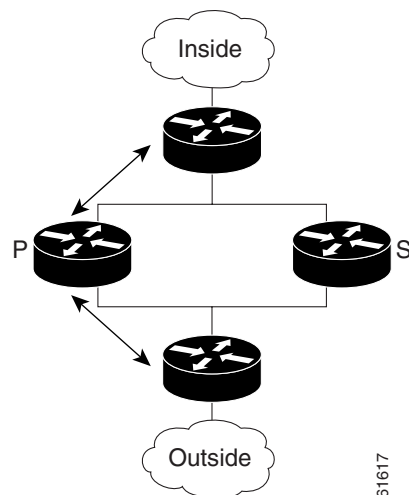
Hot Standby Router Protocol (HSRP) is designed to provide high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single router. HSRP is particularly useful for hosts that do not support a router discovery protocol, such as ICMP Router Discovery Protocol (IRDP), and do not have the functionality to switch to a new router when their selected router reloads or loses power. Without this functionality, a router that loses its default gateway because of a router failure is unable to communicate with the network.

HSRP is configurable on LAN interfaces using standby command-line interface (CLI) commands. It is now possible to use the standby IP address from an interface as the local IPsec identity, or local tunnel endpoint.

By using the standby IP address as the tunnel endpoint, failover can be applied to VPN routers by using HSRP. Remote VPN gateways connect to the local VPN router via the standby address that belongs to the *active* device in the HSRP group. In the event of failover, the *standby* device takes over ownership of the standby IP address and begins to service remote VPN gateways.

Figure 88 shows the enhanced HSRP functionality topology. Traffic is serviced by the active Router P, the active device in the standby group. In the event of failover, traffic is diverted to Router S, the original standby device. Router S assumes the role of the new active router and takes ownership of the standby IP address.

Figure 88 **Topology Showing Hot Standby Router Protocol Functionality**



Note

In case of a failover, HSRP does not facilitate IPsec state information transference between VPN routers. This means that without this state transference, SAs to remotes will be deleted requiring Internet Key Exchange (IKE) and IPsec SAs to be reestablished. To make IPsec failover more efficient, it is recommended that IKE keepalives be enabled on all routers.

Benefits

Reverse Route Injection

- Enables routing of IPsec traffic to a specific VPN headend device in environments that have multiple (redundant) VPN headend devices.

- Ensures predictable failover time of remote sessions between headend devices when using IKE keepalives, especially in environments in which remote device route flapping is common (not taking into consideration the effects of route convergence, which may vary depending on the routing protocol used and the size of the network).
- Eliminates the need for the administration of static routes on upstream devices as routes are dynamically learned by these devices.

Hot Standby Router Protocol with IPsec

Failover can be applied to VPN routers through the use of HSRP. Remote VPN gateways connect to the local VPN router through the standby address that belongs to the active device in the HSRP group. This functionality reduces configuration complexity on remote peers with respect to defining gateway lists because only the HSRP standby address needs to be defined.

Related Documents

- [*Stateful Failover for Ipsec*](#)
- [*SA-VAM2 Installation and Configuration Guide*](#)
- [*Release Notes for the SA-VAM2*](#)
- [*Cisco 7100 Series VPN Router Installation and Configuration Guide*](#)
- [*Cisco 7200 VXR Installation and Configuration Guide*](#)
- [*Cisco 7401ASR Installation and Configuration Guide*](#)

Supported Platforms

Cisco IOS Release 12.1(9)E and Cisco IOS Release 12.2(8)T

- Cisco 7100 series
- Cisco 7200VXR series

Cisco IOS Release 12.2(8)T Only

- Cisco 1710
- Cisco 1720
- Cisco 1750
- Cisco 1751
- Cisco 2600 series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco uBR7200

- Cisco uBR925

Cisco IOS Release 12.2(11)T Only

- Cisco AS5300 series
- Cisco AS5800 series

Cisco IOS Release 12.2(9)YE

- Cisco 7401ASR router

Cisco IOS Release 12.2(14)S

- Cisco 7200 series
- Cisco 7400 series

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Supported Standards, MIBs, and RFCs

Standards

- No new or modified standards are supported by this feature.

MIBs

- No new or modified standards are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

- No new or modified RFCs are supported by this feature.

Configuration Tasks

See the following sections for configuration tasks for the IPsec VPN High Availability Enhancements feature. Each task in the list is identified as either required or optional.

- [Configuring Reverse Route Injection on a Dynamic Crypto Map](#) (required)
- [Configuring Reverse Route Injection on a Static Crypto Map](#) (required)
- [Configuring HSRP with IPsec](#) (required)
- [Verifying VPN IPsec Crypto Configuration](#) (optional)

Configuring Reverse Route Injection on a Dynamic Crypto Map

Dynamic crypto map entries, like regular static crypto map entries, are grouped into sets. A set is a group of dynamic crypto map entries all with the same dynamic map name but each with a different dynamic sequence number. Each member of the set may be configured for RRI.

To create a dynamic crypto map entry and enable RRI, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router (config)# crypto dynamic map-name seq-num	Creates a dynamic crypto map entry and enters crypto map configuration mode.
Step 2	Router (config-crypto-m)# set transform-set	Specifies which transform sets are allowed for the crypto map entry. Lists multiple transform sets in order of priority (highest priority first). This entry is the only configuration statement required in dynamic crypto map entries.
Step 3	Router (config-crypto-m)# reverse-route	Creates source proxy information.

Configuring Reverse Route Injection on a Static Crypto Map

Before configuring RRI on a static crypto map, please note the following items:

- Routes are not created based on access list 102 as reverse-route is not enabled on mymap 2. RRI is not enabled by default and is not displayed in the router configuration.
- Enable a routing protocol to distribute the VPN routes to upstream devices.
- If Cisco Express Forwarding (CEF) is run on a VPN router configured for RRI, adjacencies need to be formed for each RRI injected network through the next hop device. As the next hop is not explicitly defined in the routing table for these routes, proxy-ARP should be enabled on the next hop router which allows the CEF adjacency to be formed using the layer two addresses of that device. In cases where there are many RRI injected routes, adjacency tables may become quite large as an entry is created for each device from each of the subnets represented by the RRI route. This issue is to be resolved in a future release.

To add RRI to a static crypto map set, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router (config)# crypto map map-name seq-num ipsec-isakmp	Adds a dynamic crypto map set to a static crypto map set and enters interface configuration mode.
Step 2	Router (config-if)# set peer ip address	Specifies an IPsec peer IP address in a crypto map entry.
Step 3	Router (config-if)# reverse-route	Creates dynamically static routes based on crypto access control lists (ACLs).
Step 4	Router (config-if)# match address	Specifies an extended access list for a crypto map entry.
Step 5	Router (config-if)# set transform-set	Specifies which transform sets are allowed for the crypto map entry. Lists multiple transform sets in order of priority (highest priority first).

Configuring HSRP with IPsec

When configuring HSRP with IPsec, the following conditions may apply:

- When HSRP is applied to a crypto map on an interface, the crypto map must be reapplied if the standby IP address or the standby name is changed on that interface.
- If HSRP is applied to a crypto map on an interface, and the user deletes the standby IP address or the standby name from that interface, the crypto tunnel endpoint is reinitialized to the actual IP address of that interface.
- If a user adds the standby IP address and the standby name to an interface with the requirement IPsec failover, the crypto map must be reapplied with the appropriate redundancy information.
- Standby priorities should be equal on active and standby routers. If they are not, the higher priority router takes over as the active router. If the old active router comes back up and immediately assumes the active role before having time to report itself standby and sync, connections will be dropped.
- The IP addresses on the HSRP-tracked interfaces on the standby and active routers should both be either lower or higher on one router than the other. In the case of equal priorities (an HA requirement), HSRP will assign the active state-based IP address. If an addressing scheme exists so that the public IP address of router A is lower than the public IP address of router B, but the opposite is true for their private interfaces, an active/standby-standby/active split condition could exist which will break connectivity.



Note

To configure HSRP without IPsec refer to the “[Configuring IP Services](#)” chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2.

To apply a crypto map set to an interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router (config)# interface <i>type slot/port</i>	Specifies an interface and enters interface configuration mode.
Step 2	Router (config-if)# standby name <i>group-name</i>	Specifies the standby group name (required).
Step 3	Router (config-if)# standby ip <i>ip-address</i>	Specifies the IP address of the standby groups (required for one device in the group).
Step 4	Router (config-if)# crypto map map-name redundancy [standby-name]	Specifies IP redundancy address as the tunnel endpoint for IPsec.

Verifying VPN IPsec Crypto Configuration

To verify your VPN IPsec crypto configuration, use the following EXEC commands:

Command	Purpose
Router# show crypto ipsec transform-set	Displays your transform set configuration.
Router# show crypto map [interface <i>interface</i> tag map-name]	Displays your crypto map configuration.
Router# show crypto ipsec sa [map map-name address identity] [detail]	Displays information about IPsec SAs.
Router# show crypto dynamic-map [tag map-name]	Displays information about dynamic crypto maps.

Configuration Examples

This section provides the following configuration examples:

- [Reverse Route Injection on a Dynamic Crypto Map Example](#)
- [Reverse Route Injection on a Static Crypto Map Example](#)
- [HSRP and IPsec Example](#)

Reverse Route Injection on a Dynamic Crypto Map Example

In the following example, using the reverse route crypto map subcommand in the definition of the dynamic crypto map template ensures that routes are created for any remote proxies (subnets or hosts), protected by the connecting remote IPsec peers.

```
crypto dynamic mydynmap 1
  set transform-set esp-3des-sha
  reverse-route
```


This template is then associated with a “parent” crypto map statement and then applied to an interface.

```
crypto map mymap 3 ipsec-isakmp dynamic mydynmap

interface FastEthernet 0/0
crypto map mymap
```

Reverse Route Injection on a Static Crypto Map Example

RRI is a good solution for topologies that require encrypted traffic to be diverted to a VPN router and all other traffic to a different router.

In these scenarios, RRI eliminates the need to manually define static routes on devices.

RRI is not required if a single VPN router is used and all traffic passes through the VPN router during its path in and out of the network.

If the user chooses to manually define static routes on the VPN router for remote proxies, and have these routes permanently installed in the routing table, RRI should not be enabled on the crypto map instance that covers the same remote proxies. In this case, there is no possibility of user defined static routes being removed by RRI.

Routing convergence can affect the success of a failover based on the routing protocol used to advertise routes (link state versus periodic update). It is recommended that a link state routing protocol such as OSPF be used to help speed convergence time by ensuring that routing updates are sent as soon as a change in routing state is detected.

In the following example, RRI is enabled for mymap 1, but not for mymap 2. Upon the application of the crypto map to the interface, a route is created based on access-list 101 analogous to the following:

```
IP route 172.17.11.0 255.255.255.0 FastEthernet 0/0

crypto map mymap 1 ipsec-isakmp
  set peer 172.17.11.1
  reverse-route
  set transform-set esp-3des-sha
  match address 101
crypto map mymap 2 ipsec-isakmp
  set peer 10.1.1.1
  set transform-set esp-3des-sha
  match address 102

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255

interface FastEthernet 0/0
  crypto map mymap
```

HSRP and IPsec Example

The following example shows how all remote VPN gateways connect to the router via 192.168.0.3. The crypto map on the interface binds this standby address as the local tunnel endpoint for all instances of *mymap* and at the same time ensures that HSRP failover is facilitated between an active and standby device belonging to the same standby group, group1.

Note that RRI is also enabled to provide the ability for only the *active* device in the HSRP group to be advertising itself to inside devices as the next hop VPN gateway to the remote proxies. If there is a failover, routes are deleted on the formerly active device and created on the newly active device.

```
crypto map mymap 1 ipsec-isakmp
    set peer 10.1.1.1
    reverse-route
    set transform-set esp-3des-sha
    match address 102

Interface FastEthernet 0/0
    ip address 192.168.0.2 255.255.255.0
    standby name group1
    standby ip 192.168.0.3
    crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

The standby name needs to be configured on all devices in the standby group and the standby address needs to be configured on at least one member of the group. If the standby name is removed from the router, the IPsec SAs will be deleted. If the standby name is added again, regardless of whether the same name or a different name is used, the crypto map (using the redundancy option) will have to be reapplied to the interface.

Command Reference

The following commands are introduced or modified in the feature or features:
documented in this module:

- [crypto map \(interface IPsec\)](#)
- [reverse-route](#)

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2009 Cisco Systems, Inc. All rights reserved.



IPsec Preferred Peer

First Published: March 28, 2005

Last Updated: August 21, 2007

The IP Security (IPsec) Preferred Peer feature allows you to control the circumstances by which multiple peers on a crypto map are tried in a failover scenario.

This feature includes the following capabilities:

- Default peer configuration
- IPsec idle-timer usage with default peer

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for IPsec Preferred Peer” section on page 9](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for IPsec Preferred Peer, page 2](#)
- [Restrictions for IPsec Preferred Peer, page 2](#)
- [Information About IPsec Preferred Peer, page 2](#)
- [How to Configure IPsec Preferred Peer, page 4](#)
- [Configuration Examples for IPsec Preferred Peer, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 9](#)
- [Feature Information for IPsec Preferred Peer, page 9](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Glossary, page 10](#)

Prerequisites for IPsec Preferred Peer

- You must have a properly defined, complete crypto map.

Restrictions for IPsec Preferred Peer

Default peer:

- This feature must be used in conjunction with Dead Peer Detection (DPD). It is most effective on a remote site running DPD in periodic mode. DPD detects the failure of a device quickly and resets the peer list so that the default peer is tried for the next attempted connection.
- Only one peer can be designated as the default peer in a crypto map.
- The default peer must be the first peer in the peer list.

IPsec idle-timer usage with default peer:

- This feature works only on the crypto map for which it is configured. You cannot configure the capability globally for all crypto maps.
- If there is a global idle timer, the crypto map idle-timer value must be different from the global value; otherwise, the idle timer is not added to the crypto map.

Information About IPsec Preferred Peer

To configure IPsec Preferred Peer, you need to understand the following concepts:

- [IPsec, page 2](#)
- [Dead Peer Detection, page 3](#)
- [Default Peer Configuration, page 3](#)
- [Idle Timers, page 4](#)
- [IPsec Idle-Timer Usage with Default Peer, page 4](#)
- [Peers on Crypto Maps, page 4](#)

IPsec

IPsec is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPsec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating Internet Protocol (IP) packets between participating IPsec devices (peers), such as Cisco routers.

IPsec provides the following network security services. These services are optional. In general, local security policy dictates the use of one or more of these services:

- **Data Confidentiality**—The IPsec sender can encrypt packets before transmitting them across a network.

- **Data Integrity**—The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.
- **Data Origin Authentication**—The IPsec receiver can authenticate the source of the IPsec packets sent.
- **Anti-Replay**—The IPsec receiver can detect and reject replayed packets.

With IPsec, data can be transmitted across a public network without fear of observation, modification, or spoofing. This enables applications such as Virtual Private Networks (VPNs), including intranets, extranets, and remote user access.

IPsec provides secure tunnels between two peers, such as two routers. You define which packets are considered sensitive and should be sent through these secure tunnels, and you define the parameters that should be used to protect these sensitive packets, by specifying characteristics of these tunnels. When the IPsec peer sees such a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

Dead Peer Detection

The VPN Client uses a keepalive mechanism called Dead Peer Detection (DPD) to check the availability of the VPN device on the other side of an IPsec tunnel. If the network is unusually busy or unreliable, you can increase the number of seconds that the VPN Client will wait before deciding whether the peer is no longer active.

Keepalive packets are not sent if traffic is received. This lowers the overhead associated with DPD, because on a heavily loaded network very few keepalive packets will be sent because traffic is being received on the tunnels. In addition, DPD sends keepalive packets only if there is user traffic to send (and no user traffic is received).

You can configure Internet Key Exchange (IKE) DPD so that DPD sends the keepalive packets whether or not there is outbound user data. That is, as long as there is no inbound user data, the keepalive packets are sent at the configured keepalive interval.

Default Peer Configuration

If a connection timeout occurs, the connection to the current peer is closed. The **set peer** command allows you to configure the first peer as the default peer. If there is a default peer, the next time a connection is initiated, the connection is directed to the default peer instead of to the next peer in the peer list. If the default peer is unresponsive, the next peer in the peer list becomes the current peer and future connections through the crypto map try that peer.

This capability is useful when traffic on a physical link stops due to the failure of a remote peer. DPD indicates that the remote peer is unavailable, but that peer remains the current peer.

A default peer facilitates the failover to a preferred peer that was previously unavailable, but has returned to service. Users can give preference to certain peers in the event of a failover. This is useful if the original failure was due to a network connectivity problem rather than failure of the remote peer.

Idle Timers

When a router running Cisco IOS software creates an IPsec security association (SA) for a peer, resources must be allocated to maintain the SA. The SA requires both memory and several managed timers. For idle peers, these resources are wasted. If enough resources are wasted by idle peers, the router could be prevented from creating new SAs with other peers.

IPsec SA idle timers increase the availability of resources by deleting SAs associated with idle peers. Because IPsec SA idle timers prevent the wasting of resources by idle peers, more resources are available to create new SAs when required.

If IPsec SA idle timers are not configured, only the global lifetimes for IPsec SAs are applied. SAs are maintained until the global timers expire, regardless of peer activity.

IPsec Idle-Timer Usage with Default Peer

If all connections to the current peer time out, the next time a connection is initiated it is directed to the default peer configured in the **set peer** command. If a default peer is not configured and there is a connection timeout, the current peer remains the one that timed out.

This enhancement helps facilitate a failover to a preferred peer that was previously unavailable but is in service now.

Peers on Crypto Maps

A crypto map set can contain multiple entries, each with a different access list. The router searches the crypto map entries in order, and attempts to match the packet to the access list specified in that entry.

When a packet matches a **permit** entry in a particular access list, and the corresponding crypto map entry is tagged as Cisco, connections are established with the remote peer as specified in the set peer statements within the crypto map.

How to Configure IPsec Preferred Peer

This section contains the following procedures:

- [Configuring a Default Peer, page 4](#) (required)
- [Configuring the Idle Timer, page 5](#) (optional)

Configuring a Default Peer

To configure a default peer, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

4. **set peer** {*host-name* [dynamic] [default] | *ip-address* [default] }
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name</i> <i>seq-num</i> [ipsec-isakmp] [dynamic <i>dynamic-map-name</i>] [discover] [profile <i>profile-name</i>] Example: Router(config)# crypto map mymap 10 ipsec-isakmp	Enters crypto map configuration mode. Creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list.
Step 4	set peer { <i>host-name</i> [dynamic] [default] <i>ip-address</i> [default] } Example: Router(config-crypto-map)# set peer 10.0.0.2 default	Specifies an IPsec peer in a crypto map entry. Ensures that the first peer specified is defined as the default peer.
Step 5	exit Example: Router(config-crypto-map)# exit	Exits crypto map configuration mode and returns to global configuration mode.

Configuring the Idle Timer

To configure the idle timer, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name* *seq-num* [ipsec-isakmp] [dynamic *dynamic-map-name*] [discover] [profile *profile-name*]
4. **set security-association idletime** *seconds* [default]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-num</i> [ipsec-isakmp] [dynamic <i>dynamic-map-name</i>] [discover] [profile <i>profile-name</i>] Example: Router(config)# crypto map mymap 10 ipsec-isakmp	Enters crypto map configuration mode. Creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list.
Step 4	set security-association idletime <i>seconds</i> [default] Example: Router(config-crypto-map)# set security-association idletime 120 default	Specifies the maximum amount of time for which the current peer can be idle before the default peer is used.
Step 5	exit Example: Router(config-crypto-map)# exit	Exits crypto map configuration mode and returns to global configuration mode.

Configuration Examples for IPsec Preferred Peer

- [Configuring a Default Peer: Example, page 6](#)
- [Configuring the IPsec Idle Timer: Example, page 6](#)

Configuring a Default Peer: Example

The following example shows that the first peer, at IP address 10.1.1.1, is the default peer:

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
```

Configuring the IPsec Idle Timer: Example

In the following example, if the current peer is idle for 120 seconds, the default peer 10.1.1.1 (which was specified in the **set peer** command) is used for the next attempted connection:

```
crypto map tohub 1 ipsec-isakmp
```

```
set peer 10.1.1.1 default
set peer 10.2.2.2
set security-association idletime 120 default
```

Additional References

The following sections provide references related to IPsec Preferred Peer.

Related Documents

Related Topic	Document Title
IPsec	Security for VPNs with IPsec
Crypto map	<ul style="list-style-type: none"> • Security for VPNs with IPsec • Configuring Internet Key Exchange for IPsec VPNs
DPD	IPsec Dead Peer Detection Periodic Message Option
Security commands	Cisco IOS Security Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features

- **set peer (IPsec)**
- **set security-association idle-time**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Feature Information for IPsec Preferred Peer

[Table 1](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 **Feature Information for IPsec Preferred Peer**

Feature Name	Releases	Feature Information
IPsec Preferred Peer	12.3(14)T 12.2(33)SRA 12.2(33)SXH	The IPsec Preferred Peer feature allows you to control the circumstances by which multiple peers on a crypto map are tried in a failover scenario. In 12.3(14)T, this feature was introduced. In 12.2(33)SRA, this feature, the set peer (IPsec) command, and the set security-association idle-time command were integrated into this release.
IPSEC Preferred Peer	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Glossary

crypto access list—A list that defines which IP traffic will be protected by crypto and which traffic will not be protected by crypto.

crypto map—A map that specifies which traffic should be protected by IPsec, where IPsec-protected traffic should be sent, and what IPsec transform sets should be applied to this traffic.

dead peer detection—A feature that allows the router to detect an unresponsive peer.

keepalive message—A message sent by one network device to inform another network device that the virtual circuit between the two is still active.

peer—Router or other device that participates in IPsec and IKE. In IPsec, peers are devices or entities that communicate securely either through the exchange of keys or the exchange of digital certificates.

SA—security association. An instance of security policy and keying material applied to a data flow. Both IKE and IPsec use SAs, although SAs are independent of one another. IPsec SAs are unidirectional and are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPsec SA, it is bidirectional. IKE negotiates and establishes SAs on behalf of IPsec. A user also can establish IPsec SAs manually. A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports Encapsulating Security Payload (ESP) between peers, one ESP SA is required for each direction. SAs are identified uniquely by destination (IPsec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

transform set—An acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. During the IPsec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Real-Time Resolution for IPsec Tunnel Peer

After a user specifies a host name (instead of an IP address) for remote IP Security (IPsec) peer, the Real-Time Resolution for IPsec Tunnel Peer feature allows the host name to be domain name server (DNS) resolved before the router establishes the IPsec tunnel. Thus, the router can immediately discover whether the IP address of the peer has changed.

Feature History for Real-Time Resolution for IPsec Tunnel Peer

Release	Modification
12.3(4)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Real-Time Resolution for IPsec Tunnel Peer, page 2](#)
- [Information About Real-Time Resolution for IPsec Tunnel Peer, page 2](#)
- [How to Configure Real-Time Resolution, page 2](#)
- [Configuration Examples for Real-Time Resolution, page 4](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Real-Time Resolution for IPsec Tunnel Peer

Secure DNS Requirement

It is recommended that you use this feature only with secure DNS and when the DNS responses can be authenticated. Otherwise, an attacker can spoof or forge DNS responses and have access to Internet Key Exchange (IKE) authentication data, such as a certificate. If an attacker has a certificate that is trusted by the initiating host, the attacker can successfully establish Phase 1 IKE security association (SA), or the attacker can try to guess the preshared key that is shared between the initiator and the actual responder.

DNS Initiator

DNS names resolution for remote IPsec peers will work only if they are used as an initiator. The first packet that is to be encrypted will trigger a DNS lookup; after the DNS lookup is complete, subsequent packets will trigger IKE.

Information About Real-Time Resolution for IPsec Tunnel Peer

To configure real-time resolution for your IPsec peer, you should understand the following concept:

- [Benefits of Real-Time Resolution Via Secure DNS, page 2](#)

Benefits of Real-Time Resolution Via Secure DNS

When specifying the host name of a remote IPsec peer via the **set peer** command, you can also issue the **dynamic** keyword, which defers DNS resolution of the host name until right before the IPsec tunnel has been established. Deferring resolution enables the Cisco IOS software to detect whether the IP address of the remote IPsec peer has changed. Thus, the software can contact the peer at the new IP address.

If the **dynamic** keyword is not issued, the host name is resolved immediately after it is specified. So, the Cisco IOS software cannot detect an IP address change and, therefore, attempts to connect to the IP address that it previously resolved.

DNS resolution assures users that their established IPsec tunnel is secure and authenticated.

How to Configure Real-Time Resolution

This section contains the following procedure:

- [Configuring Real-Time Resolution for IPsec Peers, page 2](#)

Configuring Real-Time Resolution for IPsec Peers

Use this task to configure a router to perform real-time DNS resolution with a remote IPsec peer; that is, the host name of peer is resolved via a DNS lookup right before the router establishes a connection (an IPsec tunnel) with the peer.

Prerequisites

Before creating a crypto map, you should perform the following tasks:

- Define Internet Security Association Key Management Protocol (ISAKMP) policies.
- Define IPsec transform sets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num ipsec-isakmp*
4. **match address** *access-list-id*
5. **set peer** {*host-name* [**dynamic**] | *ip-address*}
6. **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	crypto map <i>map-name seq-num ipsec-isakmp</i>	Specifies the crypto map entry to create (or modify) and enters crypto map configuration mode.
	Example: Router(config)# crypto map secure_b 10 ipsec-isakmp	
Step 4	match address <i>access-list-id</i>	Names an extended access list.
	Example: Router(config-crypto-m)# match address 140	This access list determines which traffic should be protected by IPsec and which traffic should not be protected by IPsec in the context of this crypto map entry.

	Command or Action	Purpose
Step 5	set peer {host-name [dynamic] ip-address} Example: Router(config-crypto-m)# set peer b.cisco.com dynamic	Specifies a remote IPsec peer. This is the peer to which IPsec-protected traffic can be forwarded. <ul style="list-style-type: none"> dynamic—Allows the host name to be resolved via a DNS lookup just before the router establishes the IPsec tunnel with the remote peer. If this keyword is not specified, the host name will be resolved immediately after the host name is specified. Repeat for multiple remote peers.
Step 6	set transform-set transform-set-name1 [transform-set-name2...transform-set-name6] Example: Router(config-crypto-m)# set transform-set myset	Specifies which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).

Troubleshooting Tips

To display crypto map configuration information, use the **show crypto map** command.

What to Do Next

You need to apply a crypto map set to each interface through which IPsec traffic will flow. Applying the crypto map set to an interface instructs the router to evaluate all the interface's traffic against the crypto map set and to use the specified policy during connection or security association (SA) negotiation on behalf of traffic to be protected by crypto.

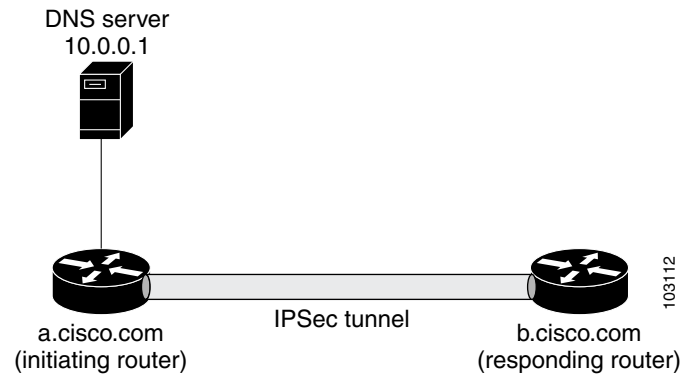
Configuration Examples for Real-Time Resolution

This section provides the following configuration example:

- [Configuring Real-Time Resolution for an IPsec Peer: Example, page 4](#)

Configuring Real-Time Resolution for an IPsec Peer: Example

[Figure 1](#) and the following example illustrate how to create a crypto map that configures the host name of a remote IPsec peer to DNS resolved via a DNS lookup right before the Cisco IOS software attempts to establish a connection with that peer.

Figure 1 **Real-Time Resolution Sample Topology**

```

! Configure the initiating router.
hostname a.cisco.com
ip domain name cisco.com
ip name server 10.0.0.1
!
crypto map secure_b 10 ipsec-isakmp
  match address 140
  set peer b.cisco.com dynamic
  set transform-set xset
interface serial1
  ip address 30.0.0.1
  crypto map secure_b
access-list 140 permit ...
!
! Configure the responding router (the remote IPsec peer).
hostname b.cisco.com
!
crypto map secure_a 10 ipsec-isakmp
  match address 150
  set peer 30.0.0.1
  set transform-set
interface serial0/1
  ip address 40.0.0.1
  crypto map secure_a
access-list 150 ...

! DNS server configuration

b.cisco.com    40.0.0.1      # the address of serial0/1 of b.cisco.com

```

Additional References

The following sections provide references related to Real-Time Resolution for IPsec Tunnel Peer.

Related Documents

Related Topic	Document Title
Crypto maps	Security for VPNs with IPsec
ISAKMP policies	Configuring Internet Key Exchange for IPsec VPNs
IPsec and IKE configuration commands	Cisco IOS Security Command Reference

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features

- **set peer (IPsec)**

For information about these commands, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



IPsec Data Plane



IPsec Anti-Replay Window: Expanding and Disabling

First Published: February 28, 2005
Last Updated: September 12, 2006

Cisco IP security (IPsec) authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. The decryptor keeps track of which packets it has seen on the basis of these numbers. Currently, the default window size is 64 packets. Generally, this number (window size) is sufficient, but there are times when you may want to expand this window size. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

History for the IPsec Anti-Replay Window: Expanding and Disabling Feature

Release	Modification
12.3(14)T	This feature was introduced.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF6	This feature was integrated into Cisco IOS Release 12.2(18)SXF6.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for IPsec Anti-Replay Window: Expanding and Disabling, page 2](#)
- [Information About IPsec Anti-Replay Window: Expanding and Disabling, page 2](#)
- [How to Configure IPsec Anti-Replay Window: Expanding and Disabling, page 3](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for IPsec Anti-Replay Window: Expanding and Disabling, page 5](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)

Prerequisites for IPsec Anti-Replay Window: Expanding and Disabling

- Before configuring this feature, you should have already created a crypto map or crypto profile.

Information About IPsec Anti-Replay Window: Expanding and Disabling

To configure the IPsec Anti-Replay Window: Expanding and Disabling feature, you should understand the following concept:

- [IPsec Anti-Replay Window, page 2](#)

IPsec Anti-Replay Window

Cisco IPsec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association [SA] anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, Cisco quality of service (QoS) gives priority to high-priority packets, which could cause some low-priority packets to be discarded even though they could be one of the last 64 packets received by the decryptor. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed to store the sequence number on the decryptor. It is recommended that you use the full 1024 window size to eliminate any future anti-replay problems.

How to Configure IPsec Anti-Replay Window: Expanding and Disabling

This section contains the following procedures:

- [Configuring IPsec Anti-Replay Window: Expanding and Disabling Globally, page 3](#) (optional)
- [Configuring IPsec Anti-Replay Window: Expanding and Disabling on a Crypto Map, page 4](#) (optional)

Configuring IPsec Anti-Replay Window: Expanding and Disabling Globally

To configure IPsec Anti-Replay Window: Expanding and Disabling globally (so that it affects all SAs that are created— except for those that are specifically overridden on a per-crypto map basis), perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association replay window-size [N]**
4. **crypto ipsec security-association replay disable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec security-association replay window-size [N] Example: Router (config)# crypto ipsec security-association replay window-size 256	Sets the size of the SA replay window globally. Note Configure this command or the crypto ipsec security-association replay disable command. The two commands are not used at the same time.
Step 4	crypto ipsec security-association replay disable Example: Router (config)# crypto ipsec security-association replay disable	Disables checking globally. Note Configure this command or the crypto ipsec security-association replay window-size command. The two commands are not used at the same time.

Configuring IPsec Anti-Replay Window: Expanding and Disabling on a Crypto Map

To configure IPsec Anti-Replay Window: Expanding and Disabling on a crypto map so that it affects those SAs that have been created using a specific crypto map or profile, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**]
4. **set security-association replay window-size** [*N*]
5. **set security-association replay disable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-num</i> [ipsec-isakmp] Example: Router (config)# crypto map ETH0 17 ipsec-isakmp	Enters crypto map configuration mode and creates a crypto profile that provides a template for configuration of dynamically created crypto maps.
Step 4	set security-association replay window-size [<i>N</i>] Example: Router (crypto-map)# set security-association replay window-size 128	Controls the SAs that are created using the policy specified by a particular crypto map, dynamic crypto map, or crypto profile. Note Configure this command or the set security-association replay disable command. The two commands are not used at the same time.
Step 5	set security-association replay disable Example: Router (crypto-map)# set security-association replay disable	Disables replay checking for a particular crypto map, dynamic crypto map, or crypto profile. Note Configure this command or the set security-association replay window-size command. The two commands are not used at the same time.

Troubleshooting Tips

- If your replay window size has not been set to a number that is high enough for the number of packets received, you will receive a system message such as the following:

```
*Nov 17 19:27:32.279: %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
connection id=1
```

The above message is generated when a received packet is judged to be outside the anti-replay window.

Configuration Examples for IPsec Anti-Replay Window: Expanding and Disabling

This section includes the following configuration examples:

- [Global Expanding and Disabling of an Anti-Replay Window: Example, page 5](#)
- [Expanding and Disabling of an Anti-Replay Window for a Particular Crypto Map, Dynamic Crypto Map, or Crypto Profile: Example, page 6](#)

Global Expanding and Disabling of an Anti-Replay Window: Example

The following example shows that the anti-replay window size has been set globally to 1024:

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Gateway1
!

boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 192.165.201.2 !
crypto ipsec security-association replay window-size 1024 !
crypto ipsec transform-set basic esp-des esp-md5-hmac !
crypto map mymap 10 ipsec-isakmp
 set peer 192.165.201.2
 set transform-set basic
 match address 101
!
!
```

```

interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
 ip address 192.165.200.2 255.255.255.252 serial restart-delay 0 crypto map mymap !
 ip classless
 ip route 0.0.0.0 0.0.0.0 192.165.200.1
 no ip http server
 no ip http secure-server
!
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.2.0 0.0.0.255 access-list 101
remark Crypto ACL
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end

```

Expanding and Disabling of an Anti-Replay Window for a Particular Crypto Map, Dynamic Crypto Map, or Crypto Profile: Example

The following example shows that anti-replay checking is disabled for IPsec connections to 172.17.150.2 but enabled (and the default window size is 64) for IPsec connections to 172.17.150.3 and 172.17.150.4:

```

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname networkserver1
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPn.tErFZl enable password ww !
ip subnet-zero
!
cns event-service server

crypto isakmp policy 1
authentication pre-share

crypto isakmp key cisco170 address 172.17.150.2 crypto isakmp key cisco180 address
172.17.150.3 crypto isakmp key cisco190 address 172.17.150.4

crypto ipsec transform-set 170cisco esp-des esp-md5-hmac crypto ipsec transform-set
180cisco esp-des esp-md5-hmac crypto ipsec transform-set 190cisco esp-des esp-md5-hmac

crypto map ETH0 17 ipsec-isakmp
 set peer 172.17.150.2
 set security-association replay disable set transform-set 170cisco match address 170
crypto map ETH0 18 ipsec-isakmp set peer 192.168.1.3 set transform-set 180cisco match
address 180 crypto map ETH0 19 ipsec-isakmp set peer 192.168.1.4 set transform-set
190cisco match address 190 !
interface Ethernet0
 ip address 172.17.150.1 255.255.255.0

```



```
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map ETH0
!
interface Serial0
 ip address 172.16.160.1 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
!
ip classless
ip route 172.18.170.0 255.255.255.0 172.17.150.2 ip route 172.19.180.0 255.255.255.0
172.17.150.3 ip route 172.20.190.0 255.255.255.0 172.17.150.4 no ip http server !

access-list 170 permit ip 172.16.160.0 0.0.0.255 172.18.170.0 0.0.0.255 access-list 180
permit ip 172.16.160.0 0.0.0.255 172.19.180.0 0.0.0.255 access-list 190 permit ip
172.16.160.0 0.0.0.255 172.20.190.0 0.0.0.255 !
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
```

```
password ww
login
end
```

Additional References

The following sections provide references related to IPsec Anti-Replay Window: Expanding and Disabling.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Security Command Reference
IP security and encryption	Configuring Security for VPNs with IPsec

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features

- **crypto ipsec security-association replay disable**
- **crypto ipsec security-association replay window-size**
- **set security-association replay disable**
- **set security-association replay window-size**

For information about these commands, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Pre-Fragmentation for IPsec VPNs

Feature History

Release	Modification
12.1(11b)E	This feature was introduced.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This feature module describes the Pre-fragmentation for IPsec VPNs feature in Cisco IOS Release 12.2(13)T and 12.2(14)S. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 5](#)
- [Configuration Tasks, page 5](#)
- [Configuration Examples, page 7](#)
- [Command Reference, page 8](#)

Feature Overview

When a packet is nearly the size of the maximum transmission unit (MTU) of the outbound link of the encrypting router, and it is encapsulated with IPsec headers, it is likely to exceed the MTU of the outbound link. This causes packet fragmentation after encryption, which makes the decrypting router reassemble in the process path. Pre-fragmentation for IPsec VPNs increases the decrypting router's performance by enabling it to operate in the high performance CEF path instead of the process path.

This feature allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPsec security association (SA). If it is predetermined that the packet will exceed the MTU of the output interface, the packet is fragmented before encryption. This function avoids process level reassembly before decryption and helps improve decryption performance and overall IPsec traffic throughput.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

**Note**

The pre-fragmentation feature is turned off by default for tunnel interfaces. To receive pre-fragmentation performance benefits, turn pre-fragmentation on after insuring that the tunnel interfaces have the same MTU on both ends.

Benefits

Increased Performance

Delivers encryption throughput at maximum encryption hardware accelerator speeds. This performance increase is for near MTU-sized packets.

Uniform Fragmentation

Packets are fragmented into equally sized units to prevent further downstream fragmentation.

Interoperability

This feature is interoperable with all Cisco IOS platforms and a number of Cisco VPN clients.

Restrictions

Take the following information into consideration before this feature is configured:

- Pre-fragmentation for IPsec VPNs operates in IPsec tunnel mode and IPsec tunnel mode with GRE, but not with IPsec transport mode.
- Pre-fragmentation for IPsec VPNs configured on the decrypting router in a unidirectional traffic scenario does not improve the performance or change the behavior of either of the peers.
- Pre-fragmentation for IPsec VPNs occurs before the transform is applied if compression is turned on for outgoing packets.
- Pre-fragmentation for IPsec VPNs functionality depends on the egress interface **crypto ipsec df-bit** configuration and the incoming packet “do not fragment” (DF) bit state. See [Table 1](#).

Table 1 *Pre-Fragmentation for IPsec VPNs Dependencies*

Pre-Fragmentation for IPsec VPNs Feature State (Enabled/Disabled)	Egress Interface “crypto ipsec df-bit” Configuration	Incoming Packet DF Bit State	Result
Enabled	crypto ipsec df-bit clear	0	Fragmentation occurs before encryption.
Enabled	crypto ipsec df-bit clear	1	Fragmentation occurs before encryption.
Disabled	crypto ipsec df-bit clear	0	Fragmentation occurs after encryption and packets are reassembled before decryption.

Table 1 *Pre-Fragmentation for IPsec VPNs Dependencies (continued)*

Pre-Fragmentation for IPsec VPNs Feature State (Enabled/Disabled)	Egress Interface “crypto ipsec df-bit” Configuration	Incoming Packet DF Bit State	Result
Disabled	crypto ipsec df-bit clear	1	Fragmentation occurs after encryption and packets are reassembled before decryption.
Enabled	crypto ipsec df-bit set	0	Fragmentation occurs before encryption.
Enabled	crypto ipsec df-bit set	1	Packets are dropped.
Disabled	crypto ipsec df-bit set	0	Fragmentation occurs after encryption and packets are reassembled before decryption.
Disabled	crypto ipsec df-bit set	1	Packets are dropped.
Enabled	crypto ipsec df-bit copy	0	Fragmentation occurs before encryption.
Enabled	crypto ipsec df-bit copy	1	Packets are dropped.
Disabled	crypto ipsec df-bit copy	0	Fragmentation occurs after encryption and packets are reassembled before decryption.
Disabled	crypto ipsec df-bit copy	1	Packets are dropped.

Supported Platforms

12.2(14)S and higher

The Pre-fragmentation for IPsec VPN feature is supported on the following platforms:

- Cisco 7200 series
- Cisco 7400 series

12.2(13)T

The Pre-fragmentation for IPsec VPN feature is supported on all platforms using Cisco IOS Release 12.2(13)T or higher, including:

- Cisco 1710
- Cisco 1720
- Cisco 1721
- Cisco 1751

- Cisco 1760
- Cisco 2600
- Cisco 2691
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7400 series

12.1(11b)E

The Pre-fragmentation for IPsec VPN feature is supported on all platforms using Cisco IOS Release 12.1(11b)E or higher, including:

- Cisco 7100 series

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

- No new or modified standards are supported by this feature.

MIBs

- No new or modified standards are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

- No new or modified RFCs are supported by this feature.

Configuration Tasks

See the following sections for configuration tasks for the Pre-fragmentation for IPsec VPNs feature. Each task in the list is identified as either required or optional.

- [Configuring Pre-Fragmentation For IPsec VPNs](#) (required)
- [Verifying Pre-Fragmentation For IPsec VPNs](#) (optional)

Configuring Pre-Fragmentation For IPsec VPNs

Pre-fragmentation for IPsec VPNs is globally enabled by default. To enable or disable pre-fragmentation for IPsec VPNs while in interface configuration mode, enter the commands in the following table. Use the **no** form of the commands to revert back to the default configuration, or use the commands themselves to enable configuration of the pre-fragmentation IPsec VPNs.



Note

Manually enabling or disabling this feature will override the global configuration.

Command	Purpose
Router(config-if)# crypto ipsec fragmentation before-encryption	Enables pre-fragmentation for IPsec VPNs on the interface.
Router(config-if)# crypto ipsec fragmentation after-encryption	Disables pre-fragmentation for IPsec VPNs on the interface.
Router(config)# crypto ipsec fragmentation before-encryption	Enables pre-fragmentation for IPsec VPNs globally.
Router(config)# crypto ipsec fragmentation after-encryption	Disables pre-fragmentation for IPsec VPNs globally.

Verifying Pre-Fragmentation For IPsec VPNs

To verify that this feature is enabled, consult the interface statistics on the encrypting router and the decrypting router. If fragmentation occurs on the encrypting router, and no reassembly occurs on the decrypting router, fragmentation is happening before encryption, and thus the packets are not being reassembled before decryption. This means that the feature is enabled.



Note

This method of verification does not apply to packets destined for the decrypting router.

- Step 1** Enter the **show running-configuration** command on the encrypting router. If the feature is enabled, you will observe output similar to the following:

```
Router# show running-configuration
crypto isakmp policy 10
  authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
!
!
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
!
crypto map bar 10 ipsec-isakmp
  set peer 25.0.0.7
  set transform-set fooprime
  match address 102
```

If the feature has been disabled, you will observe output similar to the following:

```
Router# show running-configuration
crypto isakmp policy 10
  authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
!
!
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
crypto ipsec fragmentation after-encryption
!
crypto map bar 10 ipsec-isakmp
  set peer 25.0.0.7
  set transform-set fooprime
  match address 102
```

- Step 2** Enter the **show running-configuration interface *type number*** command to display statistics for the encrypting router egress interface. If the feature is enabled, you will observe output similar to the following:

```
Router# show running-configuration interface fastethernet 0/0
interface FastEthernet0/0
  ip address 25.0.0.6 255.0.0.0
  no ip mroute-cache
  load-interval 30
  duplex full
  speed 100
  crypto map bar
```

If the feature has been disabled, you will observe output similar to the following:

```
Router# show running-configuration interface fastethernet 0/0

interface FastEthernet0/0
  ip address 25.0.0.6 255.0.0.0
  no ip mroute-cache
  load-interval 30
  duplex full
  speed 100
  crypto map bar
  crypto ipsec fragmentation after-encryption
```

Configuration Examples

This section provides the following configuration example:

- [Enabling Pre-Fragmentation For IPsec VPNs Example](#)

Enabling Pre-Fragmentation For IPsec VPNs Example

The following configuration example shows how to configure the Pre-Fragmentation for IPsec VPNs feature:



Note

This feature does not show up in the running configuration in this example because the default global pre-fragmentation for IPsec VPNs feature is enabled. Pre-fragmentation for IPsec VPNs shows in the running configuration only when you explicitly enable the feature on the interface.

```
crypto isakmp policy 10
  authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
!
!
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
!
crypto map bar 10 ipsec-isakmp
  set peer 25.0.0.7
  set transform-set fooprime
  match address 102
```

Command Reference

The following commands are introduced or modified in the feature or features

- **crypto ipsec fragmentation**
- **crypto ipsec fragmentation (interface configuration)**

For information about these commands, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



Invalid Security Parameter Index Recovery

When an invalid security parameter index error (shown as “Invalid SPI”) occurs in IP Security (IPSec) packet processing, the feature allows for an Internet Key Exchange (IKE) security association (SA) to be established. The “IKE” module sends notification of the “Invalid SPI” error to the originating IPSec peer so that Security Association Databases (SADB) can be resynchronized and successful packet processing can be resumed.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for” section on page 17](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for, page 2](#)
- [Restrictions for, page 2](#)
- [Information About, page 2](#)
- [How to Configure, page 3](#)
- [Configuration Examples for, page 10](#)
- [Additional References, page 16](#)
- [Command Reference, page 17](#)
- [Feature Information for, page 17](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for

Before configuring the feature, you must have enabled Internet Key Exchange (IKE) and IPsec on your router.

Restrictions for

If an IKE SA is being initiated to notify an IPsec peer of an “Invalid SPI” error, there is the risk that a denial-of-service (DoS) attack can occur. The feature has a built-in mechanism to minimize such a risk, but because there is a risk, the feature is not enabled by default. You must enable the command using command-line interface (CLI).

Information About

To use the feature, you should understand the following concept.

- [How the Feature Works, page 2](#)

How the Feature Works

An IPsec “black hole” occurs when one IPsec peer “dies” (for example, a peer can “die” if a reboot occurs or if an IPsec peer somehow gets reset). Because one of the peers (the receiving peer) is completely reset, it loses its IKE SA with the other peer. Generally, when an IPsec peer receives a packet for which it cannot find an SA, it tries to send an IKE “INVALID SPI NOTIFY” message to the data originator. This notification is sent using the IKE SA. If there is no IKE SA available, the receiving peer drops the packet.



Note

A single security association (SA) has only two peers. However, a SADB can have multiple SAs, whereby each SA has an association with a different peer.

When an invalid security parameter index (SPI) is encountered, the Invalid Security Parameter Index feature provides for the setting up of an IKE SA with the originator of the data, and the IKE “INVALID SPI NOTIFY” message is sent. The peer that originated the data “sees” the “INVALID SPI NOTIFY” message and deletes the IPsec SA that has the invalid SPI. If there is further traffic from the originating peer, there will not be any IPsec SAs, and new SAs will be set up. Traffic will flow again. The default behavior (that is, without configuring the feature) is that the data packet that caused the invalid SPI error is dropped. The originating peer keeps on sending the data using the IPsec SA that has the invalid SPI, and the receiving peer keeps dropping the traffic (thus creating the “black hole”).

The IPsec module uses the IKE module to send an IKE “INVALID SPI NOTIFY” message to the other peer. Once the invalid SPI recovery is in place, there should not be any significant dropping of packets although the IPsec SA setup can itself result in the dropping of a few packets.

To configure your router for the feature, use the **crypto isakmp invalid-spi-recovery** command. The IKE SA will not be initiated unless you have configured this command.

How to Configure

This section contains the following procedure.

- [Configuring, page 3](#)

Configuring

To configure the feature, perform the following steps.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto isakmp invalid-spi-recovery`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>crypto isakmp invalid-spi-recovery</code> Example: Router (config)# <code>crypto isakmp invalid-spi-recovery</code>	Initiates the IKE module process whereby the IKE module notifies the receiving peer that an “Invalid SPI” error has occurred.

Verifying an Configuration

To determine the status of the IPSec SA for traffic between two peers, you can use the **show crypto ipsec sa** command. If the IPSec SA is available on one peer and not on the other, there is a “black hole” situation, in which case you will see the invalid SPI errors being logged for the receiving peer. If you turn console logging on or check the syslog server, you will see that these errors are also being logged. [Figure 1](#) shows the topology of a typical preshared configuration setup. Host 1 is the initiating peer (initiator), and Host 2 is the receiving peer (responder).

Figure 1 Preshared Configuration Topology

SUMMARY STEPS

- To verify the preshared configuration, perform the following steps.
- 1. **Initiate the IKE and IPSec SAs between Host 1 and Host 2**
 - 2. **Clear the IKE and IPSec SAs on Router B**
 - 3. **Send traffic from Host 1 to Host 2 and ensure that IKE and IPSec SAs are correctly established**
 - 4. **Check for an invalid SPI message on Router B**

DETAILED STEPS

Step 1 Initiate the IKE and IPSec SAs between Host 1 and Host 2

Router A

```
Router# show crypto isakmp sa

f_vrf/i_vrf  dst          src          state        conn-id slot
/ 10.2.2.2    10.1.1.1     QM_IDLE      1           0
```

Router B

```
Router# show crypto isakmp sa

f_vrf/i_vrf  dst          src          state        conn-id slot
/            10.1.1.1     10.2.2.2     QM_IDLE      1           0
```

Router A

```
Router# show crypto ipsec sa interface fastethernet0/0

interface: FastEthernet0/0
  Crypto map tag: testtag1, local addr. 10.1.1.1

protected vrf:
  local  ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
```



```

current_peer: 10.2.2.2:500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.2
path mtu 1500, media mtu 1500
current outbound spi: 7AA69CB7

inbound esp sas:
  spi: 0x249C5062(614223970)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5123, flow_id: 1, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4537831/3595)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:
  spi: 0xB16D1587(2976716167)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5121, flow_id: 1, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4537831/3595)
    replay detection support: Y

inbound pcp sas:

outbound esp sas:
  spi: 0x7AA69CB7(2057739447)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5124, flow_id: 2, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4537835/3595)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:
  spi: 0x1214F0D(18960141)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5122, flow_id: 2, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4537835/3594)
    replay detection support: Y

outbound pcp sas:

```

Router B

```
Router# show crypto ipsec sa interface ethernet1/0
```

```

interface: Ethernet1/0
  Crypto map tag: testtag1, local addr. 10.2.2.2

protected vrf:
  local ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)

```

```

remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
current_peer: 10.1.1.1:500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
  #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
path mtu 1500, media mtu 1500
current outbound spi: 249C5062

inbound esp sas:
  spi: 0x7AA69CB7(2057739447)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5123, flow_id: 1, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4421281/3593)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:
  spi: 0x1214F0D(18960141)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5121, flow_id: 1, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4421281/3593)
    replay detection support: Y

inbound pcg sas:

outbound esp sas:
  spi: 0x249C5062(614223970)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5124, flow_id: 2, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4421285/3593)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:
  spi: 0xB16D1587(2976716167)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5122, flow_id: 2, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4421285/3592)
    replay detection support: Y

outbound pcg sas:

```

Step 2 Clear the IKE and IPSec SAs on Router B

```
Router# clear crypto isakmp
```

```
Router# clear crypto sa
```

```

Router# show crypto isakmp sa

      f_vrf/i_vrf    dst          src          state          conn-id slot
      /              10.2.2.2      10.1.1.1      MM_NO_STATE      1          0 (deleted)

Router# show crypto ipsec sa

interface: Ethernet1/0
  Crypto map tag: testtag1, local addr. 10.2.2.2

protected vrf:
local ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
current_peer: 10.1.1.1:500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
  path mtu 1500, media mtu 1500
  current outbound spi: 0

inbound esp sas:

inbound ah sas:

inbound pcg sas:

outbound esp sas:

outbound ah sas:

outbound pcg sas:

```

Step 3 Send traffic from Host 1 to Host 2 and ensure that new IKE and IPSec SAs are correctly established

```

ping
Protocol [ip]: ip
Target IP address: 10.0.2.2
Repeat count [5]: 30
Datagram size [100]: 100
Timeout in seconds [2]:
Extended commands [n]: no
Sweep range of sizes [n]: n
Type escape sequence to abort.
Sending 30, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds:
..!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 93 percent (28/30), round-trip min/avg/max = 1/3/8 ms

```

```

RouterB# show crypto isakmp sa

      f_vrf/i_vrf    dst          src          state          conn-id slot
      /              10.1.1.1      10.2.2.2      QM_IDLE          3          0
      /              10.1.1.1      10.2.2.2      MM_NO_STATE      1          0 (deleted)

RouterB# show crypto ipsec sa

interface: Ethernet1/0
  Crypto map tag: testtag1, local addr. 10.2.2.2

```

```

protected vrf:
local  ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
current_peer: 10.1.1.1:500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
#pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
path mtu 1500, media mtu 1500
current outbound spi: D763771F

inbound esp sas:
  spi: 0xE7AB4256(3886760534)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5127, flow_id: 3, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4502463/3596)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:
  spi: 0xF9205CED(4179647725)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5125, flow_id: 3, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4502463/3596)
    replay detection support: Y

inbound pcg sas:

outbound esp sas:
  spi: 0xD763771F(3613619999)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5128, flow_id: 4, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4502468/3596)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:
  spi: 0xEB95406F(3952427119)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5126, flow_id: 4, crypto map: testtag1
    crypto engine type: Hardware
    sa timing: remaining key lifetime (k/sec): (4502468/3595)
    replay detection support: Y

outbound pcg sas:

```

RouterA# **show crypto isakmp sa**

f_vrf/i_vrf	dst	src	state	conn-id	slot	
/	10.2.2.2	10.1.1.1	MM_NO_STATE	1	0	(deleted)

```

/          10.2.2.2          10.1.1.1          QM_IDLE          2          0

```

Check for an invalid SPI message on Router B

Router# **show logging**

```

Syslog logging: enabled (10 messages dropped, 13 messages rate-limited, 0 flushes, 0
overruns, xml disabled)
  Console logging: disabled
  Monitor logging: level debugging, 0 messages logged, xml disabled
  Buffer logging: level debugging, 43 messages logged, xml disabled
  Logging Exception size (8192 bytes)
  Count and timestamp logging messages: disabled
  Trap logging: level informational, 72 message lines logged

Log Buffer (8000 bytes):

*Mar 24 20:55:45.739: %CRYPTO-4-RECDV_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid
spi for
    destaddr=10.2.2.2, prot=51, spi=0x1214F0D(18960141), srcaddr=10.1.1.1
*Mar 24 20:55:47.743: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
  local_proxy= 10.0.2.2/255.255.255.255/0/0 (type=1),
  remote_proxy= 10.0.0.1/255.255.255.255/0/0 (type=1),
  protocol= AH, transform= ah-sha-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar 24 20:55:47.743: IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
  local_proxy= 10.0.2.2/255.255.255.255/0/0 (type=1),
  remote_proxy= 10.0.0.1/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform= esp-des esp-sha-hmac ,
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar 24 20:55:47.743: IPSEC(kei_proxy): head = testtag1, map->ivrf = , kei->ivrf =
*Mar 24 20:55:47.743: IPSEC(key_engine): got a queue event with 2 kei messages
*Mar 24 20:55:47.743: IPSEC(spi_response): getting spi 4179647725 for SA
    from 10.2.2.2          to 10.1.1.1          for prot 2
*Mar 24 20:55:47.747: IPSEC(spi_response): getting spi 3886760534 for SA
    from 10.2.2.2          to 10.1.1.1          for prot 3
*Mar 24 20:55:48.071: IPsec: Flow_switching Allocated flow for flow_id 939524099
*Mar 24 20:55:48.071: IPsec: Flow_switching Allocated flow for flow_id 939524100
*Mar 24 20:55:48.135: IPSEC(key_engine): got a queue event with 4 kei messages
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
  local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
  remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
  protocol= AH, transform= ah-sha-hmac ,
  lifedur= 3600s and 4608000kb,
  spi= 0xF9205CED(4179647725), conn_id= 939529221, keysize= 0, flags= 0x2
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.2.2.2, remote= 10.1.1.1,
  local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
  remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
  protocol= AH, transform= ah-sha-hmac ,
  lifedur= 3600s and 4608000kb,
  spi= 0xEB95406F(3952427119), conn_id= 939529222, keysize= 0, flags= 0xA
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
  local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
  remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
  protocol= ESP, transform= esp-des esp-sha-hmac ,
  lifedur= 3600s and 4608000kb,

```

```

    spi= 0xE7AB4256(3886760534), conn_id= 939529223, keysize= 0, flags= 0x2
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
    (key eng. msg.) OUTBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-sha-hmac ,

    lifedur= 3600s and 4608000kb,
    spi= 0xD763771F(3613619999), conn_id= 939529224, keysize= 0, flags= 0xA
*Mar 24 20:55:48.139: IPSEC(kei_proxy): head = testtag1, map->ivrf = , kei->ivrf =
*Mar 24 20:55:48.139: IPSEC(mtree_add_ident): src 10.2.2.2, dest 10.1.1.1, dest_port 0

*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
    (sa) sa_dest= 10.1.1.1, sa_prot= 51,
    sa_spi= 0xF9205CED(4179647725),
    sa_trans= ah-sha-hmac , sa_conn_id= 939529221
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
    (sa) sa_dest= 10.2.2.2, sa_prot= 51,
    sa_spi= 0xEB95406F(3952427119),
    sa_trans= ah-sha-hmac , sa_conn_id= 939529222
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
    (sa) sa_dest= 10.1.1.1, sa_prot= 50,
    sa_spi= 0xE7AB4256(3886760534),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 939529223
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
    (sa) sa_dest= 10.2.2.2, sa_prot= 50,
    sa_spi= 0xD763771F(3613619999),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 939529224
ipseca-72a#

```

Configuration Examples for

This section provides the following configuration example.

- [: Example, page 10](#)

: Example

The following example shows that invalid security parameter index recovery has been configured on Router A and Router B. [Figure 1](#) shows the topology used for this example.

Router A

```
Router# show running-config
```

```
Building configuration...
```

```

Current configuration : 2048 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service tcp-small-servers
!
hostname ipseca-71a
!
logging queue-limit 100

```

```
no logging console
enable secret 5 $1$4GZB$L2Y0mnenOCNAu0jgFxebT/
enable password lab
!
clock timezone PST -8

clock summer-time PDT recurring
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
mpls ldp logging neighbor-changes
no ftp-server write-enable
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 180
crypto isakmp key 0 1234 address 10.2.2.2
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag1 10 ipsec-isakmp
 set peer 10.2.2.2
 set transform-set auth2
 match address 150
!
!
controller ISA 5/1
!
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.0.0.0
 no ip route-cache cef
 duplex full
 speed 100
 crypto map testtag1
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.0.0.0
 no ip route-cache cef
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!
interface Serial1/1
 no ip address
```

```

no ip route-cache
no ip mroute-cache
shutdown
serial restart_delay 0
clockrate 128000
!

interface Serial1/2
no ip address
no ip route-cache
no ip mroute-cache
shutdown
serial restart_delay 0
!
interface Serial1/3
no ip address
no ip route-cache
no ip mroute-cache
shutdown
no keepalive
serial restart_delay 0
clockrate 128000
!
ip classless
ip route 10.3.3.3 255.0.0.0 10.2.0.1
no ip http server
no ip http secure-server
!
!
access-list 150 permit ip host 10.0.0.1 host 10.0.2.2
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
call rsvp-sync
!
!
mgcp profile default
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password lab
login
!
!
end

ipseca-71a#

```

Router B

Router# **show running-config**

Building configuration...

Current configuration : 2849 bytes

```

!
version 12.3
no service pad
service timestamps debug datetime msec localtime

```



```
service timestamps log datetime msec localtime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname ipseca-72a
!

logging queue-limit 100
no logging console
enable secret 5 $1$kKqL$5Th5Qhw1ubDkkK90KWFxi1
enable password lab
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
mpls ldp logging neighbor-changes
no ftp-server write-enable
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
crypto isakmp policy 1
  authentication pre-share
  lifetime 180
crypto isakmp key 0 1234 address 10.1.1.1
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag1 10 ipsec-isakmp
  set peer 10.1.1.1
  set transform-set auth2
  match address 150
!
!
controller ISA 5/1
!
!
interface FastEthernet0/0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  duplex half
!
interface Ethernet1/0
  ip address 10.2.2.2 255.0.0.0
  no ip route-cache cef
  duplex half
  crypto map testtag1
```

```
!  
interface Ethernet1/1  
  ip address 10.0.2.2 255.0.0.0  
  no ip route-cache cef  
  duplex half  
!  
interface Ethernet1/2  
  no ip address  
  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  duplex half  
!  
interface Ethernet1/3  
  no ip address  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  duplex half  
!  
interface Ethernet1/4  
  no ip address  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  duplex half  
!  
interface Ethernet1/5  
  no ip address  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  duplex half  
!  
interface Ethernet1/6  
  no ip address  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  duplex half  
!  
interface Ethernet1/7  
  no ip address  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  duplex half  
!  
interface Serial3/0  
  no ip address  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  serial restart_delay 0  
!  
interface Serial3/1  
  no ip address  
  no ip route-cache  
  no ip mroute-cache  
  shutdown  
  serial restart_delay 0  
  clockrate 128000  
!
```

```
interface Serial3/2
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  serial restart_delay 0
!
interface Serial3/3
  no ip address

  no ip route-cache
  no ip mroute-cache
  shutdown
  no keepalive
  serial restart_delay 0
  clockrate 128000
!
ip classless
ip route 10.0.0.0 255.0.0.0 10.2.0.1
no ip http server
no ip http secure-server
!
!
access-list 150 permit ip host 10.0.2.2 host 10.0.0.1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
  shutdown
!
!
line con 0
  exec-timeout 0 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  password lab
  login
!
!
end
```

Additional References

The following sections provide references related to .

Related Documents

Related Topic	Document Title
Configuring IKE	Configuring Internet Key Exchange for IPsec VPNs
Interface commands	Cisco IOS Master Command List , Release 12.4T

Standards

Standards	Title
This feature has no new or modified standards.	—

MIBs

MIBs	MIBs Link
This feature has no new or modified MIBs.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
This feature has no new or modified RFCs.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features

- **crypto isakmp invalid-spi-recovery**

For information about these commands, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Feature Information for

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for

Feature Name	Releases	Feature Information
	12.3(2)T	This feature was introduced.
	12.2(18)SXE	This feature was integrated into Cisco IOS Release 12.2(18)SXE.
Invalid Special Parameter Index (SPI) Recovery	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



IPsec Dead Peer Detection Periodic Message Option

First Published: May 1, 2004

Last Updated: August 21, 2007

The IPsec Dead Peer Detection Periodic Message Option feature allows you to configure your router to query the liveliness of its Internet Key Exchange (IKE) peer at regular intervals. The benefit of this approach over the default approach (on-demand dead peer detection) is earlier detection of dead peers.

History for IPsec Dead Peer Detection Periodic Message Option Feature

Release	Modification
12.3(7)T	This feature was introduced.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for IPsec Dead Peer Detection Periodic Message Option, page 2](#)
- [Restrictions for IPsec Dead Peer Detection Periodic Message Option, page 2](#)
- [Information About IPsec Dead Peer Detection Periodic Message Option, page 2](#)
- [How to Configure IPsec Dead Peer Detection Periodic Message Option, page 3](#)
- [Configuration Examples for IPsec Dead Peer Detection Periodic Message Option, page 7](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 11](#)
- [Command Reference, page 13](#)

Prerequisites for IPsec Dead Peer Detection Periodic Message Option

Before configuring the IPsec Dead Peer Detection Periodic Message Option feature, you should have the following:

- Familiarity with configuring IP Security (IPsec).
- An IKE peer that supports DPD (dead peer detection). Implementations that support DPD include the Cisco VPN 3000 concentrator, Cisco PIX Firewall, Cisco VPN Client, and Cisco IOS software in all modes of operation—site-to-site, Easy VPN remote, and Easy VPN server.

Restrictions for IPsec Dead Peer Detection Periodic Message Option

Using periodic DPD potentially allows the router to detect an unresponsive IKE peer with better response time when compared to on-demand DPD. However, use of periodic DPD incurs extra overhead. When communicating to large numbers of IKE peers, you should consider using on-demand DPD instead.

Information About IPsec Dead Peer Detection Periodic Message Option

To configure IPsec Dead Peer Detection Periodic Message Option, you should understand the following concepts:

- [How DPD and Cisco IOS Keepalive Features Work, page 2](#)
- [Using the IPsec Dead Peer Detection Periodic Message Option, page 3](#)
- [Using DPD and Cisco IOS Keepalive Features with Multiple Peers in the Crypto Map, page 3](#)
- [Using DPD in an Easy VPN Remote Configuration, page 3](#)

How DPD and Cisco IOS Keepalive Features Work

DPD and Cisco IOS keepalives function on the basis of the timer. If the timer is set for 10 seconds, the router will send a “hello” message every 10 seconds (unless, of course, the router receives a “hello” message from the peer). The benefit of IOS keepalives and periodic DPD is earlier detection of dead peers. However, IOS keepalives and periodic DPD rely on periodic messages that have to be sent with considerable frequency. The result of sending frequent messages is that the communicating peers must encrypt and decrypt more packets.

DPD also has an on-demand approach. The contrasting on-demand approach is the default. With on-demand DPD, messages are sent on the basis of traffic patterns. For example, if a router has to send outbound traffic and the liveliness of the peer is questionable, the router sends a DPD message to query the status of the peer. If a router has no traffic to send, it never sends a DPD message. If a peer is dead, and the router never has any traffic to send to the peer, the router will not find out until the IKE or IPsec security association (SA) has to be rekeyed (the liveliness of the peer is unimportant if the router is not trying to communicate with the peer). On the other hand, if the router has traffic to send to the peer, and the peer does not respond, the router will initiate a DPD message to determine the state of the peer.

Using the IPsec Dead Peer Detection Periodic Message Option

With the IPsec Dead Peer Detection Periodic Message Option feature, you can configure your router so that DPD messages are “forced” at regular intervals. This forced approach results in earlier detection of dead peers. For example, if a router has no traffic to send, a DPD message is still sent at regular intervals, and if a peer is dead, the router does not have to wait until the IKE SA times out to find out.

If you want to configure the DPD periodic message option, you should use the **crypto isakmp keepalive** command with the **periodic** keyword. If you do not configure the **periodic** keyword, the router defaults to the on-demand approach.



Note

When the **crypto isakmp keepalive** command is configured, the Cisco IOS software negotiates the use of Cisco IOS keepalives or DPD, depending on which protocol the peer supports.

Using DPD and Cisco IOS Keepalive Features with Multiple Peers in the Crypto Map

DPD and IOS keepalive features can be used in conjunction with multiple peers in the crypto map to allow for stateless failover. DPD allows the router to detect a dead IKE peer, and when the router detects the dead state, the router deletes the IPsec and IKE SAs to the peer. If you configure multiple peers, the router will switch over to the next listed peer for a stateless failover.

Using DPD in an Easy VPN Remote Configuration

DPD can be used in an Easy VPN remote configuration. See the section [“Configuring DPD for an Easy VPN Remote” section on page 5](#).

How to Configure IPsec Dead Peer Detection Periodic Message Option

This section contains the following procedures:

- [Configuring a Periodic DPD Message, page 4](#)
- [Configuring DPD and Cisco IOS Keepalives with Multiple Peers in the Crypto Map, page 4](#)
- [Configuring DPD for an Easy VPN Remote, page 5](#)
- [Verifying That DPD Is Enabled, page 6](#)

Configuring a Periodic DPD Message

To configure a periodic DPD message, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp keepalive *seconds* [*retries*] [**periodic** | **on-demand**]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp keepalive <i>seconds</i> [<i>retries</i>] [periodic on-demand] Example: Router (config)# crypto isakmp keepalive 10 periodic	Allows the gateway to send DPD messages to the peer. <ul style="list-style-type: none"> • <i>seconds</i>—Number of seconds between DPD messages. • <i>retries</i>—(Optional) Number of seconds between DPD retries if the DPD message fails. • periodic—(Optional) DPD messages are sent at regular intervals. • on-demand—(Optional) DPD retries are sent on demand. This is the default behavior.

Configuring DPD and Cisco IOS Keepalives with Multiple Peers in the Crypto Map

To configure DPD and IOS keepalives to be used in conjunction with the crypto map to allow for stateless failover, perform the following steps. This configuration will cause a router to cycle through the peer list when it detects that the first peer is dead.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map *map-name seq-num ipsec-isakmp***
4. **set peer {*host-name* [**dynamic**] | *ip-address*}**

5. **set transform-set** *transform-set-name*
6. **match address** [*access-list-id* | *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name</i> <i>seq-num</i> ipsec-isakmp Example: Router (config)# crypto map green 1 ipsec-isakmp	Enters crypto map configuration mode and creates or modifies a crypto map entry. <ul style="list-style-type: none"> The ipsec-isakmp keyword indicates that IKE will be used to establish the IPsec SAs for protecting the traffic specified by this crypto map entry.
Step 4	set peer { <i>host-name</i> [dynamic] <i>ip-address</i> } Example: Router (config-crypto-map)# set peer 10.12.12.12	Specifies an IPsec peer in a crypto map entry. <ul style="list-style-type: none"> You can specify multiple peers by repeating this command.
Step 5	set transform-set <i>transform-set-name</i> Example: Router (config-crypto-map)# set transform-set txfm	Specifies which transform sets can be used with the crypto map entry. <ul style="list-style-type: none"> You can specify more than one transform set name by repeating this command.
Step 6	match address [<i>access-list-id</i> <i>name</i>] Example: Router (config-crypto-map)# match address 101	Specifies an extended access list for a crypto map entry.

Configuring DPD for an Easy VPN Remote

To configure DPD in an Easy VPN remote configuration, perform the following steps. This configuration also will cause a router to cycle through the peer list when it detects that the first peer is dead.



Note

IOS keepalives are not supported for Easy VPN remote configurations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto ipsec client ezvpn** *name*
4. **connect** {**auto** | **manual**}
5. **group** *group-name* **key** *group-key*
6. **mode** {**client** | **network-extension**}
7. **peer** {*ipaddress* | *hostname*}

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec client ezvpn <i>name</i> Example: Router (config)# crypto ipsec client ezvpn ezvpn-config1	Creates a Cisco Easy VPN remote configuration and enters the Cisco Easy VPN Remote configuration mode.
Step 4	connect { auto manual }	Manually establishes and terminates an IPsec VPN tunnel on demand. <ul style="list-style-type: none">The auto keyword option is the default setting.
Step 5	group <i>group-name</i> key <i>group-key</i> Example: Router (config-crypto-ezvpn)# group unity key preshared	Specifies the group name and key value for the Virtual Private Network (VPN) connection.
Step 6	mode { client network-extension }	Specifies the VPN mode of operation of the router. Example: Router (config-crypto-ezvpn)# mode client
Step 7	peer { <i>ipaddress</i> <i>hostname</i> }	Sets the peer IP address or host name for the VPN connection. <ul style="list-style-type: none">A hostname can be specified only when the router has a DNS server available for host-name resolution.This command can be repeated multiple times.

Verifying That DPD Is Enabled

DPD allows the router to clear the IKE state when a peer becomes unreachable. If DPD is enabled and the peer is unreachable for some time, you can use the **clear crypto session** command to manually clear IKE and IPsec SAs.

The **debug crypto isakmp** command can be used to verify that DPD is enabled.

SUMMARY STEPS

1. **enable**
2. **clear crypto session** [*local ip-address* [*port local-port*]] [*remote ip-address* [*port remote-port*]] | [*fvrif vrf-name*] [*ivrf vrf-name*]
3. **debug crypto isakmp**

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	clear crypto session [<i>local ip-address</i> [<i>port local-port</i>]] [<i>remote ip-address</i> [<i>port remote-port</i>]] [<i>fvrif vrf-name</i>] [<i>ivrf vrf-name</i>] Example: Router# clear crypto session	Deletes crypto sessions (IPsec and IKE SAs).
Step 3	debug crypto isakmp Example: Router# debug crypto isakmp	Displays messages about IKE events.

Configuration Examples for IPsec Dead Peer Detection Periodic Message Option

This section provides the following configuration examples:

- [Site-to-Site Setup with Periodic DPD Enabled: Example, page 7](#)
- [Easy VPN Remote with DPD Enabled: Example, page 8](#)
- [Verifying DPD Configuration Using the debug crypto isakmp Command: Example, page 8](#)
- [DPD and Cisco IOS Keepalives Used in Conjunction with Multiple Peers in a Crypto Map: Example, page 11](#)
- [DPD Used in Conjunction with Multiple Peers for an Easy VPN Remote: Example, page 11](#)

Site-to-Site Setup with Periodic DPD Enabled: Example

The following configurations are for a site-to-site setup with no periodic DPD enabled. The configurations are for the IKE Phase 1 policy and for the IKE preshared key.

IKE Phase 1 Policy

```
crypto isakmp policy 1
  encryption 3des
```

```

authentication pre-share
group 2
!

```

IKE Preshared Key

```

crypto isakmp key kd94j1ksldz address 10.2.80.209 255.255.255.0
crypto isakmp keepalive 10 periodic
crypto ipsec transform-set esp-3des-sha esp-3des esp-sha-hmac
crypto map test 1 ipsec-isakmp
    set peer 10.2.80.209
    set transform-set esp-3des-sha
    match address 101
!
!
interface FastEthernet0
    ip address 10.1.32.14 255.255.255.0
    speed auto
    crypto map test
!

```

Easy VPN Remote with DPD Enabled: Example

The following configuration tells the router to send a periodic DPD message every 30 seconds. If the peer fails to respond to the DPD R_U_THERE message, the router will resend the message every 20 seconds (four transmissions altogether).

```

crypto isakmp keepalive 30 20 periodic
crypto ipsec client ezvpn ezvpn-config
    connect auto
    group unity key preshared
    mode client
    peer 10.2.80.209
!
!
interface Ethernet0
    ip address 10.2.3.4 255.255.255.0
    half-duplex
    crypto ipsec client ezvpn ezvpn-config inside
!
interface FastEthernet0
    ip address 10.1.32.14 255.255.255.0
    speed auto
    crypto ipsec client ezvpn ezvpn-config outside

```

Verifying DPD Configuration Using the debug crypto isakmp Command: Example

The following sample output from the **debug crypto isakmp** command verifies that IKE DPD is enabled:

```
*Mar 25 15:17:14.131: ISAKMP:(0:1:HW:2):IKE_DPD is enabled, initializing timers
```

To see that IKE DPD is enabled (and that the peer supports DPD): when periodic DPD is enabled, you should see the following debug messages at the interval specified by the command:

```
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2):purging node 899852982 *Mar 25 15:18:52.111:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:18:52.111: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

The above message corresponds to sending the DPD R_U_THERE message.

```
*Mar 25 15:18:52.123: ISAKMP (0:268435457): received packet from 10.2.80.209
dport 500 sport 500 Global (I) QM_IDLE
*Mar 25 15:18:52.123: ISAKMP: set new node -443923643 to QM_IDLE *Mar 25 15:18:52.131:
ISAKMP:(0:1:HW:2): processing HASH payload. message ID =
-443923643
*Mar 25 15:18:52.131: ISAKMP:(0:1:HW:2): processing NOTIFY R_U_THERE_ACK protocol 1
spi 0, message ID = -443923643, sa = 81BA4DD4
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2): DPD/R_U_THERE_ACK received from peer
10.2.80.209, sequence 0x9
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):deleting node -443923643 error FALSE
reason "informational (in) state 1"
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_PEER, IKE_INFO_NOTIFY *Mar
25 15:18:52.135: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

The above message corresponds to receiving the acknowledge (ACK) message from the peer.

```
Router#
*Mar 25 15:47:35.335: ISAKMP: set new node -90798077 to QM_IDLE *Mar 25 15:47:35.343:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:35.343: ISAKMP:(0:1:HW:2):purging node -90798077 *Mar 25 15:47:35.347:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:47:35.347: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:36.611: ISAKMP:(0:1:HW:2):purging node 1515050537 *Mar 25 15:47:37.343:
ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:37.343: ISAKMP: set new node -1592471565 to QM_IDLE *Mar 25 15:47:37.351:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:37.351: ISAKMP:(0:1:HW:2):purging node -1592471565 *Mar 25 15:47:37.355:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:37.355: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:39.355: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:39.355: ISAKMP: set new node 1758739401 to QM_IDLE *Mar 25 15:47:39.363:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:39.363: ISAKMP:(0:1:HW:2):purging node 1758739401 *Mar 25 15:47:39.367:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:39.367: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:41.367: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
```

Configuration Examples for IPsec Dead Peer Detection Periodic Message Option

```

PEERS_ALIVE_TIMER
*Mar 25 15:47:41.367: ISAKMP: set new node 320258858 to QM_IDLE *Mar 25 15:47:41.375:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:41.379: ISAKMP:(0:1:HW:2):purging node 320258858 *Mar 25 15:47:41.379:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:41.379: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:43.379: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:43.379: ISAKMP: set new node -744493014 to QM_IDLE *Mar 25 15:47:43.387:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:43.387: ISAKMP:(0:1:HW:2):purging node -744493014 *Mar 25 15:47:43.391:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:43.391: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):peer 10.2.80.209 not responding! *Mar 25
15:47:45.391: ISAKMP:(0:1:HW:2):peer does not do paranoid keepalives.

*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.395: ISAKMP: Unlocking IPSEC struct 0x81E5C4E8 from
delete_siblings, count 0
*Mar 25 15:47:45.395: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN. Peer
10.2.80.209:500 Id: 10.2.80.209
*Mar 25 15:47:45.399: ISAKMP: set new node -2061951065 to QM_IDLE *Mar 25 15:47:45.411:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:45.411: ISAKMP:(0:1:HW:2):purging node -2061951065 *Mar 25 15:47:45.411:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:45.411: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_DEST_SA

*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.415: ISAKMP: Unlocking IKE struct 0x81E5C4E8 for
isadb_mark_sa_deleted(), count 0
*Mar 25 15:47:45.415: ISAKMP: Deleting peer node by peer_reap for 10.2.80.209:
81E5C4E8
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting node -1067612752 error TRUE
reason "peers alive"
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting node -114443536 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):deleting node 2116015069 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):deleting node -1981865558 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):Input = IKE_MSG_INTERNAL, IKE_PHASE1_DEL *Mar 25
15:47:45.419: ISAKMP:(0:1:HW:2):Old State = IKE_DEST_SA New State =
IKE_DEST_SA

*Mar 25 15:47:45.419: ISAKMP: received ke message (4/1)
*Mar 25 15:47:45.419: ISAKMP: received ke message (3/1)
*Mar 25 15:47:45.423: ISAKMP: ignoring request to send delete notify (no ISAKMP
sa) src 10.1.32.14 dst 10.2.80.209 for SPI 0x3A7B69BF
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting SA reason "" state (I)

```



```
MM_NO_STATE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -1067612752 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -114443536 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node 2116015069 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):deleting node -1981865558 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH *Mar 25
15:47:45.427: ISAKMP:(0:1:HW:2):Old State = IKE_DEST_SA New State =
IKE_DEST_SA
```

The above message shows what happens when the remote peer is unreachable. The router sends one DPD R_U_THERE message and four retransmissions before it finally deletes the IPsec and IKE SAs.

DPD and Cisco IOS Keepalives Used in Conjunction with Multiple Peers in a Crypto Map: Example

The following example shows that DPD and Cisco IOS keepalives are used in conjunction with multiple peers in a crypto map configuration when IKE will be used to establish the security associations (SAs). In this example, an SA could be set up to the IPsec peer at 10.0.0.1, 10.0.0.2, or 10.0.0.3.

```
crypto map green 1 ipsec-isakmp
 set peer 10.0.0.1
 set peer 10.0.0.2
 set peer 10.0.0.3
 set transform-set txfm
 match address 101
```

DPD Used in Conjunction with Multiple Peers for an Easy VPN Remote: Example

The following example shows that DPD is used in conjunction with multiple peers in an Easy VPN remote configuration. In this example, an SA could be set up to the IPsec peer at 10.10.10.10, 10.2.2.2, or 10.3.3.3.

```
crypto ipsec client ezvpn ezvpn-config
 connect auto
 group unity key preshared
 mode client
 peer 10.10.10.10
 peer 10.2.2.2
 peer 10.3.3.3
```

Additional References

The following sections provide references related to IPsec Dead Peer Detection Periodic Message Option.

Related Documents

Related Topic	Document Title
Configuring IPsec	Configuring Security for VPNs with IPsec
IPsec commands	Cisco IOS Security Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
DPD conforms to the Internet draft “draft-ietf-ipsec-dpd-04.txt,” which is pending publication as an Informational RFC (a number has not yet been assigned).	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features

- **crypto isakmp keepalive**

For information about these commands, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



IPsec Security Association Idle Timers

When a router running the Cisco IOS software creates an IPsec security association (SA) for a peer, resources must be allocated to maintain the SA. The SA requires both memory and several managed timers. For idle peers, these resources are wasted. If enough resources are wasted by idle peers, the router could be prevented from creating new SAs with other peers. The IPsec Security Association Idle Timers feature introduces a configurable idle timer to monitor SAs for activity, allowing SAs for idle peers to be deleted. Benefits of this feature include:

- Increased availability of resources
- Improved scalability of Cisco IOS IPsec deployments

Feature Specifications for IPsec Security Association Idle Timers

Feature History

Release	Modification
12.2(15)T	This feature was introduced.
12.3(14)T	The set security-association idle-time command was added, allowing for the configuration of an IPsec idle timer for a specified crypto map.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Supported Platforms

Cisco 1700 series access routers, Cisco 2400 series integrated access devices, Cisco 2600 series multiservice platforms, Cisco 3600 series multiservice platforms, Cisco 3700 series multiservice access routers, Cisco 7100 series VPN routers, Cisco 7200 series routers, Cisco 7400 series routers, Cisco 7500 series routers, Cisco 801–804 ISDN routers, Cisco 805 serial router, Cisco 806 broadband router, Cisco 811, Cisco 813, Cisco 820, Cisco 827 ADSL router, Cisco 828 G.SHDSL router, Cisco 8850-RPM, Cisco 950, Cisco AS5350 universal gateway, Cisco AS5400 series universal gateways, Cisco integrated communications system 7750, Cisco MC3810 series multiservice access concentrators, Cisco ubr7200, Cisco ubr900 series cable access routers

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for IPsec Security Association Idle Timers, page 2](#)
- [Information About IPsec Security Association Idle Timers, page 2](#)
- [Information About IPsec Security Association Idle Timers, page 2](#)
- [How to Configure IPsec Security Association Idle Timers, page 3](#)
- [Configuration Examples for IPsec Security Association Idle Timers, page 5](#)
- [Additional References, page 5](#)
- [Command Reference, page 7](#)

Prerequisites for IPsec Security Association Idle Timers

You must configure Internet Key Exchange (IKE) as described in the “[Configuring Internet Key Exchange Security Protocol](#)” chapter of the *Cisco IOS Security Configuration Guide*, Release 12.2.

Information About IPsec Security Association Idle Timers

To configure the IPsec Security Association Idle Timers feature, you must understand the following concepts:

- [Lifetimes for IPsec Security Associations, page 2](#)
- [IPsec Security Association Idle Timers, page 2](#)
- [Benefits of IPsec Security Association Idle Timers, page 3](#)

Lifetimes for IPsec Security Associations

The Cisco IOS software currently allows the configuration of lifetimes for IPsec SAs. Lifetimes can be configured globally or per crypto map. There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. A security association expires after the first of these lifetimes is reached.

IPsec Security Association Idle Timers

The IPsec SA idle timers are different from the global lifetimes for IPsec SAs. The expiration of the global lifetime is independent of peer activity. The IPsec SA idle timer allows SAs associated with inactive peers to be deleted before the global lifetime has expired.

If the IPsec SA idle timers are not configured, only the global lifetimes for IPsec SAs are applied. SAs are maintained until the global timers expire, regardless of peer activity.

**Note**

If the last IPsec SA to a given peer is deleted due to idle timer expiration, the Internet Key Exchange (IKE) SA to that peer will also be deleted.

Benefits of IPsec Security Association Idle Timers

Increased Availability of Resources

Configuring the IPsec Security Association Idle Timers feature increases the availability of resources by deleting SAs associated with idle peers.

Improved Scalability of Cisco IOS IPsec Deployments

Because the IPsec Security Association Idle Timers feature prevents the wasting of resources by idle peers, more resources will be available to create new SAs as required.

How to Configure IPsec Security Association Idle Timers

- [Configuring the IPsec SA Idle Timer Globally, page 3](#)
- [Configuring the IPsec SA Idle Timer per Crypto Map, page 4](#)

Configuring the IPsec SA Idle Timer Globally

This task configures the IPsec SA idle timer globally. The idle timer configuration will be applied to all SAs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association idle-time *seconds***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec security-association idle-time <i>seconds</i> Example: Router(config)# crypto ipsec security-association idle-time 600	Configures the IPsec SA idle timer. <ul style="list-style-type: none">• The <i>seconds</i> argument specifies the time, in seconds, that the idle timer will allow an inactive peer to maintain an SA. Valid values for the <i>seconds</i> argument range from 60 to 86400.

Configuring the IPsec SA Idle Timer per Crypto Map

This task configures the IPsec SA idle timer for a specified crypto map. The idle timer configuration will be applied to all SAs under the specified crypto map.



Note

This configuration task was available effective with Cisco IOS Release 12.3(14)T.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-number ipsec-isakmp*
4. **set security-association idle-time** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-number ipsec-isakmp</i> Example: Router(config)# crypto map test 1 ipsec-isakmp	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 4	set security-association idle-time <i>seconds</i> Example: Router(config-crypto-map)# set security-association idle-time 600	Specifies the maximum amount of time for which the current peer can be idle before the default peer is used. <ul style="list-style-type: none">• The <i>seconds</i> argument is the number of seconds for which the current peer can be idle before the default peer is used. Valid values are 60 to 86400.

Configuration Examples for IPsec Security Association Idle Timers

- [Configuring the IPsec SA Idle Timer Globally Example, page 5](#)
- [Configuring the IPsec SA Idle Timer per Crypto Map Example, page 5](#)

Configuring the IPsec SA Idle Timer Globally Example

The following example globally configures the IPsec SA idle timer to drop SAs for inactive peers after 600 seconds:

```
crypto ipsec security-association idle-time 600
```

Configuring the IPsec SA Idle Timer per Crypto Map Example

The following example configures the IPsec SA idle timer for the crypto map named test to drop SAs for inactive peers after 600 seconds:

```
crypto map test 1 ipsec-isakmp  
set security-association idle-time 600
```

**Note**

The above configuration was not available until Cisco IOS Release 12.3(14)T.

Additional References

For additional information related to IPsec Security Association Idle Timers, see the following sections:

- [Related Documents, page 6](#)
- [Standards, page 6](#)
- [MIBs, page 6](#)
- [RFCs, page 7](#)
- [Technical Assistance, page 7](#)

Related Documents

Related Topic	Document Title
Additional information about configuring IKE	Internet Key Exchange for IPsec VPNs
Additional information about configuring global lifetimes for IPsec SAs	<ul style="list-style-type: none"> • Configuring Security for VPNs with IPsec • IPsec Preferred Peer
Additional Security commands	Cisco IOS Security Command Reference

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	<p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features

- **crypto ipsec security-association idle-time**
- **set security-association idle-time**

For information about these commands, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



Low Latency Queueing (LLQ) for IPsec Encryption Engines

Feature History

Release	Modification
12.2(13)T	This feature was introduced.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

This feature module describes the Low Latency Queueing (LLQ) for IPsec encryption engines feature in Cisco IOS Release 12.2(13)T and 12.2(14)S. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Monitoring and Maintaining LLQ for IPsec Encryption Engines, page 8](#)
- [Configuration Examples, page 8](#)
- [Command Reference, page 9](#)
- [Glossary, page 9](#)

Feature Overview

Low Latency Queueing (LLQ) for IPsec encryption engines helps reduce packet latency by introducing the concept of queueing before crypto engines. Prior to this, the crypto processing engine gave data traffic and voice traffic equal status. Administrators now designate voice traffic as priority. Data packets arriving at a router interface are directed into a data packet inbound queue for crypto engine processing. This queue is called the best effort queue. Voice packets arriving on a router interface are directed into



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

a priority packet inbound queue for crypto engine processing. This queue is called the priority queue. The crypto engine undertakes packet processing in a favorable ratio for voice packets. Voice packets are guaranteed a minimum processing bandwidth on the crypto engine.

Benefits

The Low Latency Queueing (LLQ) for IPsec encryption engines feature guarantees a certain level of crypto engine processing time for priority designated traffic.



Note

On the Cisco 2600 platform, with the exception of the Cisco 2691 router, the CPU utilization maximizes out before the crypto engine becomes congested, so latency is not improved.

Better Voice Performance

Voice packets can be identified as priority, allowing the crypto engine to guarantee a certain percentage of processing bandwidth. This feature impacts the end user experience by assuring voice quality if voice traffic is directed onto a congested network.

Improved Latency and Jitters

Predictability is a critical component of network performance. The Low Latency Queueing (LLQ) for IPsec encryption engines feature delivers network traffic predictability relating to VPN. With this feature disabled, an end user employing an IP phone over VPN might experience jitter or latency, both symptoms of overall network latency and congestion. With this feature enabled, these undesirable characteristics are dissipated.

Restrictions

- No per-tunnel QoS policy. An interface QoS policy represents all tunnels.
- Assume the same IP precedence/DSCP marking for inbound and outbound voice packets.
- Assume the IP precedence/DSCP marking for voice packets are done at the source.
- Limited match criteria for voice traffic in the interface QoS policy.
- Assume call admission control is enforced within the enterprise.
- No strict error checking when aggregate policy's bandwidth exceeds crypto engine bandwidth. Only a warning is displayed but configuration is allowed.
- Assume voice packets are either all encrypted or unencrypted.

Related Features and Technologies

- CBWFQ
- Priority Queueing
- Weighted Fair Queueing

Related Documents

- [Quality of Service Solutions Command Reference](#)
- [Configuring Weighted Fair Queueing](#)

Supported Platforms

12.2(14)S and higher

The LLQ for IPsec encryption engines feature is supported on the following platform:

- Cisco 7200 series

12.2(13)T

The LLQ for IPsec encryption engines feature is supported on all platforms using Cisco IOS Release 12.2(13)T or later, including:

- Cisco 2600 series
- Cisco 3600 series
- Cisco 7100 series
- Cisco 7200 series

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side-by-side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

- No new or modified standards are supported by this feature.

MIBs

- No new or modified standards are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

- No new or modified RFCs are supported by this feature.

Prerequisites

To use this feature, you should be familiar with the following:

- Access control lists
- Bandwidth management
- CBWFQ

Configuration Tasks

To configure LLQ for IPsec encryption engines, perform the tasks described in the following section.


Note

See the [Quality of Service Solutions Command Reference](#), Cisco IOS Release 12.2, to learn more about configuring server policies on interfaces.

- [Defining Class Maps](#) (required)
- [Configuring Class Policy in the Policy Map](#) (required)
- [Configuring Class Policy for a Priority Queue](#) (required)
- [Configuring Class Policy Using a Specified Bandwidth](#) (optional)
- [Configuring the Class-Default Class Policy](#) (optional)
- [Attaching the Service Policy](#) (required)
- [Verifying Configuration of Policy Maps and Their Classes](#) (optional)

Defining Class Maps

To create a class map containing match criteria against which a packet is checked to determine if it belongs to a class, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# class-map class-map-name	Specifies the name of the class map to be created.
Step 2	Router(config-cmap)# match access-group {access-group / name access-group-name} or Router(config-cmap)# match input-interface interface-name or Router(config-cmap)# match protocol protocol	Specifies the name of the access control list (ACL) against whose contents packets are checked to determine if they belong to the class. Specifies the name of the input interface used as a match criterion against which packets are checked to determine if they belong to the class. Specifies the name of the protocol used as a match criterion against which packets are checked to determine if they belong to the class.

Configuring Class Policy in the Policy Map

To configure a policy map and create class policies that make up the service policy, begin with the **policy-map** command to specify the policy map name. Then use one or more of the following commands to configure the policy for a standard class or the default class:

- **priority**
- **bandwidth**
- **queue-limit** or **random-detect**
- **fair-queue** (for class-default class only)

For each class that you define, you can use one or more of the commands listed to configure the class policy. For example, you might specify bandwidth for one class and both bandwidth and queue limit for another class.

The default class of the policy map (commonly known as the class-default class) is the class to which traffic is directed if that traffic does not satisfy the match criteria of the other classes defined in the policy map.

You can configure class policies for as many classes as are defined on the router, up to the maximum of 64. However, the total amount of bandwidth allocated for all classes in a policy map must not exceed the minimum committed information rate (CIR) configured for the virtual circuit (VC) minus any bandwidth reserved by the **frame-relay voice bandwidth** and **frame-relay ip rtp priority** commands. If the minimum CIR is not configured, the bandwidth defaults to one half of the CIR. If all of the bandwidth is not allocated, the remaining bandwidth is allocated proportionally among the classes on the basis of their configured bandwidth.

To configure class policies in a policy map, perform the tasks described in the following sections. The task in the first section is required; the tasks in the remaining sections are optional.

Configuring Class Policy for a Priority Queue

To configure a policy map and give priority to a class within the policy map, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config) # policy-map policy-map	Specifies the name of the policy map to be created or modified.
Step 2	Router(config-cmap) # class class-name	Specifies the name of a class to be created and included in the service policy.
Step 3	Router(config-pmap-c) # priority bandwidth-kbps	Creates a strict priority class and specifies the amount of bandwidth, in kbps, to be assigned to the class.

Configuring Class Policy Using a Specified Bandwidth

To configure a policy map and create class policies that make up the service policy, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config) # policy-map policy-map	Specifies the name of the policy map to be created or modified.
Step 2	Router(config-cmap) # class class-name	Specifies the name of a class to be created and included in the service policy.
Step 3	Router(config-pmap-c) # bandwidth bandwidth-kbps	Specifies the amount of bandwidth to be assigned to the class, in kbps, or as a percentage of the available bandwidth. Bandwidth must be specified in kbps or as a percentage consistently across classes. (Bandwidth of the priority queue must be specified in kbps.)

To configure more than one class in the same policy map, repeat [Step 2](#) and [Step 3](#).

Configuring the Class-Default Class Policy

The class-default class is used to classify traffic that does not fall into one of the defined classes. Even though the class-default class is predefined when you create the policy map, you still have to configure it. If a default class is not configured, then traffic that does not match any of the configured classes is given best-effort treatment, which means that the network will deliver the traffic if it can, without any assurance of reliability, delay prevention, or throughput.

To configure a policy map and the class-default class, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# policy-map policy-map	Specifies the name of the policy map to be created or modified.
Step 2	Router(config-cmap)# class class-default default-class-name	Specifies the default class so that you can configure or modify its policy.
Step 3	Router(config-pmap-c)# bandwidth bandwidth-kbps or Router(config-pmap-c)# fair-queue [number-of-dynamic-queues]	Specifies the amount of bandwidth, in kbps, to be assigned to the class. Specifies the number of dynamic queues to be reserved for use by flow-based WFQ running on the default class. The number of dynamic queues is derived from the bandwidth of the interface.

Attaching the Service Policy

To attach a service policy to the output interface and enable LLQ for IPsec encryption engines, use the following command in map-class configuration mode:

	Command	Purpose
Step 1	Router(config)# interface type number	Specifies the interface using the LLQ for IPsec encryption engines.
Step 2	Router(config-if)# service-policy output policy-map	Attaches the specified service policy map to the output interface and enables LLQ for IPsec encryption engines.

Verifying Configuration of Policy Maps and Their Classes

To display the contents of a specific policy map or all policy maps configured on an interface, use the following commands in EXEC mode, as needed:

	Command	Purpose
Step 1	Router# show frame-relay pvc dlci	Displays statistics about the PVC and the configuration of classes for the policy map on the specified data-link connection identifier (DLCI).

	Command	Purpose
Step 2	Router# show policy-map interface <i>interface-name</i>	When LLQ is configured, displays the configuration of classes for all policy maps.
Step 3	Router# show policy-map interface <i>interface-name dlci dlci</i>	When LLQ is configured, displays the configuration of classes for the policy map on the specified DLCI.

Monitoring and Maintaining LLQ for IPsec Encryption Engines

To monitor and maintain LLQ for IPsec encryption engines, use the following command in EXEC mode:

	Command	Purpose
Step 1	Router# show crypto eng qos	Displays quality of service queueing statistics for LLQ for IPsec encryption engines.

For a more detailed list of commands that can be used to monitor LLQ for IPsec encryption engines, see the section [“Verifying Configuration of Policy Maps and Their Classes”](#)

Configuration Examples

This section provides the following configuration example:

- [LLQ for IPsec Encryption Engines Example](#)

LLQ for IPsec Encryption Engines Example

In the following example, a strict priority queue with a guaranteed allowed bandwidth of 50 kbps is reserved for traffic that is sent from the source address 10.10.10.10 to the destination address 10.10.10.20, in the range of ports 16384 through 20000 and 53000 through 56000.

First, the following commands configure access list 102 to match the desired voice traffic:

```
Router(config)# access-list 102 permit udp host 10.10.10.10 host 10.10.10.20 range 16384 20000
Router(config)# access-list 102 permit udp host 10.10.10.10 host 10.10.10.20 range 53000 56000
```

Next, the class map voice is defined, and the policy map called policy1 is created; a strict priority queue for the class voice is reserved, a bandwidth of 20 kbps is configured for the class bar, and the default class is configured for WFQ. The service-policy command then attaches the policy map to the fas0/0.

```
Router(config)# class-map voice
Router(config-cmap)# match access-group 102
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50
Router(config-pmap)# class bar
Router(config-pmap-c)# bandwidth 20
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue
Router(config)# interface fas0/0
```

```
Router(config-if)# service-policy output policy1
```

Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **show crypto eng qos**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Glossary

IKE—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPsec). Before any IPsec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service.

IPsec—IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



IPsec Management Plane



IP Security VPN Monitoring

The IP Security VPN Monitoring feature provides VPN session monitoring enhancements that will allow you to troubleshoot the Virtual Private Network (VPN) and monitor the end-user interface. Session monitoring enhancements include the following:

- Ability to specify an Internet Key Exchange (IKE) peer description in the configuration file
- Summary listing of crypto session status
- Syslog notification for crypto session up or down status
- Ability to clear both IKE and IP Security (IPSec) security associations (SAs) using one command-line interface (CLI)

Feature History for IP Security VPN Monitoring

Release	Modification
12.3(4)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for IP Security VPN Monitoring, page 2](#)
- [Restrictions for IP Security VPN Monitoring, page 2](#)
- [Information About IPSec VPN Monitoring, page 2](#)
- [How to Configure IP Security VPN Monitoring, page 4](#)
- [Configuration Examples for IP Security VPN Monitoring, page 6](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 7](#)
- [Command Reference, page 8](#)

Prerequisites for IP Security VPN Monitoring

- You should be familiar with IPSec and encryption.
- Your router must support IPSec, and before using the IP Security VPN Monitoring feature, you must have configured IPSec on your router.

Restrictions for IP Security VPN Monitoring

- You must be running Cisco IOS k8 or k9 crypto images on your router.

Information About IPSec VPN Monitoring

To troubleshoot the IPSec VPN and monitor the end-user interface, you should understand the following concepts:

- [Background: Crypto Sessions, page 2](#)
- [Per-IKE Peer Description, page 2](#)
- [Summary Listing of Crypto Session Status, page 3](#)
- [Syslog Notification for Crypto Session Up or Down Status, page 3](#)
- [IKE and IPSec Security Exchange Clear Command, page 3](#)

Background: Crypto Sessions

A crypto session is a set of IPSec connections (flows) between two crypto endpoints. If the two crypto endpoints use IKE as the keying protocol, they are IKE peers to each other. Typically, a crypto session consists of one IKE security association (for control traffic) and at least two IPSec security associations (for data traffic—one per each direction). There may be duplicated IKE security associations (SAs) and IPSec SAs or duplicated IKE SAs or IPSec SAs for the same session in the duration of rekeying or because of simultaneous setup requests from both sides.

Per-IKE Peer Description

The Per-IKE Peer Description function allows you to enter a description of your choosing for an IKE peer. (Before Cisco IOS Release 12.3(4)T, you could use only the IP address or fully qualified domain name [FQDN] to identify the peer; there was no way to configure a description string.) The unique peer description, which can include up to 80 characters, can be used whenever you are referencing that particular IKE peer. To add the peer description, use the **description** command.

**Note**

IKE peers that “sit” behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.

The primary application of this description field is for monitoring purposes (for example, when using **show** commands or for logging [syslog messages]). The description field is purely informational (for example, it cannot act as a substitute for the peer address or FQDN when defining crypto maps).

Summary Listing of Crypto Session Status

You can get a list of all the active VPN sessions by entering the **show crypto session** command. The listing will include the following:

- Interface
- IKE peer description, if available
- IKE SAs that are associated with the peer by whom the IPsec SAs are created
- IPsec SAs serving the flows of a session

Multiple IKE or IPsec SAs may be established for the same peer (for the same session), in which case IKE peer descriptions will be repeated with different values for the IKE SAs that are associated with the peer and for the IPsec SAs that are serving the flows of the session.

You can also use the **show crypto session detail** variant of this command to obtain more detailed information about the sessions.

Syslog Notification for Crypto Session Up or Down Status

The Syslog Notification for Crypto Session Up or Down Status function provides syslog notification every time the crypto session comes up or goes down.

The following is a sample syslog notification showing that a crypto session is up:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is UP. Peer 10.6.6.1:500 fvrf=name10 ivrf=name20  
Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

The following is a sample syslog notification showing that a crypto session is down:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is DOWN. Peer 10.6.6.1:500 fvrf=name10  
ivrf=name20 Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

IKE and IPsec Security Exchange Clear Command

In previous IOS versions, there was no single command to clear both IKE and IPsec connections (that is, SAs). Instead, you had to use the **clear crypto isakmp** command to clear IKE and the **clear crypto ipsec** command to clear IPsec. The new **clear crypto session** command allows you to clear both IKE and IPsec with a single command. To clear a specific crypto session or a subset of all the sessions (for example, a single tunnel to one remote site), you need to provide session-specific parameters, such as a local or remote IP address, a local or remote port, a front door VPN routing and forwarding (FVRF) name, or an inside VRF (IVRF) name. Typically, the remote IP address will be used to specify a single tunnel to be deleted.

If a local IP address is provided as a parameter when you use the **clear crypto session** command, all the sessions (and their IKE SAs and IPSec SAs) that share the IP address as a local crypto endpoint (IKE local address) will be cleared. If you do not provide a parameter when you use the **clear crypto session** command, all IPSec SAs and IKE SAs that are in the router will be deleted.

How to Configure IP Security VPN Monitoring

See the following sections for configuration tasks for this feature. Each task in the list is identified as either required or optional.

- [Adding the Description of an IKE Peer, page 4](#) (optional)
- [Verifying Peer Descriptions, page 5](#) (optional)
- [Clearing a Crypto Session, page 6](#) (optional)

Adding the Description of an IKE Peer

To add the description of an IKE peer to an IPSec VPN session, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer {ip-address ip-address}**
4. **description**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	crypto isakmp peer {ip-address ip-address} Example: Router (config)# crypto isakmp peer address 10.2.2.9	Enables an IPSec peer for IKE querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode and enters ISAKMP peer configuration mode.
Step 4	description Example: Router (config-isakmp-peer)# description connection from site A	Adds a description for an IKE peer.

Verifying Peer Descriptions

To verify peer descriptions, use the **show crypto isakmp peer** command.

SUMMARY STEPS

1. **enable**
2. **show crypto isakmp peer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show crypto isakmp peer Example: Router# show crypto isakmp peer	Displays peer descriptions.

Examples

The following output example verifies that the description “connection from site A” has been added for IKE peer 10.2.2.9:

```
Router# show crypto isakmp peer

Peer: 10.2.2.9 Port: 500
Description: connection from site A
flags: PEER_POLICY
```

When the peer at address 10.2.2.9 connects and the session comes up, the syslog status will be shown as follows:

```
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 10.2.2.9:500 Description: connection from site A Id: ezvpn
```

Clearing a Crypto Session

To clear a crypto session, use the **clear crypto session** command from the router command line. No configuration statements are required in the configuration file to use this command.

SUMMARY STEPS

1. **enable**
2. **clear crypto session**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	clear crypto session Example: Router# clear crypto session	Deletes crypto sessions (IPSec and IKE SAs).

Configuration Examples for IP Security VPN Monitoring

This section provides the following configuration example:

- [show crypto session Command Output: Examples, page 6](#)

show crypto session Command Output: Examples

The following is sample output for the **show crypto session** output without the **detail** keyword:

```
Router# show crypto session

Crypto session current status

Interface: FastEthernet0/1
Session status: UP-ACTIVE
Peer: 172.0.0.2/500
    IKE SA: local 172.0.0.1/500 remote 172.0.0.2/500 Active
    IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 10.30.30.0/255.255.255.0
    Active SAs: 2, origin: crypto map
```

The following is sample output using the **show crypto session command and the detail** keyword:

```
Router# show crypto session detail

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.1.3 port 500 fvrf: (none) ivrf: (none)
    Desc: this is my peer at 10.1.1.3:500 Green
```

```

Phase1_id: 10.1.1.3
IKE SA: local 10.1.1.4/500 remote 10.1.1.3/500 Active
      Capabilities:(none) connid:3 lifetime:22:03:24
IPSEC FLOW: permit 47 host 10.1.1.4 host 10.1.1.3
      Active SAs: 0, origin: crypto map
      Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
      Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
IPSEC FLOW: permit ip host 10.1.1.4 host 10.1.1.3
      Active SAs: 4, origin: crypto map
      Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4605665/2949
      Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4605665/2949

```

Additional References

The following sections provide references related to IP Security VPN Monitoring.

Related Documents

Related Topic	Document Title
IP security, encryption, and IKE	<ul style="list-style-type: none"> Configuring Internet Key Exchange for IPsec VPNs Configuring Security for VPNs with IPsec
Security commands	Cisco IOS Security Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features

- **clear crypto session**
- **description (isakmp peer)**
- **show crypto isakmp peer**
- **show crypto session**

For information about these commands, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



IPsec VPN Accounting

The IPsec VPN Accounting feature allows for a session to be accounted for by indicating when the session starts and when it stops.

A VPN session is defined as an Internet Key Exchange (IKE) security association (SA) and the one or more SA pairs that are created by the IKE SA. The session starts when the first IP Security (IPsec) pair is created and stops when all IPsec SAs are deleted.

Session identifying information and session usage information is passed to the Remote Authentication Dial-In User Service (RADIUS) server via standard RADIUS attributes and vendor-specific attributes (VSAs).

Feature Specifications for IPsec VPN Accounting

Feature History

Release	Modification
12.2(15)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Supported Platforms

Cisco 2610–2613, Cisco 2620–Cisco 2621, Cisco 2650–Cisco 2651, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 3725, Cisco 3745, Cisco 7100, Cisco 7200, Cisco 7400, Cisco ubr7100, Cisco ubr7200.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for IPsec VPN Accounting, page 2](#)
- [Information About IPsec VPN Accounting, page 2](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [How to Configure IPsec VPN Accounting, page 6](#)
- [Configuration Examples for IPsec VPN Accounting, page 12](#)
- [Additional References, page 16](#)
- [Command Reference, page 17](#)
- [Glossary, page 18](#)

Prerequisites for IPsec VPN Accounting

- You should understand how to configure RADIUS and authentication, authorization, and accounting (AAA) accounting.
- You should know how to configure IPsec accounting.

Information About IPsec VPN Accounting

To configure IPsec VPN accounting, you must understand the following concepts:

- [RADIUS Accounting, page 2](#)
- [IKE and IPsec Subsystem Interaction, page 4](#)

RADIUS Accounting

For many large networks, it is required that user activity be recorded for auditing purposes. The method that is used most is RADIUS accounting.

RADIUS accounting allows for a session to be accounted for by indicating when the session starts and when it stops. Additionally, session identifying information and session usage information will be passed to the RADIUS server via RADIUS attributes and VSAs.

RADIUS Start Accounting

The RADIUS Start packet contains many attributes that generally identify who is requesting the service and of what the property of that service consists. [Table 1](#) represents the attributes required for the start.

Table 1 *RADIUS Accounting Start Packet Attributes*

RADIUS Attributes Value	Attribute	Description
1	user-name	Username used in extended authentication (XAUTH).The username may be NULL when XAUTH is not used.
4	nas-ip-address	Identifying IP address of the network access server (NAS) that serves the user. It should be unique to the NAS within the scope of the RADIUS server.
5	nas-port	Physical port number of the NAS that serves the user.

Table 1 *RADIUS Accounting Start Packet Attributes (continued)*

RADIUS Attributes Value	Attribute	Description
8	framed-ip-address	Private address allocated for the IP Security (IPsec) session.
40	acct-status-type	Status type. This attribute indicates whether this accounting request marks the beginning (start), the end (stop), or an update of the session.
41	acct-delay-time	Number of seconds the client has been trying to send a particular record.
44	acct-session-id	Unique accounting identifier that makes it easy to match start and stop records in a log file.
26	vrf-id	String that represents the name of the Virtual Route Forwarder (VRF).
26	isakmp-initiator-ip	Endpoint IP address of the remote Internet Key Exchange (IKE) initiator (V4).
26	isakmp-group-id	Name of the VPN group profile used for accounting.
26	isakmp-phase1-id	Phase 1 identification (ID) used by IKE (for example, domain name [DN], fully qualified domain name [FQDN], IP address) to help identify the session initiator.

RADIUS Stop Accounting

The RADIUS Stop packet contains many attributes that identify the usage of the session. Table 2 represents the additional attributes required for the RADIUS stop packet. It is possible that only the stop packet will be sent without the start if configured to do so. If only the stop packet is sent, this allows an easy way to reduce the number of records going to the AAA server.

Table 2 *RADIUS Accounting Stop Packet Attributes*

RADIUS Attributes Value	Attribute	Description
42	acct-input-octets	Number of octets that have been received from the Unity client over the course of the service that is being provided.
43	acct-output-octets	Number of octets that have been sent to the Unity client in the course of delivering this service.
46	acct-session-time	Length of time (in seconds) that the Unity client has received service.
47	acct-input-packets	Quantity of packets that have been received from the Unity client in the course of delivering this service.
48	acct-output-packets	Quantity of packets that have been sent to the Unity client in the course of delivering this service.
49	acct-terminate-cause	For future use.

Table 2 *RADIUS Accounting Stop Packet Attributes (continued)*

RADIUS Attributes Value	Attribute	Description
52	acct-input-gigawords	How many times the Acct-Input-Octets counter has wrapped around the 2^{32} (2 to the 32nd power) over the course of this service.
52	acct-output-gigawords	How many times the Acct-Input-Octets counter has wrapped around the 2^{32} (2 to the 32nd power) over the course of this service.

RADIUS Update Accounting

RADIUS accounting updates are supported. Packet and octet counts are shown in the updates.

IKE and IPsec Subsystem Interaction

Accounting Start

If IPsec accounting is configured, after IKE phases are complete, an accounting start record is generated for the session. New accounting records are not generated during a rekeying.

The following is an account start record that was generated on a router and that is to be sent to the AAA server that is defined:

```
*Aug 23 04:06:20.131: RADIUS(00000002): sending
*Aug 23 04:06:20.131: RADIUS(00000002): Send Accounting-Request to 10.1.1.4:1646 id 4, len 220
*Aug 23 04:06:20.131: RADIUS: authenticator 38 F5 EB 46 4D BE 4A 6F - 45 EB EF 7D B7 19 FB 3F
*Aug 23 04:06:20.135: RADIUS: Acct-Session-Id [44] 10 "00000001"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 31
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 25 "isakmp-group-id=cclient"
*Aug 23 04:06:20.135: RADIUS: Framed-IP-Address [8] 6 10.13.13.1
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 20
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 14 "vrf-id=cisco"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 35
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 29 "isakmp-initiator-ip=11.1.2.2"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 36
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 30 "connect-progress=No Progress"
*Aug 23 04:06:20.135: RADIUS: User-Name [1] 13 "joe@cclient"
*Aug 23 04:06:20.135: RADIUS: Acct-Status-Type [40] 6 Start [1]
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 25
*Aug 23 04:06:20.135: RADIUS: cisco-nas-port [2] 19 "FastEthernet0/0.1"
*Aug 23 04:06:20.135: RADIUS: NAS-Port [5] 6 0
*Aug 23 04:06:20.135: RADIUS: NAS-IP-Address [4] 6 10.1.1.147
*Aug 23 04:06:20.135: RADIUS: Acct-Delay-Time [41] 6 0
*Aug 23 04:06:20.139: RADIUS: Received from id 21645/4 10.1.1.4:1646, Accounting-response, len 20
*Aug 23 04:06:20.139: RADIUS: authenticator B7 E3 D0 F5 61 9A 89 D8 - 99 A6 8A 8A 98 79 9D 5D
```

Accounting Stop

An accounting stop packet is generated when there are no more flows (IPsec SA pairs) with the remote peer.

The accounting stop records contain the following information:

- Packets out
- Packets in
- Octets out
- Gigawords in
- Gigawords out

Below is an account start record that was generated on a router. The account start record is to be sent to the AAA server that is defined.

```
*Aug 23 04:20:16.519: RADIUS(00000003): Using existing nas_port 0
*Aug 23 04:20:16.519: RADIUS(00000003): Config NAS IP: 100.1.1.147
*Aug 23 04:20:16.519: RADIUS(00000003): sending
*Aug 23 04:20:16.519: RADIUS(00000003): Send Accounting-Request to 100.1.1.4:1646 id 19,
len 238
*Aug 23 04:20:16.519: RADIUS: authenticator 82 65 5B 42 F0 3F 17 C3 - 23 F3 4C 35 A2 8A
3E E6
*Aug 23 04:20:16.519: RADIUS: Acct-Session-Id [44] 10 "00000002"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 20
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 14 "vrf-id=cisco"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 35
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 29 "isakmp-initiator-ip=11.1.1.2"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 36
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 30 "connect-progress=No
Progress"
*Aug 23 04:20:16.519: RADIUS: Acct-Session-Time [46] 6 709
*Aug 23 04:20:16.519: RADIUS: Acct-Input-Octets [42] 6 152608
*Aug 23 04:20:16.519: RADIUS: Acct-Output-Octets [43] 6 152608
*Aug 23 04:20:16.519: RADIUS: Acct-Input-Packets [47] 6 1004
*Aug 23 04:20:16.519: RADIUS: Acct-Output-Packets [48] 6 1004
*Apr 23 04:20:16.519: RADIUS: Acct-Input-Giga-Word[52] 6 0
*Apr 23 04:20:16.519: RADIUS: Acct-Output-Giga-Wor[53] 6 0
*Aug 23 04:20:16.519: RADIUS: Acct-Terminate-Cause[49] 6 none [0]
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 32
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 26 "disc-cause-ext=No Reason"
*Aug 23 04:20:16.519: RADIUS: Acct-Status-Type [40] 6 Stop [2]
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 25
*Aug 23 04:20:16.519: RADIUS: cisco-nas-port [2] 19 "FastEthernet0/0.1"
*Aug 23 04:20:16.519: RADIUS: NAS-Port [5] 6 0
*Aug 23 04:20:16.519: RADIUS: NAS-IP-Address [4] 6 100.1.1.147
*Aug 23 04:20:16.519: RADIUS: Acct-Delay-Time [41] 6 0
*Aug 23 04:20:16.523: RADIUS: Received from id 21645/19 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 04:20:16.523: RADIUS: authenticator F1 CA C1 28 CE A0 26 C9 - 3E 22 C9 DA EA B8
22 A0
```

Accounting Updates

If accounting updates are enabled, accounting updates are sent while a session is “up.” The update interval is configurable. To enable the accounting updates, use the **aaa accounting update** command.

The following is an accounting update record that is being sent from the router:

Router#

```

*Aug 23 21:46:05.263: RADIUS(00000004): Using existing nas_port 0
*Aug 23 21:46:05.263: RADIUS(00000004): Config NAS IP: 100.1.1.147
*Aug 23 21:46:05.263: RADIUS(00000004): sending
*Aug 23 21:46:05.263: RADIUS(00000004): Send Accounting-Request to 100.1.1.4:1646 id 22,
len 200
*Aug 23 21:46:05.263: RADIUS: authenticator 30 FA 48 86 8E 43 8E 4B - F9 09 71 04 4A F1
52 25
*Aug 23 21:46:05.263: RADIUS: Acct-Session-Id [44] 10 "00000003"
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 20
*Aug 23 21:46:05.263: RADIUS: Cisco AVpair [1] 14 "vrf-id=cisco"
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 35
*Aug 23 21:46:05.263: RADIUS: Cisco AVpair [1] 29 "isakmp-initiator-ip=11.1.1.2"
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 36
*Aug 23 21:46:05.263: RADIUS: Cisco AVpair [1] 30 "connect-progress=No
Progress"
*Aug 23 21:46:05.263: RADIUS: Acct-Session-Time [46] 6 109
*Aug 23 21:46:05.263: RADIUS: Acct-Input-Octets [42] 6 608
*Aug 23 21:46:05.263: RADIUS: Acct-Output-Octets [43] 6 608
*Aug 23 21:46:05.263: RADIUS: Acct-Input-Packets [47] 6 4
*Aug 23 21:46:05.263: RADIUS: Acct-Output-Packets [48] 6 4
*Aug 23 21:46:05.263: RADIUS: Acct-Status-Type [40] 6 Watchdog [3]
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 25
*Aug 23 21:46:05.263: RADIUS: cisco-nas-port [2] 19 "FastEthernet0/0.1"
*Aug 23 21:46:05.263: RADIUS: NAS-Port [5] 6 0
*Aug 23 21:46:05.263: RADIUS: NAS-IP-Address [4] 6 100.1.1.147
*Aug 23 21:46:05.263: RADIUS: Acct-Delay-Time [41] 6 0
*Aug 23 21:46:05.267: RADIUS: Received from id 21645/22 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 21:46:05.267: RADIUS: authenticator 51 6B BB 27 A4 F5 D7 61 - A7 03 73 D3 0A AC
1C

```

How to Configure IPsec VPN Accounting

This section contains the following procedures:

- [Configuring IPsec VPN Accounting, page 6](#)
- [Configuring Accounting Updates, page 10](#)
- [Troubleshooting for IPsec VPN Accounting, page 11](#)

Configuring IPsec VPN Accounting

To enable IPsec VPN Accounting, you need to perform the following required task:

Prerequisites

Before configuring IPsec VPN accounting, you must first configure IPsec.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login *list-name* method**

5. **aaa authorization network** *list-name method*
6. **aaa accounting network** *list-name start-stop [broadcast] group group-name*
7. **aaa session-id common**
8. **crypto isakmp profile** *profile-name*
9. **vrf** *ivrif*
10. **match identity group** *group-name*
11. **client authentication list** *list-name*
12. **isakmp authorization list** *list-name*
13. **client configuration address** [initiate | respond]
14. **accounting** *list-name*
15. **exit**
16. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
17. **set transform-set** *transform-set-name*
18. **set isakmp-profile** *profile-name*
19. **reverse-route** [remote-peer]
20. **exit**
21. **crypto map** *map-name ipsec-isakmp dynamic dynamic-template-name*
22. **radius-server host** *ip-address* [auth-port *port-number*] [acct-port *port-number*]
23. **radius-server key** *string*
24. **radius-server vsa send accounting**
25. **interface** *interface-id*
26. **crypto map** *map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router (config)# aaa new-model	Enables periodic interim accounting records to be sent to the accounting server.

	Command or Action	Purpose
Step 4	aaa authentication login <i>list-name method</i> Example: Router (config)# aaa authentication login cisco-client group radius	Enforces authentication, authorization, and accounting (AAA) authentication for extended authorization (XAUTH) via RADIUS or local.
Step 5	aaa authorization network <i>list-name method</i> Example: Router (config)# aaa authorization network cisco-client group radius	Sets AAA authorization parameters on the remote client from RADIUS or local.
Step 6	aaa accounting network list-name start-stop [broadcast] group group-name Example: Router (config)# aaa accounting network acc start-stop broadcast group radius	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
Step 7	aaa session-id common Example: Router (config)# aaa session-id common	Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.
Step 8	crypto isakmp profile profile-name Example: Route (config)# crypto isakmp profile cisco	Audits IP security (IPsec) user sessions and enters isakmp-profile submode.
Step 9	vrf ivrf Example: Router (conf-isa-prof)# vrf cisco	Associates the on-demand address pool with a Virtual Private Network (VPN) routing and forwarding (VRF) instance name.
Step 10	match identity group group-name Example: Router(conf-isa-prof)# match identity group cisco	Matches an identity from a peer in an ISAKMP profile.
Step 11	client authentication list list-name Example: Router(conf-isa-prof)# client authentication list cisco	Configures Internet Key Exchange (IKE) extended authentication (XAUTH) in an Internet Security Association and Key Management Protocol (ISAKMP) profile.
Step 12	isakmp authorization list list-name Example: Router(conf-isa-prof)# isakmp authorization list cisco-client	Configures an IKE shared secret and other parameters using the AAA server in an ISAKMP profile. The shared secret and other parameters are generally pushed to the remote peer via mode configuration (MODECFG).

	Command or Action	Purpose
Step 13	client configuration address [initiate respond] Example: Router(conf-isa-prof)# client configuration address respond	Configures IKE mode configuration (MODECFG) in the ISAKMP profile.
Step 14	accounting <i>list-name</i> Example: Router(conf-isa-prof)# accounting acc	Enables AAA accounting services for all peers that connect via this ISAKMP profile.
Step 15	exit Example: Router(conf-isa-prof)# exit	Exits isakmp-profile submode.
Step 16	crypto dynamic-map <i>dynamic-map-name</i> <i>dynamic-seq-num</i> Example: Router(config)# crypto dynamic-map mymap 10 ipsec-isakmp	Creates a dynamic crypto map template and enters the crypto map configuration command mode.
Step 17	set transform-set <i>transform-set-name</i> Example: Router(config-crypto-map)# set transform-set aswan	Specifies which transform sets can be used with the crypto map template.
Step 18	set isakmp-profile <i>profile-name</i> Example: Router(config-crypto-map)# set isakmp-profile cisco	Sets the ISAKMP profile name.
Step 19	reverse-route [remote-peer] Example: Router(config-crypto-map)# reverse-route	Allows routes (ip addresses) to be injected for destinations behind the VPN remote tunnel endpoint and may include a route to the tunnel endpoint itself (using the remote-peer keyword for the crypto map).
Step 20	exit Example: Router(config-crypto-map)# exit	Exits dynamic crypto map configuration mode.
Step 21	crypto map <i>map-name</i> ipsec-isakmp dynamic <i>dynamic-template-name</i> Example: Router(config)# crypto map mymap ipsec-isakmp dynamic dmap	Enters crypto map configuration mode

	Command or Action	Purpose
Step 22	radius-server host <i>ip-address</i> [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] Example: Router(config)# radius-server host 172.16.1.4	Specifies a RADIUS server host.
Step 23	radius-server key <i>string</i> Example: Router(config)# radius-server key nsite	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
Step 24	radius-server vsa send accounting Example: Router(config)# radius-server vsa send accounting	Configures the network access server to recognize and use vendor-specific attributes.
Step 25	interface <i>type slot/port</i> Example: Router(config)# interface FastEthernet 1/0	Configures an interface type and enters interface configuration mode.
Step 26	crypto map <i>map-name</i> Example: Router(config-if)# crypto map mymap	Applies a previously defined crypto map set to an interface.

Configuring Accounting Updates

To send accounting updates while a session is “up,” perform the following optional task:

Prerequisites

Before you configure accounting updates, you must first configure IPsec VPN accounting. See the section “[Configuring IPsec VPN Accounting](#).”

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting update periodic *number***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	aaa accounting update periodic <i>number</i>	(Optional) Enables periodic interim accounting records to be sent to the accounting server.
	Example: Router (config)# aaa accounting update periodic 1-2147483647	

Troubleshooting for IPsec VPN Accounting

To display messages about IPsec accounting events, perform the following optional task:

SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp aaa**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug crypto isakmp aaa	Displays messages about Internet Key Exchange (IKE) events.
	Example: Router# debug crypto isakmp aaa	<ul style="list-style-type: none"> • The aaa keyword specifies accounting events.

Configuration Examples for IPsec VPN Accounting

- [Accounting and ISAKMP-Profile Example, page 12](#)
- [Accounting Without ISAKMP Profiles Example, page 14](#)

Accounting and ISAKMP-Profile Example

The following example shows a configuration for supporting remote access clients with accounting and ISAKMP profiles:

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
authentication pre-share
group 2
!
crypto isakmp policy 10
hash md5
authentication pre-share
lifetime 200
crypto isakmp key cisco address 172.31.100.2

crypto iakmp client configuration group cclient
key jegjegjhrj
pool addressA

crypto-isakmp profile groupA
vrf cisco
match identity group cclient
client authentication list cisco-client
isakmp authorization list cisco-client
client configuration address respond
accounting acc
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto dynamic-map remotes 1
set peer 172.31.100.2
```

```
set security-association lifetime seconds 120
set transform-set esp-des-md5
reverse-route

!
crypto map test 10 ipsec-isakmp dynamic remotes
!
voice call carrier capacity active
!
interface Loopback0
ip address 10.20.20.20 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0
ip address 10.2.80.203 255.255.255.0
no ip mroute-cache
load-interval 30
duplex full
!
interface FastEthernet1/0
ip address 192.168.219.2 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 172.28.100.1 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.20.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73

ip local pool addressA 192.168.1.1 192.168.1.253
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
```

```

gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
exec prompt timestamp
line aux 0
line vty 5 15
  ntp server 172.31.150.52
end

```

Accounting Without ISAKMP Profiles Example

The following example shows a full Cisco IOS configuration that supports accounting remote access peers when ISAKMP profiles are not used:

```

version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
  authentication pre-share
  group 2
!
crypto isakmp policy 10
  hash md5
  authentication pre-share
  lifetime 200
crypto isakmp key cisco address 172.31.100.2
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto map test client accounting list ipsecaaa
crypto map test 10 ipsec-isakmp
  set peer 172.31.100.2
  set security-association lifetime seconds 120
  set transform-set esp-des-md5
  match address 101
!
voice call carrier capacity active
!

```



```
interface Loopback0
 ip address 10.20.20.20 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 10.2.80.203 255.255.255.0
 no ip mroute-cache
 load-interval 30
 duplex full
!
interface FastEthernet1/0
 ip address 192.168.219.2 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 172.28.100.1 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.30.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
 permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
line aux 0
line vty 5 15
!
exception core-file ioscrypto/core/sheep-core
```

```
exception dump 172.25.1.129
ntp clock-period 17208229
ntp server 172.71.150.52
!
end
```

Additional References

For additional information related to IPsec VPN accounting, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring AAA accounting	<ul style="list-style-type: none"> Configuring Accounting
Configuring IPsec VPN accounting	<ul style="list-style-type: none"> Configuring Security for VPNs with IPsec
Configuring basic AAA RADIUS	<ul style="list-style-type: none"> The section “Configuring RADIUS” in the <i>Cisco IOS Security Configuration Guide: User Services</i> on Cisco.com
Configuring ISAKMP profiles	VRF Aware IPsec
Privilege levels with TACACS+ and RADIUS	<ul style="list-style-type: none"> Configuring TACACS+ “Configuring RADIUS” section of the <i>Cisco IOS Security Configuration Guide: User Services</i> on Cisco.com
IP security, RADIUS, and AAA commands	Cisco IOS Security Command Reference

Standards

Standards	Title
None	

MIBs

MIBs	MIBs Link
None	<p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs	Title
None	

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features

- **client authentication list**
- **client configuration address**
- **crypto isakmp profile**
- **crypto map (global IPsec)**
- **debug crypto isakmp**
- **isakmp authorization list**
- **match identity**
- **set isakmp-profile**
- **vrf**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Glossary

IKE—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IP security [IPsec]) that require keys. Before any IPsec traffic can be passed, each router, firewall, and host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a certification authority (CA) service.

IPsec—IP security. IPsec is A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

ISAKMP—Internet Security Association and Key Management Protocol. ISAKMP is an Internet IPsec protocol (RFC 2408) that negotiates, establishes, modifies, and deletes security associations. It also exchanges key generation and authentication data (independent of the details of any specific key generation technique), key establishment protocol, encryption algorithm, or authentication mechanism.

L2TP session—Layer 2 Transport Protocol. L2TP are communications transactions between the L2TP access concentrator (LAC) and the L2TP network server (LNS) that support tunneling of a single PPP connection. There is a one-to-one relationship among the PPP connection, L2TP session, and L2TP call.

NAS—network access server. A NAS is a Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the public switched telephone network [PSTN]).

PFS—perfect forward secrecy. **PFS is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised because subsequent keys are not derived from previous keys.**

QM—Queue Manager. The Cisco IP Queue Manager (IP QM) is an intelligent, IP-based, call-treatment and routing solution that provides powerful call-treatment options as part of the Cisco IP Contact Center (IPCC) solution.

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a database for authenticating modem and ISDN connections and for tracking connection time.

RSA—Rivest, Shamir, and Adelman. Rivest, Shamir, and Adelman are the inventors of the Public-key cryptographic system that can be used for encryption and authentication.

SA—security association. A SA is an instance of security policy and keying material that is applied to a data flow.

TACACS+—Terminal Access Controller Access Control System Plus. TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server.

TED—Tunnel Endpoint Discovery. TED is a Cisco IOS software feature that allows routers to discover IPsec endpoints.

VPN—Virtual Private Network. A VPN enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

VRF—A VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

VSA—vendor-specific attribute. A VSA is an attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.

XAUTH—Extended authentication. XAUTH is an optional exchange between IKE Phase 1 and IKE Phase 2, in which the router demands additional authentication information in an attempt to authenticate the actual user (as opposed to authenticating the peer).

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



Public Key Infrastructure (PKI)



Implementing and Managing PKI Features Roadmap

This roadmap lists the features documented in the *Cisco IOS Security Configuration Guide: Secure Connectivity* and maps them to the modules in which they appear.

Roadmap History

This roadmap was first published on May 2, 2005, and last updated on May 2, 2005.

Feature and Release Support

[Table 56](#) lists public key infrastructure (PKI) feature support for the following Cisco IOS software release trains:

- [Cisco IOS Releases 12.2T, 12.3, and 12.3T](#)

Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table. *Not all features may be supported in your Cisco IOS software release.*

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

[Table 56](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Table 56 **Supported PKI Features**

Release	Feature Name	Feature Description	Where Documented
Cisco IOS Releases 12.2T, 12.3, and 12.3T			
12.3(14)T	Administrative Secure Device Provisioning Introducer	This feature allows you to act as an administrative introducer to introduce a device into a PKI network and then provide a username as the device name for the record locator in the AAA database.	“Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI”
12.3(14)T	Persistent Self-Signed Certificates	This feature allows users the HTTPS server to generate and save a self-signed certificate in the router’s startup configuration. Thus, future SSL handshakes between the client and the HTTPS server can use the same self-signed certificate without user intervention.	“Configuring Certificate Enrollment for a PKI”
12.3(14)T	Secure Device Provisioning Certificate-Based Authorization	This feature allows certificates issued by other authority (CA) servers to be used for SDP introductions.	“Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI”
12.3(14)T	Subordinate Certificate Server	This enhancement allows you to configure a subordinate certificate server to grant all or certain SCEP or manual certificate requests.	“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment”
12.3(14)T	USB Storage	This feature explains how to store RSA keys on a device external to the router via a USB eToken. The SmartCard technology (which is owned by Aladdin Knowledge Systems) in a USB key form factor (also referred to as a USB eToken) provides secure configuration distribution and allows users to store PKI credentials, such as RSA keys, for deployment.	“Storing PKI Credentials External to the Router”
12.3(11)T	The Certificate Server Auto Archive enhancement	This enhancement enables the CA certificate and CA key to be backed up automatically just once after they are generated by the certificate server. As a result, it is not necessary to generate an exportable CA key if CA backup is desirable.	“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment”
12.3(11)T	PKI AAA Authorization Using the Entire Subject Name	This feature provides users with the ability to query the AAA server using the entire subject name from the certificate as a unique AAA username.	“Configuring Revocation and Authorization of Certificates in a PKI”
12.3(11)T	PKI Status	This enhancement added the status keyword to the show crypto pki trustpoints command, which allows you to view the current status of the trustpoint. Prior to this enhancement, you had to issue the show crypto pki certificates and the show crypto pki timers commands for the current status.	“Configuring Certificate Enrollment for a PKI” and “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment”
12.3(11)T	Reenroll Using Existing Certificates	This feature allows users to reenroll a router with a Cisco IOS CA via existing certificates from a third-party vendor CA.	“Configuring Certificate Enrollment for a PKI”
12.3(8)T	Easy Secure Device Deployment	This feature introduces support for SDP (formerly called EzSDD), which offers a web-based enrollment interface that enables network administrators to deploy new devices in large networks.	“Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI”

Table 56 **Supported PKI Features (continued)**

Release	Feature Name	Feature Description	Where Documented
12.3(8)T	Easy Secure Device Deployment AAA Integration	This feature integrates an external AAA database, allowing the introducer to be authenticated against a AAA database instead of having to use the enable password of the local Cisco certificate server.	“Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI”
12.3(7)T	The Certificate Server Registration Authority (RA) Mode enhancement	A certificate server can be configured to run in RA mode.	“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment”
12.3(7)T	The “crypto pki” commands should be a synonym for “crypto ca” commands	This enhancement changes all commands that begin as “crypto ca” to “crypto pki.” Although the router will still accept crypto ca, all output will be read back as crypto pki.	All modules that contain crypto ca commands.
12.3(7)T	Key Rollover for Certificate Renewal	This feature allows the certificate renewal request to be made before the certificate expires and retains the old key and certificate until the new certificate is available.	“Configuring Certificate Enrollment for a PKI”
12.3(7)T	PKI: Query Multiple Servers During Certificate Revocation Check	This feature introduces the ability for Cisco IOS software to make multiple attempts to retrieve the CRL, allowing operations to continue when a particular server is not available. In addition, the ability to override the CDPs in a certificate with a manually configured CDP has been introduced. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for an extended period of time. The certificate’s CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP.	“Configuring Revocation and Authorization of Certificates in a PKI”
12.3(7)T	Protected Private Key Storage	This feature allows a user to encrypt and lock the RSA private keys that are used on a Cisco IOS router, thereby, preventing unauthorized use of the private keys.	“Deploying RSA Keys Within a PKI”
12.3(4)T	Import of RSA Key Pair and Certificates in PEM Format	This feature allows customers to use PEM-formatted files to import or export RSA key pairs. PEM-formatted files allow customers to directly use existing RSA key pairs on their Cisco IOS routers instead of generating new keys. Also, customers can issue certificate requests and receive issued certificates in PEM-formatted files.	“Deploying RSA Keys Within a PKI” and “Configuring Certificate Enrollment for a PKI”
12.3(4)T	Using Certificate ACLs to Ignore Revocation Check and Expired Certificates	This feature allows a certificate that meets specified criteria to be accepted regardless of the validity period of the certificate, or if the certificate meets the specified criteria, revocation checking does not have to be performed. Certificate ACLs are used to specify the criteria that the certificate must meet to be accepted or to avoid revocation checking. In addition, if AAA communication is protected by a certificate, this feature provides for the AAA checking of the certificate to be ignored.	“Configuring Revocation and Authorization of Certificates in a PKI”

Table 56 **Supported PKI Features (continued)**

Release	Feature Name	Feature Description	Where Documented
12.3(4)T	Cisco IOS Certificate Server	This feature introduces support for the Cisco IOS CS, which offers users a CA that is directly integrated with Cisco IOS software to more easily deploy basic PKI networks.	“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment”
12.3(4)T	Direct HTTP Enrollment with CA Servers	This feature allows users to configure an enrollment profile if their CA server does not support SCEP and they do not want to use an RA as a proxy. The enrollment profile allows users to send HTTP requests directly to the CA server instead of the RA proxy.	“Configuring Certificate Enrollment for a PKI”
12.3(2)T	Online Certificate Status Protocol (OCSP)	This feature allows users to enable OCSP instead of CRLs to check certificate status. Unlike CRLs, which provide only periodic certificate status, OCSP can provide timely information regarding the status of a certificate.	“Configuring Revocation and Authorization of Certificates in a PKI”
12.3(1)	PKI Integration with AAA Server	This feature provides additional scalability for authorization by generating a AAA username from the certificate presented by the peer. A AAA server is queried to determine whether the certificate is authorized for use by the internal component. The authorization is indicated by a component-specified label that must be present in the AV pair for the user.	“Configuring Revocation and Authorization of Certificates in a PKI”
12.2(15)T	Certificate Security Attribute-Based Access Control	Under the IPsec protocol, CA interoperability permits Cisco IOS devices and a CA to communicate so that the Cisco IOS device can obtain and use digital certificates from the CA. Certificates contain several fields that are used to determine whether a device or user is authorized to perform a specified action. This feature adds fields to the certificate that allow specifying an ACL, to create a certificate-based ACL.	“Configuring Revocation and Authorization of Certificates in a PKI”
12.2(15)T	Exporting and Importing RSA Keys	This feature allows you to transfer security credentials between devices by exporting and importing RSA keys. The key pair that is shared between two devices will allow one device to immediately and transparently take over the functionality of the other router.	“Deploying RSA Keys Within a PKI”
12.2(15)T	Multiple-Tier CA Hierarchy	This enhancement enables users to set up a PKI in a hierarchical framework to support multiple CAs. Within a hierarchical PKI, all enrolled peers can validate the certificate of one another as long as the peers share a trusted root CA certificate or a common subordinate CA.	“Configuring Certificate Enrollment for a PKI”
12.2(13)T	Manual Certificate Enrollment (TFTP Cut-and-Paste)	This feature allows users to generate a certificate request and accept CA certificates as well as the router’s certificates via a TFTP server or manual cut-and-paste operations.	“Configuring Certificate Enrollment for a PKI”
12.2(8)T	Certificate Autoenrollment	This feature introduces certificate autoenrollment, which allows the router to automatically request a certificate from the CA that is using the parameters in the configuration.	“Configuring Certificate Enrollment for a PKI”

Table 56 **Supported PKI Features (continued)**

Release	Feature Name	Feature Description	Where Documented
12.2(8)T	Certificate Enrollment Enhancements	This feature introduces five new crypto ca trustpoint subcommands that provide new options for certificate requests and allow users to specify fields in the configuration instead of having to go through prompts.	“Configuring Certificate Enrollment for a PKI”
12.2(8)T	Multiple RSA Key Pair Support	This feature allows a user to configure a router to have multiple RSA key pairs. Thus, the Cisco IOS software can maintain a different key pair for each identity certificate.	“Deploying RSA Keys Within a PKI”
12.2(8)T	Trustpoint CLI	This feature introduces the crypto ca trustpoint command, which adds support for trustpoint CAs.	“Configuring Certificate Enrollment for a PKI”

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.





Cisco IOS PKI Overview: Understanding and Planning a PKI

Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL).

This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI.

Module History

This module was first published on May 2, 2005, and last updated on July 17, 2008.

Contents

- [Information About Cisco IOS PKI, page 1](#)
- [Planning for a PKI, page 5](#)
- [Where to Go Next, page 6](#)
- [Additional References, page 6](#)
- [Glossary, page 7](#)

Information About Cisco IOS PKI

Before implementing a basic PKI, you should understand the following concepts:

- [What Is Cisco IOS PKI?, page 2](#)
- [RSA Keys Overview, page 3](#)
- [What Are CAs?, page 3](#)
- [Certificate Enrollment: How It Works, page 4](#)
- [Certificate Revocation: Why It Occurs, page 5](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007, 2008 Cisco Systems, Inc. All rights reserved.

What Is Cisco IOS PKI?

A PKI is composed of the following entities:

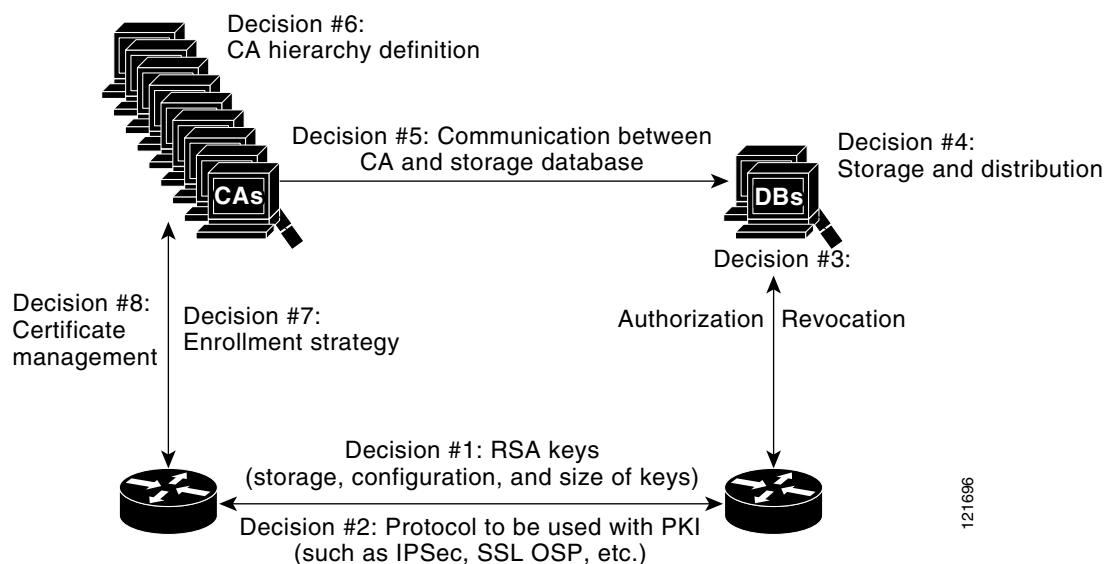
- Peers communicating on a secure network
- At least one certification authority (CA) that grants and maintains certificates
- Digital certificates, which contain information such as the certificate validity period, peer identity information, encryption keys that are used for secure communications, and the signature of the issuing CA
- An optional registration authority (RA) to offload the CA by processing enrollment requests
- A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs)

PKI provides customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Every entity (a person or a device) participating in the secured communication is enrolled in the PKI in a process where the entity generates an Rivest, Shamir, and Adelman (RSA) key pair (one private key and one public key) and has their identity validated by a trusted entity (also known as a CA or trustpoint).

After each entity enrolls in a PKI, every peer (also known as an end host) in a PKI is granted a digital certificate that has been issued by a CA. When peers must negotiate a secured communication session, they exchange digital certificates. Based on the information in the certificate, a peer can validate the identity of another peer and establish an encrypted session with the public keys contained in the certificate.

Although you can plan for and set up your PKI in a number of different ways, [Figure 97](#) shows the major components that make up a PKI and suggests an order in which each decision within a PKI can be made. [Figure 97](#) is a suggested approach; you can choose to set up your PKI from a different perspective.

Figure 97 **Deciding How to Set Up Your PKI**



121696

RSA Keys Overview

An RSA key pair consists of a public key and a private key. When setting up your PKI, you must include the public key in the certificate enrollment request. After the certificate has been granted, the public key will be included in the certificate so that peers can use it to encrypt data that is sent to the router. The private key is kept on the router and used both to decrypt the data sent by peers and to digitally sign transactions when negotiating with peers.

RSA key pairs contain a key modulus value. The modulus determines the size of the RSA key. The larger the modulus, the more secure the RSA key. However, keys with large modulus values take longer to generate, and encryption and decryption operations take longer with larger keys.

What Are CAs?

A CA, also known as a trustpoint, manages certificate requests and issues certificates to participating network devices. These services (managing certificate requests and issuing certificates) provide centralized key management for the participating devices and are explicitly trusted by the receiver to validate identities and to create digital certificates. Before any PKI operations can begin, the CA generates its own public key pair and creates a self-signed CA certificate; thereafter, the CA can sign certificate requests and begin peer enrollment for the PKI.

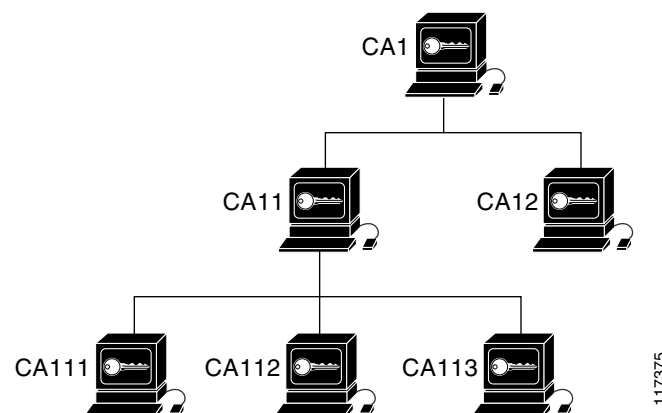
You can use a CA provided by a third-party CA vendor, or you can use an “internal” CA, which is the Cisco IOS Certificate Server.

Hierarchical PKI: Multiple CAs

PKI can be set up in a hierarchical framework to support multiple CAs. At the top of the hierarchy is a root CA, which holds a self-signed certificate. The trust within the entire hierarchy is derived from the RSA key pair of the root CA. The subordinate CAs within the hierarchy can be enrolled with either the root CA or with another subordinate CA. These enrollment options are how multiple tiers of CAs are configured. Within a hierarchical PKI, all enrolled peers, can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA.

Figure 98 shows the enrollment relationships among CAs within a three-tiered hierarchy.

Figure 98 *Three-Tiered CA Hierarchy Sample Topology*



Each CA corresponds to a trustpoint. For example, CA11 and CA12 are subordinate CAs, holding CA certificates that have been issued by CA1; CA111, CA112, and CA113 are also subordinate CAs, but their CA certificates have been issued by CA11.

When to Use Multiple CAs

Multiple CAs provide users with added flexibility and reliability. For example, subordinate CAs can be placed in branch offices while the root CA is at the office headquarters. Also, different granting policies can be implemented per CA, so you can set up one CA to automatically grant certificate requests while another CA within the hierarchy requires each certificate request to be manually granted.

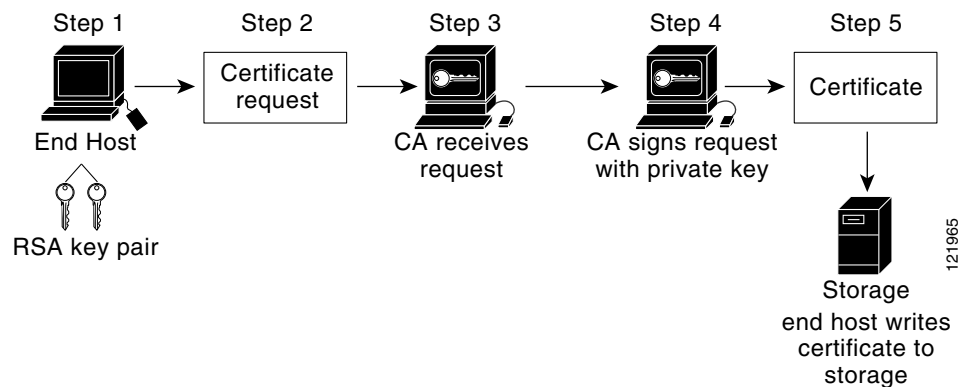
Scenarios in which at least a two-tier CA is recommended are as follows:

- Large and very active networks in which a large number of certificates are revoked and reissued. A multiple tier CA helps to control the size of the CRLs.
- When online enrollment protocols are used, the root CA can be kept offline with the exception of issuing subordinate CA certificates. This scenario provides added security for the root CA.

Certificate Enrollment: How It Works

Certificate enrollment is the process of obtaining a certificate from a CA. Each end host that wants to participate in the PKI must obtain a certificate. Certificate enrollment occurs between the end host requesting the certificate and the CA. [Figure 99](#) and the following steps describe the certificate enrollment process.

Figure 99 *Certificate Enrollment Process*



1. The end host generates an RSA key pair.
2. The end host generates a certificate request and forwards it to the CA (or the RA, if applicable).
3. The CA receives the certificate enrollment request, and, depending on your network configuration, one of the following options occurs:
 - c. Manual intervention is required to approve the request.
 - d. The end host is configured to automatically request a certificate from the CA. Thus, operator intervention is no longer required at the time the enrollment request is sent to the CA server.

**Note**

If you configure the end host to automatically request certificates from the CA, you should have an additional authorization mechanism.

4. After the request is approved, the CA signs the request with its private key and returns the completed certificate to the end host.
5. The end host writes the certificate to a storage area such as NVRAM.

Certificate Enrollment Via Secure Device Provisioning

Secure Device Provisioning (SDP) is a web-based certificate enrollment interface that can be used to easily deploy PKI between two end devices, such as a Cisco IOS client and a Cisco IOS certificate server.

SDP (also referred to as Trusted Transitive Introduction [TTI]) is a communication protocol that provides a bidirectional introduction between two end entities, such as a new network device and a Virtual Private Network (VPN). SDP involves the following three entities:

- **Introducer**—A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- **Petitioner**—A new device that is joined to the secure domain.
- **Registrar**—A certificate server or other server that authorizes the petitioner.

SDP is implemented over a web browser in three phases—welcome, introduction, and completion. Each phase is shown to the user via a web page. For more information on each phase and how SDP works, see the “Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI” module.

Certificate Revocation: Why It Occurs

After each participant has successfully enrolled in the PKI, the peers are ready to begin negotiations for a secure connection with each other. Thus, the peers present their certificates for validation followed by a revocation check. After the peer verifies that the other peer's certificate was issued by an authenticated CA, the CRL or Online Certificate Status Protocol (OCSP) server is checked to ensure that the certificate has not been revoked by the issuing CA. The certificate usually contains a certificate distribution point (CDP) in the form of a URL. Cisco IOS software uses the CDP to locate and retrieve the CRL. If the CDP server does not respond, the Cisco IOS software reports an error, which may result in the peer's certificate being rejected.

Planning for a PKI

Planning for a PKI requires evaluating the requirements and expected use for each of the PKI components shown in [Figure 97](#). It is recommended that you (or the network administrator) thoroughly plan the PKI before beginning any PKI configuration.

Although there are a number of approaches to consider when planning the PKI, this document begins with peer-to-peer communication and proceeds as shown in [Figure 97](#). However you or the network administrator choose to plan the PKI, understand that certain decisions influence other decisions within the PKI. For example, the enrollment and deployment strategy could influence the planned CA hierarchy. Thus, it is important to understand how each component functions within the PKI and how certain component options are dependent upon decisions made earlier in the planning process.

Where to Go Next

As suggested in [Figure 97](#), you begin to configure a PKI by setting up and deploying RSA keys. For more information, see the module “Deploying RSA Keys Within a PKI.”

Additional References

The following sections provide references related to Cisco IOS PKI.

Related Documents

Related Topic	Document Title
PKI commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Security Command Reference
Certificate enrollment: supported methods, enrollment profiles, configuration tasks	“Configuring Certificate Enrollment for a PKI” module
Certificate revocation and authorization: configuration tasks	“Configuring Revocation and Authorization of Certificates in a PKI” module
Cisco IOS certificate server overview information and configuration tasks	“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” module
Secure Device Provisioning: functionality overview and configuration tasks	“Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI” module
Storing RSA keys and certificates on a USB eToken	“Storing PKI Credentials” module

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 2511	Internet X.509 Certificate Request Message Format
RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
RFC 2528	Internet X.509 Public Key Infrastructure
RFC 2559	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
RFC 2585	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP
RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema
RFC 2875	Diffie-Hellman Proof-of-Possession Algorithms
RFC 3029	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Glossary

CDP—certificate distribution point. Field within a digital certificate containing information that describes how to retrieve the CRL for the certificate. The most common CDPs are HTTP and LDAP URLs. A CDP may also contain other types of URLs or an LDAP directory specification. Each CDP contains one URL or directory specification.

certificates—Electronic documents that bind a user's or device's name to its public key. Certificates are commonly used to validate a digital signature.

CRL—certificate revocation list. Electronic document that contains a list of revoked certificates. The CRL is created and digitally signed by the CA that originally issued the certificates. The CRL contains dates for when the certificate was issued and when it expires. A new CRL is issued when the current CRL expires.

CA—certification authority. Service responsible for managing certificate requests and issuing certificates to participating IPsec network devices. This service provides centralized key management for the participating devices and is explicitly trusted by the receiver to validate identities and to create digital certificates.

peer certificate—Certificate presented by a peer, which contains the peer's public key and is signed by the trustpoint CA.

PKI—public key infrastructure. System that manages encryption keys and identity information for components of a network that participate in secured communications.

RA—registration authority. Server that acts as a proxy for the CA so that CA functions can continue when the CA is offline. Although the RA is often part of the CA server, the RA could also be an additional application, requiring an additional device to run it.

RSA keys—Public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. An RSA key pair (a public and a private key) is required before you can obtain a certificate for your router.

**Note**

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006–2009 Cisco Systems, Inc. All rights reserved.



Deploying RSA Keys Within a PKI

First Published: May 2, 2005

Last Updated: November 17, 2006

This module explains how to set up and deploy Rivest, Shamir, and Adelman (RSA) keys within a public key infrastructure (PKI). An RSA key pair (a public and a private key) is required before you can obtain a certificate for your router; that is, the end host must generate a pair of RSA keys and exchange the public key with the certification authority (CA) to obtain a certificate and enroll in a PKI.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for RSA Keys Within a PKI”](#) section on page 20.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Configuring RSA Keys for a PKI, page 2](#)
- [Information About RSA Keys Configuration, page 2](#)
- [How to Set Up and Deploy RSA Keys Within a PKI, page 4](#)
- [Configuration Examples for RSA Key Pair Deployment, page 14](#)
- [Where to Go Next, page 19](#)
- [Additional References, page 19](#)
- [Feature Information for RSA Keys Within a PKI, page 20](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Configuring RSA Keys for a PKI

- Before setting up and deploying RSA keys for a PKI, you should be familiar with the module “Cisco IOS PKI Overview: Understanding and Planning a PKI.”
- As of Cisco IOS Release 12.3(7)T, all commands that begin as “crypto ca” have been changed to begin as “crypto pki.” Although the router will still accept crypto ca commands, all output will be read back as crypto pki.

Information About RSA Keys Configuration

To deploy RSA keys within a PKI, you should understand the following concepts:

- [RSA Keys Overview, page 2](#)
- [Reasons to Store Multiple RSA Keys on a Router, page 3](#)
- [Benefits of Exportable RSA Keys, page 3](#)
- [Passphrase Protection While Importing and Exporting RSA Keys, page 4](#)

RSA Keys Overview

An RSA key pair consists of a public key and a private key. When setting up your PKI, you must include the public key in the certificate enrollment request. After the certificate has been granted, the public key will be included in the certificate so that peers can use it to encrypt data that is sent to the router. The private key is kept on the router and used both to decrypt the data sent by peers and to digitally sign transactions when negotiating with peers.

RSA key pairs contain a key modulus value. The modulus determines the size of the RSA key. The larger the modulus, the more secure the RSA key. However, keys with large modulus values take longer to generate, and encryption and decryption operations take longer with larger keys.

If you want a modulus value between 512 and 1024, enter an integer value that is a multiple of 64. If you want a value higher than 1024, enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

**Note**

As of Cisco IOS Release 12.4(11)T, peer *public* RSA key modulus values up to 4096 bits are automatically supported.

The largest private RSA key modulus is 2048 bits. Therefore, the largest RSA private key a router may generate or import is 2048 bits.

The recommended modulus value for a CA is 2048 bits; the recommended modulus value for a client is 1024 bits.

Usage RSA Keys Versus General-Purpose RSA Keys

There are two mutually exclusive types of RSA key pairs—usage keys and general-purpose keys. When you generate RSA key pairs (via the **crypto key generate rsa** command), you will be prompted to select either usage keys or general-purpose keys.

Usage RSA Keys

Usage keys consist of two RSA key pairs—one RSA key pair is generated and used for encryption and one RSA key pair is generated and used for signatures. With usage keys, each key is not unnecessarily exposed. (Without usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

General-Purpose RSA Keys

General-purpose keys consist of only one RSA key pair that used for both encryption and signatures. General-purpose key pairs are used more frequently than usage key pairs.

Reasons to Store Multiple RSA Keys on a Router

Configuring multiple RSA key pairs allows the Cisco IOS software to maintain a different key pair for each CA with which it is dealing or the software can maintain multiple key pairs and certificates with the same CA. Thus, the Cisco IOS software can match policy requirements for each CA without compromising the requirements specified by the other CAs, such as key length, key lifetime, and general-purpose versus usage keys.

Named key pairs (which are specified via the **label** *key-label* option) allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

Benefits of Exportable RSA Keys



Caution

Exportable RSA keys should be carefully evaluated before use because using exportable RSA keys introduces the risk that these keys might be exposed.

Any existing RSA keys are *not* exportable. New keys are generated as nonexportable by default. It is not possible to convert an existing nonexportable key to an exportable key.

As of Cisco IOS Release 12.2(15)T, users can share the private RSA key pair of a router with standby routers, therefore transferring the security credentials between networking devices. The key pair that is shared between two routers will allow one router to immediately and transparently take over the functionality of the other router. If the main router were to fail, the standby router could be dropped into the network to replace the failed router without the need to regenerate keys, reenroll with the CA, or manually redistribute keys.

Exporting and importing an RSA key pair also enables users to place the same RSA key pair on multiple routers so that all management stations using Secure Shell (SSH) can be configured with a single public RSA key.

Exportable RSA Keys in PEM-Formatted Files

Using privacy-enhanced mail (PEM)-formatted files to import or export RSA keys can be helpful for customers who are running Cisco IOS software Release 12.3(4)T or later and who are using secure socket layer (SSL) or secure shell (SSH) applications to manually generate RSA key pairs and import the keys back into their PKI applications. PEM-formatted files allow customers to directly use existing RSA key pairs on their Cisco IOS routers instead of generating new keys.

Passphrase Protection While Importing and Exporting RSA Keys

You have to include a passphrase to encrypt the PKCS12 file or the PEM file that will be exported, and when the PKCS12 or PEM file is imported, the same passphrase has to be entered to decrypt it. Encrypting the PKCS12 or PEM file when it is being exported, deleted, or imported protects the file from unauthorized access and use while it is being transported or stored on an external device.

The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

How to Convert an Exportable RSA Key Pair to a Nonexportable RSA Key Pair

Passphrase protection protects the external PKCS12 or PEM file from unauthorized access and use. To prevent an RSA key pair from being exported, it must be labeled “nonexportable.” To convert an exportable RSA key pair into a nonexportable key pair, the key pair must be exported and then reimported without specifying the “exportable” keyword.

How to Set Up and Deploy RSA Keys Within a PKI

This section contains the following procedures:

- [Generating an RSA Key Pair, page 4](#)
- [Generating and Storing Multiple RSA Key Pairs, page 5](#)
- [Exporting and Importing RSA Keys, page 6](#)
- [Encrypting and Locking Private Keys on a Router, page 10](#)
- [Removing RSA Key Pair Settings, page 13](#)

Generating an RSA Key Pair

Perform this task to manually generate an RSA key pair.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa {general-keys | usage-keys} [label *key-label*] [modulus *modulus-size*] [exportable]**
4. **exit**
5. **show crypto key mypubkey rsa**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto key generate rsa {general-keys usage-keys} [label key-label] [modulus modulus-size] [exportable] Example: Router(config)# crypto key generate rsa general-keys modulus 360	Generates RSA key pairs. <ul style="list-style-type: none"> If a <i>key-label</i> argument is not specified, the default value, which is the fully qualified domain name (FQDN) of the router, is used.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.
Step 5	show crypto key mypubkey rsa Example: Router# show crypto key mypubkey rsa	(Optional) Displays the RSA public keys of your router. This step allows you to verify that the RSA key pair has been successfully generated.

What to Do Next

After you have successfully generated an RSA key pair, you can proceed to any of the additional tasks in this module to generate additional RSA key pairs, perform export and import of RSA key pairs, or configure additional security parameters for the RSA key pair (such as encrypting or locking the private key).

Generating and Storing Multiple RSA Key Pairs

Perform this task to configure the router to generate and store multiple RSA key pairs and associate the key pairs with a trustpoint.

A trustpoint (also known as a CA) manages certificate requests and issues certificates to participating network devices. These services provide centralized key management for the participating devices and are explicitly trusted by the receiver to validate identities and to create digital certificates. Before any PKI operations can begin, the CA generates its own public key pair and creates a self-signed CA certificate; thereafter, the CA can sign certificate requests and begin peer enrollment for the PKI.

Prerequisites

You must have already generated an RSA key pair as shown in the task “[Generating an RSA Key Pair](#).”

SUMMARY STEPS

1. **crypto pki trustpoint** *name*
2. **rsa**keypair *key-label* [*key-size* [*encryption-key-size*]]
3. **exit**
4. **exit**
5. **show crypto key mypubkey** *rsa*

DETAILED STEPS

	Command or Action	Purpose
Step 1	crypto pki trustpoint <i>name</i> Example: Router(config)# crypto pki trustpoint fancy-ca	Creates a trustpoint and enters ca-trustpoint configuration mode.
Step 2	rsa keypair <i>key-label</i> [<i>key-size</i> [<i>encryption-key-size</i>]] Example: Router(ca-trustpoint)# rsa keypair fancy-keys	Specifies the key pair that is to be used with the trustpoint. <ul style="list-style-type: none"> Specify the <i>key-size</i> argument for generating the key and specify the <i>encryption-key-size</i> argument to request separate encryption, signature keys, and certificates.
Step 3	exit Example: Router(ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.
Step 5	show crypto key mypubkey <i>rsa</i> Example: Router# show crypto key mypubkey <i>rsa</i>	(Optional) Displays the RSA public keys of your router. This step allows you to verify that the RSA key pair has been successfully generated.

Exporting and Importing RSA Keys

This section contains the following tasks that can be used for exporting and importing RSA keys. Whether you are using PKCS12 files or PEM files, exportable RSA keys allow you to use existing RSA keys on Cisco IOS routers instead of having to generate new RSA keys if the main router were to fail.

- [Exporting and Importing RSA Keys in PKCS12 Files, page 7](#)
- [Exporting and Importing RSA Keys in PEM-Formatted Files, page 8](#)

Exporting and Importing RSA Keys in PKCS12 Files

Exporting and importing RSA key pairs enables users to transfer security credentials between devices. The key pair that is shared between two devices allows one device to immediately and transparently take over the functionality of the other router.

Prerequisites for Exporting and Importing RSA Key in PKCS12 Files

You must generate an RSA key pair and mark it “exportable” as specified in the task “[Generating an RSA Key Pair](#).”

Restrictions for Exporting and Importing RSA Keys in PKCS12 Files

- You cannot export RSA keys that existed on the router before your system was upgraded to Cisco IOS Release 12.2(15)T or later. You have to generate new RSA keys and label them as “exportable” after you upgrade the Cisco IOS software.
- When you import a PKCS12 file that was generated by a third-party application, the PKCS12 file must include a CA certificate.
- If you want reexport an RSA key pair after you have already exported the key pair and imported them to a target router, you must specify the **exportable** keyword when you are importing the RSA key pair.
- The largest RSA key a router may import is 2048-bits.

SUMMARY STEPS

1. **crypto pki trustpoint** *name*
2. **rsa****keypair** *key-label* [*key-size* [*encryption-key-size*]]
3. **exit**
4. **crypto pki export** *trustpointname* **pkcs12** *destination-url* *passphrase*
5. **crypto pki import** *trustpointname* **pkcs12** *source-url* *passphrase*
6. **exit**
7. **show crypto key mypubkey** *rsa*

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>crypto pki trustpoint <i>name</i></code> Example: <code>Router(config)# crypto pki trustpoint my-ca</code>	Creates the trustpoint name that is to be associated with the RSA key pair and enters ca-trustpoint configuration mode.
Step 2	<code>rsakeypair <i>key-label</i> [<i>key-size</i> [<i>encryption-key-size</i>]]</code> Example: <code>Router(ca-trustpoint)# rsakeypair my-keys</code>	Specifies the key pair that is to be used with the trustpoint.
Step 3	<code>exit</code> Example: <code>Router(ca-trustpoint)# exit</code>	Exits ca-trustpoint configuration mode.
Step 4	<code>crypto pki export trustpointname pkcs12 <i>destination-url</i> <i>passphrase</i></code> Example: <code>Router(config)# crypto pki export my-ca pkcs12 tftp://tftpserver/my-keys PASSWORD</code>	Exports the RSA keys via the trustpoint name. Note You can export the trustpoint using any of the following file system types: flash, FTP, null, NVRAM, remote file copying (RCP), SCP, system, TFTP, Webflash, Xmodem, or Ymodem.
Step 5	<code>crypto pki import trustpointname pkcs12 <i>source-url</i> <i>passphrase</i></code> Example: <code>Router(config)# crypto pki import my-ca pkcs12 tftp://tftpserver/my-keys PASSWORD</code>	Imports the RSA keys to the target router.
Step 6	<code>exit</code> Example: <code>Router(config)# exit</code>	Exits global configuration mode.
Step 7	<code>show crypto key mypubkey rsa</code> Example: <code>Router# show crypto key mypubkey rsa</code>	(Optional) Displays the RSA public keys of your router.

Exporting and Importing RSA Keys in PEM-Formatted Files

Perform this task to export or import RSA key pairs in PEM files.

Prerequisites for Exporting and Importing RSA Keys in PEM-Formatted Files

You must generate an RSA key pair and mark it “exportable” as specified in the task “[Generating an RSA Key Pair](#).”

Restrictions for Exporting and Importing RSA Keys in PEM Formatted Files

- You cannot export and import RSA keys that were generated without an exportable flag before your system was upgraded to Cisco IOS Release 12.3(4)T or a later release. You have to generate new RSA keys after you upgrade the Cisco IOS software.
- The largest RSA key a router may import is 2048 bits.

SUMMARY STEPS

1. **crypto key generate rsa** {usage-keys | general-keys} label *key-label* [exportable]
2. **crypto key export rsa** *key-label* **pem** {terminal | url *url*} {3des | des} *passphrase*
3. **crypto key import rsa** *key-label* **pem** [usage-keys] {terminal | url *url*} [exportable] *passphrase*

4. **exit**
5. **show crypto key mypubkey rsa**

DETAILED STEPS

	Command or Action	Purpose
Step 1	crypto key generate rsa {usage-keys general-keys} label key-label [exportable] Example: Router(config)# crypto key generate rsa general-keys label mykey exportable	Generates RSA key pairs. To use PEM files, the RSA key pair must be labeled exportable.
Step 2	crypto key export rsa key-label pem {terminal url url} {3des des} passphrase Example: Router(config)# crypto key export rsa mycs pem url nvram: 3des PASSWORD	Exports the generated RSA key pair. Tip Be sure to keep the PEM file safe. For example, you may want to store it on another backup router.
Step 3	crypto key import rsa key-label pem [usage-keys] {terminal url url} [exportable] passphrase Example: Router(config)# crypto key import rsa mycs2 pem url nvram: PASSWORD	Imports the generated RSA key pair. Note If you do not want the key to be exportable from your CA, import it back to the CA after it has been exported as a nonexportable key pair. Thus, the key cannot be taken off again.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.
Step 5	show crypto key mypubkey rsa Example: Router# show crypto key mypubkey rsa	(Optional) Displays the RSA public keys of your router.

Encrypting and Locking Private Keys on a Router

Digital signatures are used to authenticate one device to another device. To use digital signatures, private information (the private key) must be stored on the device that is providing the signature. The stored private information may aid an attacker who steals the hardware device that contains the private key; for example, a thief might be able to use the stolen router to initiate a secure connection to another site by using the RSA private keys stored in the router.



Note

RSA keys are lost during password recovery operations. If you lose your password, the RSA keys will be deleted when you perform the password recovery operation. (This function prevents an attacker from performing password recovery and then using the keys.)

To protect the private RSA key from an attacker, a user can encrypt the private key that is stored in NVRAM via a passphrase. Users can also “lock” the private key, which blocks new connection attempts from a running router and protects the key in the router if the router is stolen by an attempted attacker.

Perform this task to encrypt and lock the private key that is saved to NVRAM.

Prerequisites

Before encrypting or locking a private key, you should perform the following tasks:

- Generate an RSA key pair as shown in the task “[Generating an RSA Key Pair](#).”
- Optionally, you can authenticate and enroll each router with the CA server.



Note

The RSA keys must be unlocked while enrolling the CA. The keys can be locked while authenticating the router with the CA because the private key of the router is not used during authentication.

Restrictions for Encrypting and Locking Private Keys

Backward Compatibility Restriction

Any image prior to Cisco IOS Release 12.3(7)T does not support encrypted keys. To prevent your router from losing all encrypted keys, ensure that only unencrypted keys are written to NVRAM before booting an image prior to Cisco IOS Release 12.3(7)T.

If you must download an image prior to Cisco IOS Release 12.3(7)T, decrypt the key and immediately save the configuration so the downloaded image does not overwrite the configuration.

Interaction with Applications

An encrypted key is not effective after the router boots up until you manually unlock the key (via the **crypto key unlock rsa** command). Depending on which key pairs are encrypted, this functionality may adversely affect applications such as IP security (IPsec), SSH, and SSL; that is, management of the router over a secure channel may not be possible until the necessary key pair is unlocked.

SUMMARY STEPS

1. **crypto key encrypt** [**write**] **rsa** [**name** *key-name*] **passphrase** *passphrase*
2. **exit**
3. **show crypto key mypubkey rsa**
4. **crypto key lock rsa** [**name** *key-name*] **passphrase** *passphrase*
5. **show crypto key mypubkey rsa**
6. **crypto key unlock rsa** [**name** *key-name*] **passphrase** *passphrase*
7. **configure terminal**
8. **crypto key decrypt** [**write**] **rsa** [**name** *key-name*] **passphrase** *passphrase*

DETAILED STEPS

	Command or Action	Purpose
Step 1	crypto key encrypt [write] rsa [name <i>key-name</i>] passphrase <i>passphrase</i> Example: Router(config)# crypto key encrypt write rsa name pki.company.com passphrase password	Encrypts the RSA keys. After this command is issued, the router can continue to use the key; the key remains unlocked. Note If the write keyword is not issued, the configuration must be manually written to NVRAM; otherwise, the encrypted key will be lost next time the router is reloaded.
Step 2	exit Example: Router(config)# exit	Exits global configuration mode.
Step 3	show crypto key mypubkey rsa Example: Router# show crypto key mypubkey rsa	(Optional) Shows that the private key is encrypted (protected) and unlocked. Note You can also use this command to verify that applications such as Internet Key Exchange (IKE) and SSH are properly working after the key has been encrypted.
Step 4	crypto key lock rsa [name <i>key-name</i>] passphrase <i>passphrase</i> Example: Router# crypto key lock rsa name pki.company.com passphrase password	(Optional) Locks the encrypted private key on a running router. Note After the key is locked, it cannot be used to authenticate the router to a peer device. This behavior disables any IPsec or SSL connections that use the locked key. Any existing IPsec tunnels created on the basis of the locked key will be closed. If all RSA keys are locked, SSH will automatically be disabled.
Step 5	show crypto key mypubkey rsa Example: Router# show crypto key mypubkey rsa	(Optional) Shows that the private key is protected and locked. The output will also show failed connection attempts via applications such as IKE, SSH, and SSL.
Step 6	crypto key unlock rsa [name <i>key-name</i>] passphrase <i>passphrase</i> Example: Router# crypto key unlock rsa name pki.company.com passphrase password	(Optional) Unlocks the private key. Note After this command is issued, you can continue to establish IKE tunnels.

	Command or Action	Purpose
Step 7	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 8	<code>crypto key decrypt [write] rsa [name key-name] passphrase passphrase</code> Example: Router(config)# <code>crypto key decrypt write rsa name pki.company.com passphrase password</code>	(Optional) Deletes the encrypted key and leaves only the unencrypted key. Note The write keyword immediately saves the unencrypted key to NVRAM. If the write keyword is not issued, the configuration must be manually written to NVRAM; otherwise, the key will remain encrypted the next time the router is reloaded.

Removing RSA Key Pair Settings

You might want to remove an RSA key pair for one of the following reasons:

- During manual PKI operations and maintenance, old RSA keys can be removed and replaced with new keys.
- An existing CA is replaced and the new CA requires newly generated keys; for example, the required key size might have changed in an organization so you would have to delete the old 1024-bit keys and generate new 2048-bit keys.

Perform this task to remove all RSA keys or the specified RSA key pair that has been generated by your router.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto key zeroize rsa [key-pair-label]`
4. `exit`
5. `show crypto key mypubkey rsa`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto key zeroize rsa [<i>key-pair-label</i>] Example: Router(config)# crypto key zeroize rsa fancy-keys	Deletes RSA key pairs from your router. <ul style="list-style-type: none">• If the <i>key-pair-label</i> argument is not specified, all RSA keys that have been generated by your router will be deleted.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.
Step 5	show crypto key mypubkey rsa Example: Router# show crypto key mypubkey rsa	(Optional) Displays the RSA public keys of your router. This step allows you to verify that the RSA key pair has been successfully generated.

Configuration Examples for RSA Key Pair Deployment

This section contains the following configuration examples:

- [Generating and Specifying RSA Keys: Example, page 14](#)
- [Exporting and Importing RSA Keys: Examples, page 14](#)
- [Encrypting and Locking Private Keys on a Router: Examples, page 18](#)

Generating and Specifying RSA Keys: Example

The following example is a sample trustpoint configuration that shows how to generate and specify the RSA key pair “exampleCAkeys”:

```
crypto key generate rsa general-purpose exampleCAkeys
crypto ca trustpoint exampleCAkeys
  enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
  rsakeypair exampleCAkeys 1024 1024
```

Exporting and Importing RSA Keys: Examples

This section contains the following configuration examples:

- [Exporting and Importing RSA Keys in PKCS12 Files: Example, page 15](#)
- [Generating, Exporting, Importing, and Verifying RSA Keys in PEM Files: Example, page 15](#)
- [Exporting Router RSA Key Pairs and Certificates from PEM Files: Example, page 16](#)
- [Importing Router RSA Key Pairs and Certificate from PEM Files: Example, page 18](#)

Exporting and Importing RSA Keys in PKCS12 Files: Example

In the following example, an RSA key pair “mynewkp” is generated on Router A, and a trustpoint name “mynewtp” is created and associated with the RSA key pair. The trustpoint is exported to a TFTP server, so that it can be imported on Router B. By importing the trustpoint “mynewtp” to Router B, the user has imported the RSA key pair “mynewkp” to Router B.

Router A

```
crypto key generate rsa general label mykeys exportable
! The name for the keys will be:mynewkp
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
!
crypto pki trustpoint mynewtp
  rsakeypair mykeys
exit

crypto pki export mytp pkcs12 flash:myexport companyname
Destination filename [myexport]?
Writing pkcs12 file to tftp://mytftpserver/myexport
CRYPTO_PKI:Exported PKCS12 file successfully.
Verifying checksum... OK (0x3307)
!
Feb 18 17:30:09 GMT:%CRYPTO-6-PKCS12EXPORT_SUCCESS:PKCS #12 Successfully Exported.
```

Router B

```
crypto pki import mynewtp pkcs12 flash:myexport companyname
Source filename [myexport]?
CRYPTO_PKI:Imported PKCS12 file successfully.

!
Feb 18 18:07:50 GMT:%CRYPTO-6-PKCS12IMPORT_SUCCESS:PKCS #12 Successfully Imported.
```

Generating, Exporting, Importing, and Verifying RSA Keys in PEM Files: Example

The following example shows how to generate, export, bring the key back (import), and verify the status of the RSA key pair “mycs”:

```
! Generate the key pair
!
Router(config)# crypto key generate rsa general-purpose label mycs exportable
The name for the keys will be: mycs

Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]
!
```

```

! Archive the key pair to a remote location, and use a good password.
!
Router(config)# crypto key export rsa mycs pem url nvram:3des PASSWORD

% Key name:mycs
Usage:General Purpose Key
Exporting public key...
Destination filename [mycs.pub]?
Writing file to nvram:mycs.pub
Exporting private key...
Destination filename [mycs.prv]?
Writing file to nvram:mycs.prv
!
! Import the key as a different name.
!
Router(config)# crypto key import rsa mycs2 pem url nvram:mycs PASSWORD

% Importing public key or certificate PEM file...
Source filename [mycs.pub]?
Reading file from nvram:mycs.pub
% Importing private key PEM file...
Source filename [mycs.prv]?
Reading file from nvram:mycs.prv% Key pair import succeeded.
!
! After the key has been imported, it is no longer exportable.
!
! Verify the status of the key.
!
Router# show crypto key mypubkey rsa

% Key pair was generated at:18:04:56 GMT Jun 6 2003
Key name:mycs
Usage:General Purpose Key
Key is exportable.
Key Data:
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
% Key pair was generated at:18:17:25 GMT Jun 6 2003
Key name:mycs2
Usage:General Purpose Key
Key is not exportable.
Key Data:
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001

```

Exporting Router RSA Key Pairs and Certificates from PEM Files: Example

The following example shows how to generate and export the RSA key pair “aaa” and certificates of the router in PEM files that are associated with the trustpoint “mycs.” This example also shows PEM-formatted files, which include PEM boundaries before and after the base64-encoded data, that are used by other SSL and SSH applications.

```

Router(config)# crypto key generate rsa general-keys label aaa exportable

The name for the keys will be:aaa

```

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

```

!
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
!
Router(config)# crypto pki trustpoint mycs
Router(ca-trustpoint)# enrollment url http://mycs
Router(ca-trustpoint)# rsakeypair aaa
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate mycs
Certificate has the following attributes:
Fingerprint:C21514AC 12815946 09F635ED FBB6CF31
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
!
Router(config)# crypto pki enroll mycs
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The fully-qualified domain name in the certificate will be: Router
% The subject name in the certificate will be:host.company.com
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

Router(config)# Fingerprint:8DA777BC 08477073 A5BE2403 812DD157

00:29:11:%CRYPTO-6-CERTRET:Certificate received from Certificate Authority

Router(config)# crypto ca export aaa pem terminal 3des password
% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAZCCAa2gAwIBAgIBATANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzES
<snip>
waDeNOSI3WlDa0AWq5DkVBkxwgn0TqIJXJOcTtjHnWHK1LMcMVGn
-----END CERTIFICATE-----

% Key name:aaa
Usage:General Purpose Key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type:4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,ED6B210B626BC81A

Urguv0jnjwOgowWVUQ2XR5nbzzYHI2vGLunpH/IxIsJuNjRVjbAAUpGk7VnPCT87
<snip>
kLC0txzEv7JHc72gMku9uUlrLSnFH5slzAtoC0czfU4=
-----END RSA PRIVATE KEY-----

% Certificate:
-----BEGIN CERTIFICATE-----
MIICTjCCAFigAwIBAgICIQUwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCMVVMx
<snip>
6x1BaIsuMxnHmr89KkKkYlU6

```

```
-----END CERTIFICATE-----
```

Importing Router RSA Key Pairs and Certificate from PEM Files: Example

The following example shows how to import the RSA key pairs and certificate to the trustpoint “ggg” from PEM files via TFTP:

```
Router(config)# crypto pki import ggg pem url tftp://10.1.1.2/username/msca password
% Importing CA certificate...
Address or name of remote host [10.1.1.2]?
Destination filename [username/msca.ca]?
Reading file from tftp://10.1.1.2/username/msca.ca
Loading username/msca.ca from 10.1.1.2 (via Ethernet0):!
[OK - 1082 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [username/msca.prv]?
Reading file from tftp://10.1.1.2/username/msca.prv
Loading username/msca.prv from 10.1.1.2 (via Ethernet0):!
[OK - 573 bytes]

% Importing certificate PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [username/msca.crt]?
Reading file from tftp://10.1.1.2/username/msca.crt
Loading username/msca.crt from 10.1.1.2 (via Ethernet0):!
[OK - 1289 bytes]
% PEM files import succeeded.
Router(config)#
```

Encrypting and Locking Private Keys on a Router: Examples

This section contains the following configuration examples:

- [Configuring and Verifying an Encrypted Key: Example, page 18](#)
- [Configuring and Verifying a Locked Key: Example, page 19](#)

Configuring and Verifying an Encrypted Key: Example

The following example shows how to encrypt the RSA key “pki-123.company.com.” Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the RSA key is encrypted (protected) and unlocked.

```
Router(config)# crypto key encrypt rsa name pki-123.company.com passphrase password
Router(config)# exit
Router# show crypto key mypubkey rsa

% Key pair was generated at:00:15:32 GMT Jun 25 2003
Key name:pki-123.company.com
Usage:General Purpose Key
*** The key is protected and UNLOCKED. ***
Key is not exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E0CC9A 1D23B52C
CD00910C ABD392AE BA6D0E3F FC47A0EF 8AFEE340 0EC1E62B D40E7DCC
23C4D09E
03018B98 E0C07B42 3CFD1A32 2A3A13C0 1FF919C5 8DE9565F 1F020301 0001
```



```
% Key pair was generated at:00:15:33 GMT Jun 25 2003
Key name:pki-123.company.com.server
Usage:Encryption Key
Key is exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D3491E 2A21D383
854D7DA8 58AFBDAC 4E11A7DD E6C40AC6 66473A9F 0C845120 7C0C6EC8 1FFF5757
3A41CE04 FDCB40A4 B9C68B4F BC7D624B 470339A3 DE739D3E F7DDB549 91CD4DA4
DF190D26 7033958C 8A61787B D40D28B8 29BCD0ED 4E6275C0 6D020301 0001
Router#
```

Configuring and Verifying a Locked Key: Example

The following example shows how to lock the key “pki-123.company.com.” Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the key is protected (encrypted) and locked.

```
Router# crypto key lock rsa name pki-123.company.com passphrase password
!
Router# show crypto key mypubkey rsa

% Key pair was generated at:20:29:41 GMT Jun 20 2003
Key name:pki-123.company.com
Usage:General Purpose Key
*** The key is protected and LOCKED. ***
Key is exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D7808D C5FF14AC
0D2B55AC 5D199F2F 7CB4B355 C555E07B 6D0DECBE 4519B1F0 75B12D6F 902D6E9F
B6FDAD8D 654EF851 5701D5D7 EDA047ED 9A2A619D 5639DF18 EB020301 0001
```

Where to Go Next

After you have generated an RSA key pair, you should set up the trustpoint. If you have already set up the trustpoint, you should authenticate and enroll the routers in a PKI. For information on enrollment, see the module “Configuring Certificate Enrollment for a PKI.”

Additional References

The following sections provide references related to configuring RSA keys for a PKI.

Related Documents

Related Topic	Document Title
Overview of PKI, including RSA keys, certificate enrollment, and CAs	“Cisco IOS PKI Overview: Understanding and Planning a PKI” module
PKI commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Security Command Reference

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for RSA Keys Within a PKI

[Table 57](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the *“Implementing and Managing PKI Features Roadmap”*.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

[Table 57](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 57 **Feature Information for RSA Keys Within a PKI**

Feature Name	Software Releases	Feature Configuration Information
Cisco IOS 4096-Bit Peer Public Key Support	12.4(12)T	<p>This feature introduces Cisco IOS 4096-bit peer public key support.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • RSA Keys Overview
Exporting and Importing RSA Keys	12.2(15)T Cisco IOS XE Release 2.1	<p>This feature allows you to transfer security credentials between devices by exporting and importing RSA keys. The key pair that is shared between two devices will allow one device to immediately and transparently take over the functionality of the other router.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Benefits of Exportable RSA Keys • Exporting and Importing RSA Keys in PKCS12 Files <p>The following commands were introduced or modified by this feature: crypto ca export pkcs12, crypto ca import pkcs12, crypto key generate rsa (IKE)</p>
Import of RSA Key Pair and Certificates in PEM Format	12.3(4)T Cisco IOS XE Release 2.1	<p>This feature allows customers to use PEM-formatted files to import or export RSA key pairs. PEM-formatted files allow customers to directly use existing RSA key pairs on their Cisco IOS routers instead of generating new keys.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Benefits of Exportable RSA Keys • Exporting and Importing RSA Keys in PEM-Formatted Files <p>The following commands were introduced by this feature: crypto ca export pem, crypto ca import pem, crypto key export pem, crypto key import pem</p>

Table 57 **Feature Information for RSA Keys Within a PKI (continued)**

Feature Name	Software Releases	Feature Configuration Information
Multiple RSA Key Pair Support	12.2(8)T Cisco IOS XE Release 2.1	<p>This feature allows a user to configure a router to have multiple RSA key pairs. Thus, the Cisco IOS software can maintain a different key pair for each identity certificate.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Reasons to Store Multiple RSA Keys on a Router • Generating and Storing Multiple RSA Key Pairs <p>The following commands were introduced or modified by this feature: crypto key generate rsa, crypto key zeroize rsa, rsa keypair</p>
Protected Private Key Storage	12.3(7)T Cisco IOS XE Release 2.1	<p>This feature allows a user to encrypt and lock the RSA private keys that are used on a Cisco IOS router, thereby, preventing unauthorized use of the private keys.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Encrypting and Locking Private Keys on a Router <p>The following commands were introduced or modified by this feature: crypto key decrypt rsa, crypto key encrypt rsa, crypto key lock rsa, crypto key unlock rsa, show crypto key mypubkey rsa</p>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and

coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



Configuring Authorization and Revocation of Certificates in a PKI

First Published: May 2, 2005

Last Updated: June 19, 2006

This module describes how to configure authorization and revocation of certificates in a public key infrastructure (PKI).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Certificate Authorization and Revocation](#)” section on page 40.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Authorization and Revocation of Certificates](#), page 2
- [Information About Authorization and Revocation of Certificates](#), page 2
- [How to Configure Authorization and Revocation of Certificates for Your PKI](#), page 9
- [Configuration Examples for Setting Up Authorization and Revocation of Certificates](#), page 26
- [Additional References](#), page 39
- [Feature Information for Certificate Authorization and Revocation](#), page 40



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Authorization and Revocation of Certificates

Plan Your PKI Strategy



Tip

It is strongly recommended that you plan your entire PKI strategy before you begin to deploy actual certificates.

Authorization and revocation can occur only after you or a network administrator have completed the following tasks:

- Configured the CA.
- Enrolled peer devices with the CA.
- Identified and configured the protocol (such as IP Security [IPsec] or secure socket layer [SSL]) that is to be used for peer-to-peer communication.

You should decide which authorization and revocation strategy you are going to configure before enrolling peer devices because the peer device certificates might have to contain authorization and revocation-specific information.

“crypto ca” to “crypto pki” CLI Change

As of Cisco IOS Release 12.3(7)T, all commands that begin as “crypto ca” have been changed to begin as “crypto pki.” Although the router will still accept crypto ca commands, all output will be read back as crypto pki.

Information About Authorization and Revocation of Certificates

Before configuring certificate authorization and revocation, you should understand the following concepts:

- [PKI Authorization, page 2](#)
- [PKI and AAA Server Integration for Certificate Status, page 3](#)
- [CRLs or OCSP Server: Choosing a Certificate Revocation Mechanism, page 4](#)
- [When to Use Certificate-Based ACLs for Authorization or Revocation, page 7](#)
- [PKI Certificate Chain Validation, page 8](#)

PKI Authorization

PKI authentication does not provide authorization. Current solutions for authorization are specific to the router that is being configured, although a centrally managed solution is often required.

There is not a standard mechanism by which certificates are defined as authorized for some tasks and not for others. This authorization information can be captured in the certificate itself if the application is aware of the certificate-based authorization information. But this solution does not provide a simple mechanism for real-time updates to the authorization information and forces each application to be aware of the specific authorization information embedded in the certificate.

When the certificate-based ACL mechanism is configured as part of the trustpoint authentication, the application is no longer responsible for determining this authorization information, and it is no longer possible to specify for which application the certificate is authorized. In some cases, the certificate-based ACL on the router gets so large that it cannot be managed. Additionally, it is beneficial to retrieve certificate-based ACL indications from an external server. (For more information on using certificate-based ACLs for authentication, see the section [“When to Use Certificate-Based ACLs for Authorization or Revocation.”](#))

Current solutions to the real-time authorization problem involve specifying a new protocol and building a new server (with associated tasks, such as management and data distribution).

PKI and AAA Server Integration for Certificate Status

Integrating your PKI with an authentication, authorization, and accounting (AAA) server provides an alternative online certificate status solution that leverages the existing AAA infrastructure. Certificates can be listed in the AAA database with appropriate levels of authorization. For components that do not explicitly support PKI-AAA, a default label of “all” from the AAA server provides authorization. Likewise, a label of “none” from the AAA database indicates that the specified certificate is not valid. (The absence of any application label is equivalent, but “none” is included for completeness and clarity). If the application component does support PKI-AAA, the component may be specified directly; for example, the application component could be “ipsec,” “ssl,” or “osp.” (ipsec=IP Security, ssl=Secure Sockets Layer, and osp=Open Settlement Protocol.)



Note

- Currently, no application component supports specification of the application label.
- There may be a time delay when accessing the AAA server. If the AAA server is not available, the authorization fails.

RADIUS or TACACS+: Choosing a AAA Server Protocol

The AAA server can be configured to work with either the RADIUS or TACACS+ protocol. When you are configuring the AAA server for the PKI integration, you must set the RADIUS or TACACS attributes that are required for authorization.

If the RADIUS protocol is used, the password that is configured for the username in the AAA server should be set to “cisco,” which is acceptable because the certificate validation provides authentication and the AAA database is only being used for authorization. When the TACACS protocol is used, the password that is configured for the username in the AAA server is irrelevant because TACACS supports authorization without requiring authentication (the password is used for authentication).

In addition, if you are using TACACS, you must add a PKI service to the AAA server. The custom attribute “cert-application=all” is added under the PKI service for the particular user or usergroup to authorize the specific username.

Attribute-Value Pairs for PKI and AAA Server Integration

[Table 1](#) lists the attribute-value (AV) pairs that are to be used when setting up PKI integration with a AAA server. (Note the values shown in the table are possible values.) The AV pairs must match the client configuration. If they do not match, the peer certificate is not authorized.

**Note**

Users can sometimes have AV pairs that are different from those of every other user. As a result, a unique username is required for each user. The **all** parameter (within the **authorization username** command) specifies that the entire subject name of the certificate will be used as the authorization username.

Table 1 *AV Pairs That Must Match*

AV Pair	Value
cisco-avpair=pki:cert-application=all	Valid values are “all” and “none.”
cisco-avpair=pki:cert-trustpoint=msca	<p>The value is a Cisco IOS command-line interface (CLI) configuration trustpoint label.</p> <p>Note The cert-trustpoint AV pair is normally optional. If it is specified, the Cisco IOS router query must be coming from a certificate trustpoint that has a matching label, and the certificate that is authenticated must have the specified certificate serial number.</p>
cisco-avpair=pki:cert-serial=16318DB7000100001671	<p>The value is a certificate serial number.</p> <p>Note The cert-serial AV pair is normally optional. If it is specified, the Cisco IOS router query must be coming from a certificate trustpoint that has a matching label, and the certificate that is authenticated must have the specified certificate serial number.</p>
cisco-avpair=pki:cert-lifetime-end=1:00 jan 1, 2003	<p>The cert-lifetime-end AV pair is available to artificially extend a certificate lifetime beyond the time period that is indicated in the certificate itself. If the cert-lifetime-end AV pair is used, the cert-trustpoint and cert-serial AV pairs must also be specified. The value must match the following form: hours:minutes month day, year.</p> <p>Note Only the first three characters of a month are used: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. If more than three characters are entered for the month, the remaining characters are ignored (for example Janxxxx).</p>

CRLs or OCSP Server: Choosing a Certificate Revocation Mechanism

After a certificate is validated as a properly signed certificate, a certificate revocation method is performed to ensure that the certificate has not been revoked by the issuing CA. Cisco IOS software supports two revocation mechanisms—certificate revocation lists (CRLs) and Online Certificate Status Protocol (OCSP). (Cisco IOS software also supports AAA integration for certificate checking; however, additional authorization functionality is included. For more information on PKI and AAA certificate authorization and status check, see the section “[PKI and AAA Server Integration for Certificate Status](#).”)

The following sections explain how each revocation mechanism works:

- [What Is a CRL?, page 5](#)
- [What Is OCSP?, page 6](#)

What Is a CRL?

A certificate revocation list (CRL) contains a list of revoked certificates. The CRL is created and digitally signed by the CA that originally issued the certificates. The CRL contains dates for when each certificate was issued and when it expires.

CAs publish new CRLs periodically or when a certificate for which the CA is responsible has been revoked. By default, a new CRL will be downloaded after the currently cached CRL expires. An administrator may also configure the duration for which CRLs are cached in router memory or disable CRL caching completely. The CRL caching configuration will apply to all CRLs associated with a trustpoint.

When the CRL expires, the router deletes it from its cache. A new CRL is downloaded when a certificate is presented for verification; however, if a newer version of the CRL that lists the certificate under examination is on the server but the router is still using the CRL in its cache, the router will not know that the certificate has been revoked. The certificate will pass the revocation check even though it should have been denied.

When a CA issues a certificate, the CA can include in the certificate the CRL distribution point (CDP) for that certificate. Cisco IOS client devices use CDPs to locate and load the correct CRL. The Cisco IOS client supports multiple CDPs, but the Cisco IOS CA currently supports only one CDP; however, third-party vendor CAs may support multiple CDPs or different CDPs per certificate. If a CDP is not specified in the certificate, the client device will use the default Simple Certificate Enrollment Protocol (SCEP) method to retrieve the CRL. (The CDP location can be specified via the **cdp-url** command.)

When implementing CRLs, you should consider the following design considerations:

- CRL lifetimes and the security association (SA) and Internet Key Exchange (IKE) lifetimes
The CRL lifetime determines the length of time between CA-issued updates to the CRL. (The default CRL lifetime value, which is 168 hours [1 week], can be changed via the **lifetime crl** command.)
- The method and location of the CDP
 - The method determines how the CRL is retrieved; some possible choices include HTTP, Lightweight Directory Access Protocol (LDAP), SCEP, or TFTP.
HTTP, TFTP, and LDAP are the most commonly used methods. Although Cisco IOS software defaults to SCEP, an HTTP CDP is recommended for large installations using CRLs because HTTP can be made highly scalable.
 - The location determines from where the CRL is retrieved; for example, you can specify the server and file path from which to retrieve the CRL.

Querying All CDPs During Revocation Check

When a CDP server does not respond to a request, the Cisco IOS software reports an error, which may result in the peer's certificate being rejected. To prevent a possible certificate rejection and if there are multiple CDPs in a certificate, the Cisco IOS software will attempt to use the CDPs in the order in which they appear in the certificate. The router will attempt to retrieve a CRL using each CDP URL or directory specification. If an error occurs using a CDP, an attempt will be made using the next CDP.

**Note**

Prior to Cisco IOS Release 12.3(7)T, the Cisco IOS software makes only one attempt to retrieve the CRL, even when the certificate contains more than one CDP.

**Tip**

Although the Cisco IOS software will make every attempt to obtain the CRL from one of the indicated CDPs, it is recommended that you use an HTTP CDP server with high-speed redundant HTTP servers to avoid application timeouts because of slow CDP responses.

What Is OCSP?

OCSP is an online mechanism that is used to determine certificate validity and provides the following flexibility as a revocation mechanism:

- OCSP can provide real-time certificate status checking.
- OCSP allows the network administrator to specify a central OCSP server, which can service all devices within a network.
- OCSP also allows the network administrator the flexibility to specify multiple OCSP servers, either per client certificate or per group of client certificates.
- OCSP server validation is usually based on the root CA certificate or a valid subordinate CA certificate, but may also be configured so that external CA certificates or self-signed certificates may be used. Using external CA certificates or self-signed certificates allows the OCSP servers certificate to be issued and validated from an alternative PKI hierarchy.

A network administrator can configure an OCSP server to collect and update CRLs from different CA servers. The devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every peer. When peers have to check the revocation status of a certificate, they send a query to the OCSP server that includes the serial number of the certificate in question and an optional unique identifier for the OCSP request, or a nonce. The OCSP server holds a copy of the CRL to determine if the CA has listed the certificate as being revoked; the server then responds to the peer including the nonce. If the nonce in the response from the OCSP server does not match the original nonce sent by the peer, the response is considered invalid and certificate verification fails. The dialog between the OCSP server and the peer consumes less bandwidth than most CRL downloads.

If the OCSP server is using a CRL, CRL time limitations will be applicable; that is, a CRL that is still valid might be used by the OCSP server although a new CRL has been issued by the CRL containing additional certificate revocation information. Because fewer devices are downloading the CRL information on a regular basis, you can decrease the CRL lifetime value or configure the OCSP server not to cache the CRL. For more information, check your OCSP server documentation.

When to Use an OCSP Server

OCSP may be more appropriate than CRLs if your PKI has any of the following characteristics:

- Real-time certificate revocation status is necessary. CRLs are updated only periodically and the latest CRL may not always be cached by the client device. For example, if a client does not yet have the latest CRL cached and a newly revoked certificate is being checked, that revoked certificate will successfully pass the revocation check.

- There are a large number of revoked certificates or multiple CRLs. Caching a large CRL consumes large portions of Cisco IOS memory and may reduce resources available to other processes.
- CRLs expire frequently, causing the CDP to handle a larger load of CRLs.

**Note**

As of Cisco IOS Release 12.4(9)T or later, an administrator may configure CRL caching, either by disabling CRL caching completely or setting a maximum lifetime for a cached CRL per trustpoint.

When to Use Certificate-Based ACLs for Authorization or Revocation

Certificates contain several fields that are used to determine whether a device or user is authorized to perform a specified action.

Because certificate-based ACLs are configured on the device, they do not scale well for large numbers of ACLs; however, certificate-based ACLs do provide very granular control of specific device behavior. Certificate-based ACLs are also leveraged by additional features to help determine when PKI components such as revocation, authorization, or a trustpoint should be used. They provide a general mechanism allowing users to select a specific certificate or a group of certificates that are being validated for either authorization or additional processing.

Certificate-based ACLs specify one or more fields within the certificate and an acceptable value for each specified field. You can specify which fields within a certificate should be checked and which values those fields may or may not have.

There are six logical tests for comparing the field with the value—equal, not equal, contains, does not contain, less than, and greater than or equal. If more than one field is specified within a single certificate-based ACL, the tests of all of the fields within the ACL must succeed to match the ACL. The same field may be specified multiple times within the same ACL. More than one ACL may be specified, and ACL will be processed in turn until a match is found or all of the ACLs have been processed.

Ignore Revocation Checks Using a Certificate-Based ACL

Certificate-based ACLs can be configured to instruct your router to ignore the revocation check and expired certificates of a valid peer. Thus, a certificate that meets the specified criteria can be accepted regardless of the validity period of the certificate, or if the certificate meets the specified criteria, revocation checking does not have to be performed. You can also use a certificate-based ACL to ignore the revocation check when the communication with a AAA server is protected with a certificate.

Ignoring Revocation Lists

To allow a trustpoint to enforce CRLs except for specific certificates, enter the **match certificate** command with the **skip revocation-check** keyword. This type of enforcement is most useful in a hub-and-spoke configuration in which you also want to allow direct spoke-to-spoke connections. In pure hub-and-spoke configurations, all spokes connect only to the hub, so CRL checking is necessary only on the hub. For one spoke to communicate directly with another spoke, the **match certificate** command with the **skip revocation-check** keyword can be used for neighboring peer certificates instead of requiring a CRL on each spoke.

Ignoring Expired Certificates

To configure your router to ignore expired certificates, enter the **match certificate** command with the **allow expired-certificate** keyword. This command has the following purposes:

- If the certificate of a peer has expired, this command may be used to “allow” the expired certificate until the peer can obtain a new certificate.
- If your router clock has not yet been set to the correct time, the certificate of a peer will appear to be not yet valid until the clock is set. This command may be used to allow the certificate of the peer even though your router clock is not set.

**Note**

- If Network Time Protocol (NTP) is available only via the IPsec connection (usually via the hub in a hub-and-spoke configuration), the router clock can never be set. The tunnel to the hub cannot be “brought up” because the certificate of the hub is not yet valid.
- “Expired” is a generic term for a certificate that is expired or that is not yet valid. The certificate has a start and end time. An expired certificate, for purposes of the ACL, is one for which the current time of the router is outside the start and end times specified in the certificate.

Skipping the AAA Check of the Certificate

If the communication with an AAA server is protected with a certificate, and you want to skip the AAA check of the certificate, use the **match certificate** command with the **skip authorization-check** keyword. For example, if a virtual private network (VPN) tunnel is configured so that all AAA traffic goes over that tunnel, and the tunnel is protected with a certificate, you can use the **match certificate** command with the **skip authorization-check** keyword to skip the certificate check so that the tunnel can be established.

The **match certificate** command and the **skip authorization-check** keyword should be configured after PKI integration with an AAA server is configured.

**Note**

If the AAA server is available only via an IPsec connection, the AAA server cannot be contacted until after the IPsec connection is established. The IPsec connection cannot be “brought up” because the certificate of the AAA server is not yet valid.

PKI Certificate Chain Validation

A certificate chain establishes a sequence of trusted certificates—from a peer certificate to the root CA certificate. Within a PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trustpoint.

When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trustpoint, is reached. In Cisco IOS Release 12.4(6)T and later releases, an administrator may configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates.

Configuring the level to which a certificate chain is processed allows for the reauthentication of trusted certificates, the extension of a trusted certificate chain, and the completion of a certificate chain that contains a gap.

Reauthentication of Trusted Certificates

The default behavior is for the router to remove any trusted certificates from the certificate chain sent by the peer before the chain is validated. An administrator may configure certificate chain path processing so that the router does not remove CA certificates that are already trusted before chain validation, so that all certificates in the chain are re-authenticated for the current session.

Extending the Trusted Certificate Chain

The default behavior is for the router to use its trusted certificates to extend the certificate chain if there are any missing certificates in the certificate chain sent by the peer. The router will validate only certificates in the chain sent by the peer. An administrator may configure certificate chain path processing so that the certificates in the peer's certificate chain and the router's trusted certificates are validated to a specified point.

Completing Gaps in a Certificate Chain

An administrator may configure certificate chain processing so that if there is a gap in the configured Cisco IOS trustpoint hierarchy, certificates sent by the peer can be used to complete the set of certificates to be validated.

**Note**

If the trustpoint is configured to require parent validation and the peer does not provide the full certificate chain, the gap cannot be completed and the certificate chain is rejected and invalid.

**Note**

It is a configuration error if the trustpoint is configured to require parent validation and there is no parent trustpoint configured. The resulting certificate chain gap cannot be completed and the subordinate CA certificate cannot be validated. The certificate chain is invalid.

How to Configure Authorization and Revocation of Certificates for Your PKI

This section contains the following procedures:

- [Configuring PKI Integration with a AAA Server, page 9](#)
- [Configuring a Revocation Mechanism for PKI Certificate Status Checking, page 13](#)
- [Configuring Certificate Authorization and Revocation Settings, page 16](#)
- [Configuring Certificate Chain Validation, page 25](#)

Configuring PKI Integration with a AAA Server

Perform this task to generate a AAA username from the certificate presented by the peer and specify which fields within a certificate should be used to build the AAA database username.

Restrictions When Using the Entire Subject Name for PKI Authorization

The following restrictions should be considered when using the **all** keyword as the subject name for the **authorization username** command:

- Some AAA servers limit the length of the username (for example, to 64 characters). As a result, the entire certificate subject name cannot be longer than the limitation of the server.
- Some AAA servers limit the available character set that may be used for the username (for example, a space [] and an equal sign [=] may not be acceptable). You cannot use the **all** keyword for a AAA server having such a character-set limitation.

- The **subject-name** command in the trustpoint configuration may not always be the final AAA subject name. If the fully qualified domain name (FQDN), serial number, or IP address of the router are included in a certificate request, the subject name field of the issued certificate will also have these components. To turn off the components, use the **fqdn**, **serial-number**, and **ip-address** commands with the **none** keyword.
- CA servers sometimes change the requested subject name field when they issue a certificate. For example, CA servers of some vendors switch the relative distinguished names (RDNs) in the requested subject names to the following order: CN, OU, O, L, ST, and C. However, another CA server might append the configured LDAP directory root (for example, O=cisco.com) to the end of the requested subject name.
- Depending on the tools you choose for displaying a certificate, the printed order of the RDNs in the subject name could be different. Cisco IOS software always displays the least significant RDN first, but other software, such as Open Source Secure Socket Layer (OpenSSL), does the opposite. Therefore, if you are configuring a AAA server with a full distinguished name (DN) (subject name) as the corresponding username, ensure that the Cisco IOS software style (that is, with the least significant RDN first) is used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization network** *listname* [*method*]
5. **crypto pki trustpoint** *name*
6. **enrollment url** *url*
7. **revocation-check** *method*
8. **exit**
9. **authorization username** {*subjectname* *subjectname*}
10. **authorization list** *listname*
11. **tacacs-server host** *hostname* [**key** *string*]
or
radius-server host *hostname* [**key** *string*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
	Example: Router> enable	
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	aaa new-model Example: Router(config)# aaa new-model	Enables the AAA access control model.
Step 4	aaa authorization network listname [method] Example: Router (config)# aaa authorization network maxaaa group tacacs+	Sets the parameters that restrict user access to a network. <ul style="list-style-type: none"> <i>method</i>—Can be group radius, group tacacs+, or group group-name.
Step 5	crypto pki trustpoint name Example: Route (config)# crypto pki trustpoint msca	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 6	enrollment url url Example: Router (ca-trustpoint)# enrollment url http://caserver.mycompany.com	Specifies the enrollment parameters of your CA. <ul style="list-style-type: none"> The <i>url</i> argument is the URL of the CA to which your router should send certificate requests.
Step 7	revocation-check method Example: Router (ca-trustpoint)# revocation-check crl	(Optional) Checks the revocation status of a certificate.
Step 8	exit Example: Router (ca-trustpoint)# exit	Exits ca-trustpoint configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 9	<p>authorization username {subjectname <i>subjectname</i>}</p> <p>Example: Router (config)# authorization username <i>subjectname</i> <i>serialnumber</i></p>	<p>Sets parameters for the different certificate fields that are used to build the AAA username.</p> <p>The <i>subjectname</i> argument can be any of the following:</p> <ul style="list-style-type: none"> • all—Entire distinguished name (subject name) of the certificate. • commonname—Certification common name. • country—Certificate country. • email—Certificate e-mail. • ipaddress—Certificate IP address. • locality—Certificate locality. • organization—Certificate organization. • organizationalunit—Certificate organizational unit. • postalcode—Certificate postal code. • serialnumber—Certificate serial number. • state—Certificate state field. • streetaddress—Certificate street address. • title—Certificate title. • unstructuredname—Certificate unstructured name.
Step 10	<p>authorization list <i>listname</i></p> <p>Example: Route (config)# authorization list maxaaa</p>	Specifies the AAA authorization list.
Step 11	<p>tacacs-server host <i>hostname</i> [key <i>string</i>]</p> <p>Example: Router(config)# tacacs-server host 192.0.2.2 key a_secret_key</p> <p>or</p> <p>radius-server host <i>hostname</i> [key <i>string</i>]</p> <p>Example: Router(config)# radius-server host 192.0.2.1 key another_secret_key</p>	<p>Specifies a TACACS+ host.</p> <p>or</p> <p>Specifies a RADIUS host.</p>

Troubleshooting Tips

To display debug messages for the trace of interaction (message type) between the CA and the router, use the **debug crypto pki transactions** command. (See the sample output, which shows a successful PKI integration with AAA server exchange and a failed PKI integration with AAA server exchange.)

Successful Exchange

Router# **debug crypto pki transactions**

```
Apr 22 23:15:03.695: CRYPTO_PKI: Found a issuer match
Apr 22 23:15:03.955: CRYPTO_PKI: cert revocation status unknown.
Apr 22 23:15:03.955: CRYPTO_PKI: Certificate validated without revocation check
```

Each line that shows “CRYPTO_PKI_AAA” indicates the state of the AAA authorization checks. Each of the AAA AV pairs is indicated, and then the results of the authorization check are shown.

```
Apr 22 23:15:04.019: CRYPTO_PKI_AAA: checking AAA authorization (ipsecca_script_aaalist,
PKIAAA-L, <all>)
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = "15DE")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: authorization passed
Apr 22 23:12:30.327: CRYPTO_PKI: Found a issuer match
```

Failed Exchange

Router# **debug crypto pki transactions**

```
Apr 22 23:11:13.703: CRYPTO_PKI_AAA: checking AAA authorization =
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = "233D")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: parsed cert-lifetime-end as: 21:30:00
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: timezone specific extended
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end is expired
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end check failed.
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: authorization failed
```

In the above failed exchange, the certificate has expired.

Configuring a Revocation Mechanism for PKI Certificate Status Checking

Perform this task to set up a CRL as the certificate revocation mechanism—CRLs or OCSP—that is used to check the status of certificates in a PKI.

The revocation-check Command

Use the **revocation-check** command to specify at least one method (OCSP, CRL, or skip the revocation check) that is to be used to ensure that the certificate of a peer has not been revoked. For multiple methods, the order in which the methods are applied is determined by the order specified via this command.

If your router does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your router will reject the peer’s certificate—unless you include the **none** keyword in your configuration. If the **none** keyword is configured, a revocation check will not be performed and the certificate will always be accepted.

Nonces and Peer Communications with OCSP Servers

When using OCSP, nonces, unique identifiers for OCSP requests, are sent by default during peer communications with your OCSP server. The use of nonces offers a more secure and reliable communication channel between the peer and OCSP server.

If your OCSP server does not support nonces, you may disable the sending of nonces. For more information, check your OCSP server documentation.

Prerequisites

- Before issuing any client certificates, the appropriate settings on the server (such as setting the CDP) should be configured.
- When configuring an OCSP server to return the revocation status for a CA server, the OCSP server must be configured with an OCSP response signing certificate that is issued by that CA server. Ensure that the signing certificate is in the correct format, or the router will not accept the OCSP response. See your OCSP manual for additional information.

Restrictions

- OCSP transports messages over HTTP, so there may be a time delay when you access the OCSP server.
- If the OCSP server depends on normal CRL processing to check revocation status, the same time delay that affects CRLs will also apply to OCSP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint *name***
4. **ocsp url *url***
5. **revocation-check *method1* [*method2* [*method3*]]**
6. **ocsp disable-nonce**
7. **exit**
8. **exit**
9. **show crypto pki certificates**
10. **show crypto pki trustpoints [*status* | *label* [*status*]]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint name Example: Router(config)# crypto pki trustpoint hazel	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 4	ocsp url url Example: Router(ca-trustpoint)# ocsp url http://ocsp-server	(Optional) Specifies the URL of an OCSP server so that the trustpoint can check the certificate status. This URL will override the URL of the OCSP server (if one exists) in the Authority Info Access (AIA) extension of the certificate.
Step 5	revocation-check method1 [method2 [method3]] Example: Router(ca-trustpoint)# revocation-check ocsp none	Checks the revocation status of a certificate. <ul style="list-style-type: none"> crl—Certificate checking is performed by a CRL. This is the default option. none—Certificate checking is ignored. ocsp—Certificate checking is performed by an OCSP server. If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.
Step 6	ocsp disable-nonce Example: Router(ca-trustpoint)# ocsp disable-nonce	(Optional) Specifies that a nonce, or an OCSP request unique identifier, will not be sent during peer communications with the OCSP server.
Step 7	exit Example: Router(ca-trustpoint)# exit	Returns to global configuration mode.
Step 8	exit Example: Router(config)# exit	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 9	<code>show crypto pki certificates</code> Example: Router# show crypto pki certificates	(Optional) Displays information about your certificates.
Step 10	<code>show crypto pki trustpoints [status label [status]]</code> Example: Router# show crypto pki trustpoints	Displays information about the trustpoint configured in router.

Configuring Certificate Authorization and Revocation Settings

Perform this task to specify a certificate-based ACL, to ignore revocation checks or expired certificates, to manually override the default CDP location, to manually override the OCSP server setting, to configure CRL caching, or to set session acceptance or rejection based on a certificate serial number, as appropriate.

Configuring Certificate-Based ACLs to Ignore Revocation Checks

To configure your router to use certificate-based ACLs to ignore revocation checks and expired certificates, perform the following steps:

- Identify an existing trustpoint or create a new trustpoint to be used when verifying the certificate of the peer. Authenticate the trustpoint if it has not already been authenticated. The router may enroll with this trustpoint if you want. Do not set optional CRLs for the trustpoint if you plan to use the **match certificate** command and **skip revocation-check** keyword.
- Determine the unique characteristics of the certificates that should not have their CRL checked and of the expired certificates that should be allowed.
- Define a certificate map to match the characteristics identified in the prior step.
- You can add the **match certificate** command and **skip revocation-check** keyword and the **match certificate command** and **allow expired-certificate** keyword to the trustpoint that was created or identified in the first step.

Manually Overriding CDPs in a Certificate

Users can override the CDPs in a certificate with a manually configured CDP. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for an extended period of time. The certificate's CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP.

Manually Overriding the OCSP Server Setting in a Certificate

Administrators can override the OCSP server setting specified in the Authority Information Access (AIA) field of the client certificate or set by the issuing the **ocsp url** command. One or more OCSP servers may be manually specified, either per client certificate or per group of client certificates by the

match certificate override ocsp command. The **match certificate override ocs**p command overrides the client certificate AIA field or the **ocs url** command setting if a client certificate is successfully matched to a certificate map during the revocation check.

**Note**

Only one OCSF server can be specified per client certificate.

Configuring CRL Cache Control

By default, a new CRL will be downloaded after the currently cached CRL expires. Administrators can either configure the maximum amount of time in minutes a CRL remains in the cache by issuing the **crl cache delete-after** command or disable CRL caching by issuing the **crl cache none** command. Only the **crl-cache delete-after** command or the **crl-cache none** command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed.

Neither the **crl-cache none** command nor the **crl-cache delete-after** command affects the currently cached CRL. If you configure the **crl-cache none** command, all CRLs downloaded after this command is issued will not be cached. If you configure the **crl-cache delete-after** command, the configured lifetime will only affect CRLs downloaded after this command is issued.

This functionality is useful is when a CA issues CRLs with no expiration date or with expiration dates days or weeks ahead.

Configuring Certificate Serial Number Session Control

A certificate serial number can be specified to allow a certificate validation request to be accepted or rejected by the trustpoint for a session. A session may be rejected, depending on certificate serial number session control, even if a certificate is still valid. Certificate serial number session control may be configured by using either a certificate map with the **serial-number** field or an AAA attribute, with the **cert-serial-not** command.

Using certificate maps for session control allows an administrator to specify a single certificate serial number. Using the AAA attribute allows an administrator to specify one or more certificate serial numbers for session control.

Prerequisites

- The trustpoint should be defined and authenticated before attaching certificate maps to the trustpoint.
- The certificate map must be configured before the CDP override feature can be enabled or the **serial-number** command is issued.
- The PKI and AAA server integration must be successfully completed to use AAA attributes as described in [“PKI and AAA Server Integration for Certificate Status.”](#)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki certificate map** *label sequence-number*
4. *field-name match-criteria match-value*

5. **exit**
6. **crypto pki trustpoint** *name*
7. **crl-cache** none
8. **crl-cache delete-after** *time*
9. **match certificate** *certificate-map-label* [**allow expired-certificate** | **skip revocation-check** | **skip authorization-check**]
10. **match certificate** *certificate-map-label* **override cdp** {**url** | **directory**} *string*
11. **match certificate** *certificate-map-label* **override ocsp** [**trustpoint** *trustpoint-label*] *sequence-number* **url** *ocsp-url*
12. **exit**
13. **aaa new-model**
14. **aaa attribute list** *list-name*
15. **attribute type** {*name*} {*label*}
16. **exit**
17. **exit**
18. **show crypto pki certificates**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki certificate map <i>label</i> <i>sequence-number</i> Example: Router(config)# crypto pki certificate map Group 10	Defines values in a certificate that should be matched or not matched and enters ca-certificate-map configuration mode.

	Command or Action	Purpose
Step 4	<p><i>field-name match-criteria match-value</i></p> <p>Example: Router(ca-certificate-map)# subject-name co MyCompany</p>	<p>Specifies one or more certificate fields together with their matching criteria and the value to match.</p> <p>The <i>field-name</i> is one of the following case-insensitive name strings or a date:</p> <ul style="list-style-type: none"> • alt-subject-name • expires-on • issuer-name • name • serial-number • subject-name • unstructured-subject-name • valid-start <p>Note Date field format is dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.</p> <p>The <i>match-criteria</i> is one of the following logical operators:</p> <ul style="list-style-type: none"> • co —contains (valid only for name fields and serial number field) • eq —equal (valid for name, serial number, and date fields) • ge —greater than or equal (valid only for date fields) • lt —less than (valid only for date fields) • nc —does not contain (valid only for name fields and serial number field) • ne —not equal (valid for name, serial number, and date fields) <p>The <i>match-value</i> is the name or date to test with the logical operator assigned by match-criteria.</p> <p>Note Use this command only when setting up a certificate-based ACL—not when setting up a certificate-based ACL to ignore revocation checks or expired certificates.</p>
Step 5	<p>exit</p> <p>Example: Router(ca-certificate-map)# exit</p>	Returns to global configuration mode.
Step 6	<p>crypto pki trustpoint name</p> <p>Example: Router(config)# crypto pki trustpoint Access2</p>	Declares the trustpoint, given name and enters ca-trustpoint configuration mode.

	Command or Action	Purpose
Step 7	crl-cache none Example: Router(ca-trustpoint)# crl-cache none	(Optional) Disables CRL caching completely for all CRLs associated with the trustpoint. The crl-cache none command does not affect any currently cached CRLs. All CRLs downloaded after this command is configured will not be cached.
Step 8	crl-cache delete-after time Example: Router(ca-trustpoint)# crl-cache delete-after 2	(Optional) Specifies the maximum time CRLs will remain in the cache for all CRLs associated with the trustpoint. <ul style="list-style-type: none"> <i>time</i>—The amount of time in minutes before the CRL is deleted. The crl-cache delete-after command does not affect any currently cached CRLs. The configured lifetime will only affect CRLs downloaded after this command is configured.
Step 9	match certificate certificate-map-label [allow expired-certificate skip revocation-check skip authorization-check] Example: Router(ca-trustpoint)# match certificate Group skip revocation-check	(Optional) Associates the certificate-based ACL (that was defined via the crypto pki certificate map command) to a trustpoint. <ul style="list-style-type: none"> <i>certificate-map-label</i>—Must match the <i>label</i> argument specified via the crypto pki certificate map command. allow expired-certificate—Ignores expired certificates. skip revocation-check—Allows a trustpoint to enforce CRLs except for specific certificates. skip authorization-check—Skips the AAA check of a certificate when PKI integration with an AAA server is configured.
Step 10	match certificate certificate-map-label override cdp {url directory} string Example: Router(ca-trustpoint)# match certificate Group1 override cdp url http://server.cisco.com	(Optional) Manually overrides the existing CDP entries for a certificate with a URL or directory specification. <ul style="list-style-type: none"> <i>certificate-map-label</i>—A user-specified label that must match the <i>label</i> argument specified in a previously defined crypto pki certificate map command. url—Specifies that the certificate's CDPs will be overridden with an HTTP or LDAP URL. directory—Specifies that the certificate's CDPs will be overridden with an LDAP directory specification. <i>string</i>—The URL or directory specification. <p>Note Some applications may time out before all CDPs have been tried and will report an error message. The error message will not affect the router, and the Cisco IOS software will continue attempting to retrieve a CRL until all CDPs have been tried.</p>

	Command or Action	Purpose
Step 11	<p>match certificate <i>certificate-map-label</i> override ocs [<i>trustpoint trustpoint-label</i>] <i>sequence-number url ocs</i>-url</p> <p>Example: Router(ca-trustpoint)# match certificate mycertmapname override ocs trustpoint mytp 15 url http://192.0.2.2</p>	<p>(Optional) Specifies an OCS server, either per client certificate or per group of client certificates, and may be issued more than once to specify additional OCS servers and client certificate settings including alternative PKI hierarchies.</p> <ul style="list-style-type: none"> • <i>certificate-map-label</i>—The name of an existing certificate map. • trustpoint—The trustpoint to be used when validating the OCS server certificate. • <i>sequence-number</i>—The order the match certificate override ocs command statements apply to the certificate being verified. Matches are performed from the lowest sequence number to the highest sequence number. If more than one command is issued with the same sequence number, it overwrites the previous OCS server override setting. • url—The URL of the OCS server. <p>When the certificate matches a configured certificate map, the AIA field of the client certificate and any previously issued ocs url command settings are overwritten with the specified OCS server.</p> <p>If no map-based match occurs, one of the following two cases will continue to apply to the client certificate.</p> <ul style="list-style-type: none"> • If OCS is specified as the revocation method, the AIA field value will continue to apply to the client certificate. • If the ocs url configuration exists, the ocs url configuration settings will continue to apply to the client certificates.
Step 12	<p>exit</p> <p>Example: Router(ca-trustpoint)# exit</p>	Returns to global configuration mode.
Step 13	<p>aaa new-model</p> <p>Example: Router(config)# aaa new-model</p>	(Optional) Enables the AAA access control model.
Step 14	<p>aaa attribute list <i>list-name</i></p> <p>Example: Router(config)# aaa attribute list crl</p>	(Optional) Defines an AAA attribute list locally on a router and enters config-attr-list configuration mode.

	Command or Action	Purpose
Step 15	attribute type {name}{value} Example: Router(config-attr-list)# attribute type cert-serial-not 6C4A	(Optional) Defines an AAA attribute type that is to be added to an AAA attribute list locally on a router. To configure certificate serial number session control, an administrator may specify a specific certificate in the <i>value</i> field to be accepted or rejected based on its serial number where <i>name</i> is set to cert-serial-not . If the serial number of the certificate matches the serial number specified by the attribute type setting, the certificate will be rejected. For a full list of available AAA attribute types, execute the show aaa attributes command.
Step 16	exit Example: Router(ca-trustpoint)# exit Example: Router(config-attr-list)# exit	Returns to global configuration mode.
Step 17	exit Example: Router(config)# exit	Returns to privileged EXEC mode.
Step 18	show crypto pki certificates Example: Router# show crypto pki certificates	(Optional) Displays the components of the certificates installed on the router if the CA certificate has been authenticated.

Examples

The following is a sample OCSP response when signing a certificate. The OCSP-related extensions are in bold.

```
Certificate:
  Data:
    Version: v3
    Serial Number:0x14
    Signature Algorithm:MD5withRSA - 1.2.840.113549.1.1.4
    Issuer:CN=CA server,OU=PKI,O=Cisco Systems
    Validity:
      Not Before:Thursday, August 8, 2002 4:38:05 PM PST
      Not After:Tuesday, August 7, 2003 4:38:05 PM PST
    Subject:CN=OCSP server,OU=PKI,O=Cisco Systems
    Subject Public Key Info:
      Algorithm:RSA - 1.2.840.113549.1.1.1
      Public Key:
        Exponent:65537
        Public Key Modulus:(1024 bits) :
          <snip>

    Extensions:
      Identifier:Subject Key Identifier - 2.5.29.14
      Critical:no
```

```

Key Identifier:
  <snip>
Identifier:Authority Key Identifier - 2.5.29.35
Critical:no
Key Identifier:
  <snip>

Identifier:OCSP NoCheck:- 1.3.6.1.5.5.7.48.1.5
Critical:no
Identifier:Extended Key Usage:- 2.5.29.37
Critical:no
Extended Key Usage:
  OCSPSigning
Identifier:CRL Distribution Points - 2.5.29.31
Critical:no
Number of Points:1
Point 0
  Distribution Point:
[URIName:ldap://CA-server/CN=CA server,OU=PKI,O=Cisco Systems]
Signature:
  Algorithm:MD5withRSA - 1.2.840.113549.1.1.4
Signature:
  <snip>

```

The following example shows an excerpt of the running configuration output when adding a **match certificate override ocs** command to the beginning of an existing sequence:

```

match certificate map3 override ocs 5 url http://192.0.2.3/
show running-configuration
.
.
.
      match certificate map3 override ocs 5 url http://192.0.2.3/
      match certificate map1 override ocs 10 url http://192.0.2.1/
      match certificate map2 override ocs 15 url http://192.0.2.2/

```

The following example shows an excerpt of the running configuration output when an existing **match certificate override ocs** command is replaced and a trustpoint is specified to use an alternative PKI hierarchy:

```

match certificate map4 override ocs trustpoint tp4 10 url http://192.0.2.4/newvalue
show running-configuration
.
.
.
      match certificate map3 override ocs trustpoint tp3 5 url http://192.0.2.3/
      match certificate map1 override ocs trustpoint tp1 10 url http://192.0.2.1/
      match certificate map4 override ocs trustpoint tp4 10 url
        http://192.0.2.4/newvalue
      match certificate map2 override ocs trustpoint tp2 15 url http://192.0.2.2/

```

Troubleshooting Tips

If you ignored revocation check or expired certificates, you should carefully check your configuration. Verify that the certificate map properly matches either the certificate or certificates that should be allowed or the AAA checks that should be skipped. In a controlled environment, try modifying the certificate map and determine what is not working as expected.

Configuring Certificate Chain Validation

Perform this task to configure the processing level for the certificate chain path of your peer certificates.

Prerequisites

- The device must be enrolled in your PKI hierarchy.
- The appropriate key pair must be associated with the certificate.

Restrictions

- A trustpoint associated with the root CA cannot be configured to be validated to the next level.

The **chain-validation** command is configured with the **continue** keyword for the trustpoint associated with the root CA, an error message will be displayed and the chain validation will revert to the default **chain-validation** command setting.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **chain-validation** [{**stop** | **continue**} [*parent-trustpoint*]]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint name Example: Router(config)# crypto pki trustpoint ca-sub1	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 4	chain-validation [{ stop continue } [<i>parent-trustpoint</i>]] Example: Router(ca-trustpoint)# chain-validation continue ca-sub1	Configures the level to which a certificate chain is processed on all certificates including subordinate CA certificates. <ul style="list-style-type: none">Use the stop keyword to specify that the certificate is already trusted. This is the default setting.Use the continue keyword to specify that the subordinate CA certificate associated with the trustpoint must be validated.The <i>parent-trustpoint</i> argument specifies the name of the parent trustpoint the certificate must be validated against.
Step 5	exit Example: Router(ca-trustpoint)# exit	Returns to global configuration mode

Configuration Examples for Setting Up Authorization and Revocation of Certificates

This section contains the following configuration examples:

- [Configuring and Verifying PKI AAA Authorization: Examples, page 27](#)
- [Configuring a Revocation Mechanism: Examples, page 31](#)
- [Configuring a Hub Router at a Central Site for Certificate Revocation Checks: Example, page 32](#)
- [Configuring Certificate Authorization and Revocation Settings: Examples, page 36](#)
- [Configuring Certificate Chain Validation: Examples, page 38](#)

Configuring and Verifying PKI AAA Authorization: Examples

This section provides configuration examples of PKI AAA authorizations:

- [Router Configuration: Example, page 27](#)
- [Debug of a Successful PKI AAA Authorization: Example, page 29](#)
- [Debugs of a Failed PKI AAA Authorization: Example, page 30](#)

Router Configuration: Example

The following **show running-config** command output shows the working configuration of a router that is set up to authorize VPN connections using the PKI Integration with AAA Server feature:

```
Router# show running-config

Building configuration...
!
version 12.3
!
hostname router7200router7200
!
aaa new-model
!
!
aaa authentication login default group tacacs+
aaa authentication login no_tacacs enable
aaa authentication ppp default group tacacs+
aaa authorization exec ACSLab group tacacs+
aaa authorization network ACSLab group tacacs+
aaa accounting exec ACSLab start-stop group tacacs+
aaa accounting network default start-stop group ACSLab
aaa session-id common
!
ip domain name company.com
!
crypto pki trustpoint EM-CERT-SERV
  enrollment url http://192.0.2.33:80
  serial-number
  crl optional
  rsa-keypair STOREVPN 1024
  auto-enroll
  authorization list ACSLab
!
crypto pki certificate chain EM-CERT-SERV
certificate 04
  30820214 3082017D A0030201 02020104 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30343031
  31393232 30323535 5A170D30 35303131 38323230 3235355A 3030312E 300E0603
  55040513 07314437 45424434 301C0609 2A864886 F70D0109 02160F37 3230302D
  312E6772 696C2E63 6F6D3081 9F300D06 092A8648 86F70D01 01010500 03818D00
  30818902 818100BD F3B837AA D925F391 2B64DA14 9C2EA031 5A7203C4 92F8D6A8
  7D2357A6 BCC8596F A38A9B10 47435626 D59A8F2A 123195BB BE5A1E74 B1AA5AE0
  5CA162FF 8C3ACA4F B3EE9F27 8B031642 B618AE1B 40F2E3B4 F996BEFE 382C7283
  3792A369 236F8561 8748AA3F BC41F012 B859BD9C DB4F75EE 3CEE2829 704BD68F
  FD904043 0F555702 03010001 A3573055 30250603 551D1F04 1E301C30 1AA018A0
  16861468 7474703A 2F2F3633 2E323437 2E313037 2E393330 0B060355 1D0F0404
  030205A0 301F0603 551D2304 18301680 1420FC4B CF0B1C56 F5BD4C06 0AFD4E67
  341AE612 D1300D06 092A8648 86F70D01 01040500 03818100 79E97018 FB955108
  12F42A56 2A6384BC AC8E22FE F1D6187F DA5D6737 C0E241AC AAAEC75D 3C743F59
  08DEEFF2 0E813A73 D79E0FA9 D62DC20D 8E2798CD 2C1DC3EC 3B2505A1 3897330C
```

```

15A60D5A 8A13F06D 51043D37 E56E45DF A65F43D7 4E836093 9689784D C45FD61D
EC1F160C 1ABC8D03 49FB11B1 DA0BED6C 463E1090 F34C59E4
quit
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30333132
31363231 34373432 5A170D30 36313231 35323134 3734325A 30173115 30130603
55040313 0C454D2D 43455254 2D534552 5630819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C14D 833641CF D784F516 DA6B50C0 7B3CB3C9
589223AB 99A7DC14 04F74EF2 AAEEE8F5 E3BFAE97 F2F980F7 D889E6A1 2C726C69
54A29870 7E7363FF 3CD1F991 F5A37CFF 3FFDD3D0 9E486C44 A2E34595 C2D078BB
E9DE981E B733B868 AA8916C0 A8048607 D34B83C0 64BDC101 161FC103 13C06500
22D6EE75 7D6CF133 7F1B515F 32830203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
16041420 FC4BCF0B 1C56F5BD 4C060AFD 4E67341A E612D130 1F060355 1D230418
30168014 20FC4BCF 0B1C56F5 BD4C060A FD4E6734 1AE612D1 300D0609 2A864886
F70D0101 04050003 81810085 D2E386F5 4107116B AD3AC990 CBE84063 5FB2A6B5
BD572026 528E92ED 02F3A0AE 1803F2AE AA4C0ED2 0F59F18D 7B50264F 30442C41
0AF19C4E 70BD3CB5 0ADD8DE8 8EF636BD 24410DF4 DB62DAFC 67DA6E58 3879AA3E
12AFB1C3 2E27CB27 EC74E1FC AEE2F5CF AA80B439 615AA8D5 6D6DEDC3 7F9C2C79
3963E363 F2989FB9 795BA8
quit
!
!
crypto isakmp policy 10
  encr 3des
  group 2
!
!
crypto ipsec transform-set ISC_TS_1 esp-3des esp-sha-hmac
!
crypto ipsec profile ISC_IPSEC_PROFILE_2
  set security-association lifetime kilobytes 530000000
  set security-association lifetime seconds 14400
  set transform-set ISC_TS_1
!
!
controller ISA 1/1
!
!
interface Tunnel0
  description MGRE Interface provisioned by ISC
  bandwidth 10000
  ip address 192.0.2.172 255.255.255.0
  no ip redirects
  ip mtu 1408
  ip nhrp map multicast dynamic
  ip nhrp network-id 101
  ip nhrp holdtime 500
  ip nhrp server-only
  no ip split-horizon eigrp 101
  tunnel source FastEthernet2/1
  tunnel mode gre multipoint
  tunnel key 101
  tunnel protection ipsec profile ISC_IPSEC_PROFILE_2
!
interface FastEthernet2/0
  ip address 192.0.2.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet2/1
  ip address 192.0.2.2 255.255.255.0
  duplex auto

```

```

speed auto
!
!
tacacs-server host 192.0.2.55 single-connection
tacacs-server directed-request
tacacs-server key company lab
!
ntp master 1
!
end

```

Debug of a Successful PKI AAA Authorization: Example

The following **show debugging** command output shows a successful authorization using the PKI Integration with AAA Server feature:

Router# **show debugging**

General OS:

```

TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on

```

Cryptographic Subsystem:

Crypto PKI Trans debugging is on

Router#

```

May 28 19:36:11.117: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:36:12.789: CRYPTO_PKI: Found a issuer match
May 28 19:36:12.805: CRYPTO_PKI: cert revocation status unknown.
May 28 19:36:12.805: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:36:12.813: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.company.com,
<all>)
May 28 19:36:12.813: AAA/BIND(00000042): Bind i/f
May 28 19:36:12.813: AAA/AUTHOR (0x42): Pick method list 'ACSLab'
May 28 19:36:12.813: TPLUS: Queuing AAA Authorization request 66 for processing
May 28 19:36:12.813: TPLUS: processing authorization request id 66
May 28 19:36:12.813: TPLUS: Protocol set to None .....Skipping
May 28 19:36:12.813: TPLUS: Sending AV service=pki
May 28 19:36:12.813: TPLUS: Authorization request created for 66(POD5.company.com)
May 28 19:36:12.813: TPLUS: Using server 192.0.2.55
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT/203A4628: Started 5 sec timeout
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:36:12.813: TPLUS: Would block while reading pak header
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 12 header bytes (expect 27 bytes)
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 39 bytes response
May 28 19:36:12.817: TPLUS(00000042)/0/203A4628: Processing the reply packet
May 28 19:36:12.817: TPLUS: Processed AV cert-application=all
May 28 19:36:12.817: TPLUS: received authorization response for 66: PASS
May 28 19:36:12.817: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
May 28 19:36:12.817: CRYPTO_PKI_AAA: authorization passed

```

Router#

Router#

```

May 28 19:36:18.681: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 101: Neighbor 192.0.2.171 (Tunnel0) is
up: new adjacency

```

Router#

Router# **show crypto isakmp sa**

dst	src	state	conn-id	slot
192.0.2.22	192.0.2.102	QM_IDLE	84	0

Debugs of a Failed PKI AAA Authorization: Example

The following **show debugging** command output shows that the router is not authorized to connect using VPN. The messages are typical of those that you might see in such a situation.

In this example, the peer username was configured as not authorized, by moving the username to a Cisco Secure ACS group called VPN_Router_Disabled in Cisco Secure ACS. The router, router7200.company.com, has been configured to check with a Cisco Secure ACS AAA server prior to establishing a VPN connection to any peer.

Router# **show debugging**

General OS:

TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on

Cryptographic Subsystem:

Crypto PKI Trans debugging is on

Router#

```
May 28 19:48:29.837: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:31.509: CRYPTO_PKI: Found a issuer match
May 28 19:48:31.525: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:31.525: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:31.533: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.company.com,
<all>)
May 28 19:48:31.533: AAA/BIND(00000044): Bind i/f
May 28 19:48:31.533: AAA/AUTHOR (0x44): Pick method list 'ACSLab'
May 28 19:48:31.533: TPLUS: Queuing AAA Authorization request 68 for processing
May 28 19:48:31.533: TPLUS: processing authorization request id 68
May 28 19:48:31.533: TPLUS: Protocol set to None .....Skipping
May 28 19:48:31.533: TPLUS: Sending AV service=pki
May 28 19:48:31.533: TPLUS: Authorization request created for 68(POD5.company.com)
May 28 19:48:31.533: TPLUS: Using server 192.0.2.55
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT/203A4C50: Started 5 sec timeout
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:48:31.533: TPLUS: Would block while reading pak header
May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 12 header bytes (expect 6 bytes)
May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 18 bytes response
May 28 19:48:31.537: TPLUS(00000044)/0/203A4C50: Processing the reply packet
May 28 19:48:31.537: TPLUS: received authorization response for 68: FAIL
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:31.537: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:31.537: CRYPTO_PKI: AAA authorization for list 'ACSLab', and user
'POD5.company.com' failed.
May 28 19:48:31.537: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.162 is
bad: certificate invalid
May 28 19:48:39.821: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:41.481: CRYPTO_PKI: Found a issuer match
May 28 19:48:41.501: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:41.501: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:41.505: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.company.com,
<all>)
May 28 19:48:41.505: AAA/BIND(00000045): Bind i/f
May 28 19:48:41.505: AAA/AUTHOR (0x45): Pick method list 'ACSLab'
May 28 19:48:41.505: TPLUS: Queuing AAA Authorization request 69 for processing
May 28 19:48:41.505: TPLUS: processing authorization request id 69
May 28 19:48:41.505: TPLUS: Protocol set to None .....Skipping
May 28 19:48:41.505: TPLUS: Sending AV service=pki
May 28 19:48:41.505: TPLUS: Authorization request created for 69(POD5.company.com)
May 28 19:48:41.505: TPLUS: Using server 198.168.244.55
```

```

May 28 19:48:41.509: TPLUS(00000045)/0/IDLE/63B22834: got immediate connect on new 0
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE/63B22834: Started 5 sec timeout
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE: wrote entire 46 bytes request
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 12 header bytes (expect 6 bytes)
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 18 bytes response
May 28 19:48:41.509: TPLUS(00000045)/0/63B22834: Processing the reply packet
May 28 19:48:41.509: TPLUS: received authorization response for 69: FAIL
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:41.509: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:41.509: CRYPTO_PKI: AAA authorization for list 'ACSLab', and user
'POD5.company.com' failed.
May 28 19:48:41.509: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.162 is
bad: certificate invalid
Router#

Router# show crypto iskmp sa

```

dst	src	state	conn-id	slot
192.0.2.2	192.0.2.102	MM_KEY_EXCH	95	0

Configuring a Revocation Mechanism: Examples

This section contains the following configuration examples that can be used when specifying a revocation mechanism for your PKI:

- [Configuring an OCSP Server: Example, page 31](#)
- [Specifying a CRL and Then an OCSP Server: Example, page 31](#)
- [Specifying an OCSP Server: Example, page 31](#)
- [Disabling Nonces in Communications with the OCSP Server: Example, page 32](#)

Configuring an OCSP Server: Example

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:

```

Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp

```

Specifying a CRL and Then an OCSP Server: Example

The following example shows how to configure the router to download the CRL from the CDP. If the CRL is unavailable, the OCSP server that is specified in the AIA extension of the certificate will be used. If both options fail, certificate verification will also fail.

```

Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsp

```

Specifying an OCSP Server: Example

The following example shows how to configure your router to use the OCSP server at the HTTP URL “http://myocspserver:81.” If the server is down, the revocation check will be ignored.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsdp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsdp none
```

Disabling Nonces in Communications with the OCSP Server: Example

The following example shows communications when a nonce, or a unique identifier for the OCSP request, is disabled for communications with the OCSP server:

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsdp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsdp none
Router(ca-trustpoint)# ocsdp disable-nonce
```

Configuring a Hub Router at a Central Site for Certificate Revocation Checks: Example

The following example shows a hub router at a central site that is providing connectivity for several branch offices to the central site.

The branch offices are also able to communicate directly with each other using additional IPsec tunnels between the branch offices.

The CA publishes CRLs on an HTTP server at the central site. The central site checks CRLs for each peer when setting up an IPsec tunnel with that peer.

The example does not show the IPsec configuration—only the PKI-related configuration is shown.

Home Office Hub Configuration

```
crypto pki trustpoint VPN-GW
enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
serial-number none
fqdn none
ip-address none
subject-name o=Home Office Inc,cn=Central VPN Gateway
revocation-check crl
```

Central Site Hub Router

```
Router# show crypto ca certificate
```

```
Certificate
  Status: Available
  Certificate Serial Number: 2F62BE1400000000CA0
  Certificate Usage: General Purpose
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    Name: Central VPN Gateway
    cn=Central VPN Gateway
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 00:43:26 GMT Sep 26 2003
    end date: 00:53:26 GMT Sep 26 2004
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: VPN-GW
```

```

CA Certificate
  Status: Available
  Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
  Certificate Usage: Signature
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    cn=Central Certificate Authority
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 22:19:29 GMT Oct 31 2002
    end   date: 22:27:27 GMT Oct 31 2017
  Associated Trustpoints: VPN-GW

```

Trustpoint on the Branch Office Router

```

crypto pki trustpoint home-office
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none

ip-address none
subject-name o=Home Office Inc,cn=Branch 1
revocation-check crl

```

A certificate map is entered on the branch office router.

Router# configure terminal

```

Enter configuration commands, one per line.  End with CNTL/Z.
branch1(config)# crypto pki certificate map central-site 10
branch1(ca-certificate-map)#

```

The output from the **show certificate** command on the central site hub router shows that the certificate was issued by the following:

```

cn=Central Certificate Authority
o=Home Office Inc

```

These two lines are combined into one line using a comma (,) to separate them, and the original lines are added as the first criteria for a match.

```

Router (ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home Office Inc

```

!The above line wrapped but should be shown on one line with the line above it.

The same combination is done for the subject name from the certificate on the central site router (note that the line that begins with "Name:" is not part of the subject name and must be ignored when creating the certificate map criteria). This is the subject name to be used in the certificate map.

```

cn=Central VPN Gateway
o=Home Office Inc

```

```

Router (ca-certificate-map)# subject-name eq cn=central vpn gateway, o=home office inc

```

Now the certificate map is added to the trustpoint that was configured earlier.

```

Router (ca-certificate-map)# crypto pki trustpoint home-office
Router (ca-trustpoint)# match certificate central-site skip revocation-check
Router (ca-trustpoint)# exit
Router (config)# exit

```

The configuration is checked (most of configuration is not shown).

```
Router# write term
!Many lines left out
.
.
.
crypto pki trustpoint home-office
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Branch 1
  revocation-check crl
  match certificate central-site skip revocation-check
!
!
crypto pki certificate map central-site 10
  issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
  subject-name eq cn = central vpn gateway, o = home office inc
!many lines left out
```

Note that the issuer-name and subject-name lines have been reformatted to make them consistent for later matching with the certificate of the peer.

If the branch office is checking the AAA, the trustpoint will have lines similar to the following:

```
crypto pki trustpoint home-office
  auth list allow_list
  auth user subj commonname
```

After the certificate map has been defined as was done above, the following command is added to the trustpoint to skip AAA checking for the central site hub.

```
match certificate central-site skip authorization-check
```

In both cases, the branch site router has to establish an IPSec tunnel to the central site to check CRLs or to contact the AAA server. However, without the **match certificate** command and **central-site skip authorization-check (argument and keyword)**, the branch office cannot establish the tunnel until it has checked the CRL or the AAA server. (The tunnel will not be established unless the **match certificate** command and **central-site skip authorization-check** argument and keyword are used.)

The **match certificate** command and **allow expired-certificate** keyword would be used at the central site if the router at a branch site had an expired certificate and it had to establish a tunnel to the central site to renew its certificate.

Trustpoint on the Central Site Router

```
crypto pki trustpoint VPN-GW
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Central VPN Gateway
  revocation-check crl
```

Trustpoint on the Branch 1 Site Router

```
Router# show crypto ca certificate
```

```
Certificate
  Status: Available
  Certificate Serial Number: 2F62BE1400000000CA0
```



```

Certificate Usage: General Purpose
Issuer:
  cn=Central Certificate Authority
  o=Home Office Inc
Subject:
  Name: Branch 1 Site
  cn=Branch 1 Site
  o=Home Office Inc
CRL Distribution Points:
  http://ca.home-office.com/CertEnroll/home-office.crl
Validity Date:
  start date: 00:43:26 GMT Sep 26 2003
  end   date: 00:53:26 GMT Oct 3 2003
  renew date: 00:00:00 GMT Jan 1 1970
Associated Trustpoints: home-office
CA Certificate
Status: Available
Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
Certificate Usage: Signature
Issuer:
  cn=Central Certificate Authority
  o=Home Office Inc
Subject:
  cn=Central Certificate Authority
  o=Home Office Inc
CRL Distribution Points:
  http://ca.home-office.com/CertEnroll/home-office.crl
Validity Date:
  start date: 22:19:29 GMT Oct 31 2002
  end   date: 22:27:27 GMT Oct 31 2017
Associated Trustpoints: home-office

```

A certificate map is entered on the central site router.

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)# crypto pki certificate map branch1 10
Router (ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home Office Inc
!The above line wrapped but should be part of the line above it.
Router (ca-certificate-map)# subject-name eq cn=Branch 1 Site,o=home office inc

```

The certificate map is added to the trustpoint.

```

Router (ca-certificate-map)# crypto pki trustpoint VPN-GW
Router (ca-trustpoint)# match certificate branch1 allow expired-certificate
Router (ca-trustpoint)# exit
Router (config) #exit

```

The configuration should be checked (most of the configuration is not shown).

```

Router# write term

!many lines left out

crypto pki trustpoint VPN-GW
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Central VPN Gateway
  revocation-check crl
  match certificate branch1 allow expired-certificate
!
!

```

```
crypto pki certificate map central-site 10
  issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
  subject-name eq cn = central vpn gateway, o = home office inc
! many lines left out
```

The **match certificate** command and **branch1 allow expired-certificate** (argument and keyword) and the certificate map should be removed as soon as the branch router has a new certificate.

Configuring Certificate Authorization and Revocation Settings: Examples

This section contains the following configuration examples that can be used when specifying a CRL cache control setting or certificate serial number session control:

- [Configuring CRL Cache Control, page 36](#)
- [Configuring Certificate Serial Number Session Control, page 37](#)

Configuring CRL Cache Control

The following example shows how to disable CRL caching for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
  enrollment url http://CA1:80
  ip-address FastEthernet0/0
  crl query ldap://ldap_CA1
  revocation-check crl
  crl-cache none
```

The current CRL is still cached immediately after executing the example configuration shown above:

```
Router# show crypto pki crls
CRL Issuer Name:
  cn=name Cert Manager,ou=pki,o=company.com,c=US
  LastUpdate: 18:57:42 GMT Nov 26 2005
  NextUpdate: 22:57:42 GMT Nov 26 2005
  Retrieved from CRL Distribution Point:
    ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

When the current CRL expires, a new CRL is then downloaded to the router at the next update. The **crl-cache none** command takes effect and all CRLs for the trustpoint are no longer cached; caching is disabled. You can verify that no CRL is cached by executing the **show crypto pki crls** command. No output will be shown because there are no CRLs cached.

The following example shows how to configure the maximum lifetime of 2 minutes for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
  enrollment url http://CA1:80
  ip-address FastEthernet0/0
  crl query ldap://ldap_CA1
  revocation-check crl
  crl-cache delete-after 2
```

The current CRL is still cached immediately after executing the example configuration above for setting the maximum lifetime of a CRL:

```
Router# show crypto pki crls
CRL Issuer Name:
  cn=name Cert Manager,ou=pki,o=company.com,c=US
```

```
LastUpdate: 18:57:42 GMT Nov 26 2005
NextUpdate: 22:57:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point:
  ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

When the current CRL expires, a new CRL is downloaded to the router at the next update and the **crl-cache delete-after** command takes effect. This newly cached CRL and all subsequent CRLs will be deleted after a maximum lifetime of 2 minutes.

You can verify that the CRL will be cached for 2 minutes by executing the **show crypto pki crls** command. Note that the NextUpdate time is 2 minutes after the LastUpdate time.

```
Router# show crypto pki crls

CRL Issuer Name:
  cn=name Cert Manager,ou=pki,o=company.com,c=US
  LastUpdate: 22:57:42 GMT Nov 26 2005

NextUpdate: 22:59:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point:
  ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

Configuring Certificate Serial Number Session Control

The following example shows the configuration of certificate serial number session control using a certificate map for the CA1 trustpoint:

```
crypto pki trustpoint CA1
  enrollment url http://CA1
  chain-validation stop
  crl query ldap://ldap_server
  revocation-check crl
  match certificate crl
!
crypto pki certificate map crl 10
  serial-number co 279d
```



Note

If the *match-criteria* value is set to **eq** (equal) instead of **co** (contains), the serial number must match the certificate map serial number *exactly*, including any spaces.

The following example shows the configuration of certificate serial number session control using AAA attributes. In this case, all valid certificates will be accepted if the certificate does not have the serial number “4ACA.”

```
crypto pki trustpoint CA1
  enrollment url http://CA1
  ip-address FastEthernet0/0
  crl query ldap://ldap_CA1
  revocation-check crl
  aaa new-model
!
aaa attribute list crl
attribute-type aaa-cert-serial-not 4ACA
```

The server log shows that the certificate with the serial number “4ACA” was rejected. The certificate rejection is shown in bold.

```
.
.
.
```

```

Dec 3 04:24:39.051: CRYPTO_PKI: Trust-Point CA1 picked up
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.051: CRYPTO_PKI: unlocked trustpoint CA1, refcount is 0
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.135: CRYPTO_PKI: validation path has 1 certs
Dec 3 04:24:39.135: CRYPTO_PKI: Found a issuer match
Dec 3 04:24:39.135: CRYPTO_PKI: Using CA1 to validate certificate
Dec 3 04:24:39.135: CRYPTO_PKI: Certificate validated without revocation check
Dec 3 04:24:39.135: CRYPTO_PKI: Selected AAA username: 'PKIAAA'
Dec 3 04:24:39.135: CRYPTO_PKI: Anticipate checking AAA list:'CRL'
Dec 3 04:24:39.135: CRYPTO_PKI_AAA: checking AAA authorization (CRL, PKIAAA-L1, <all>)
Dec 3 04:24:39.135: CRYPTO_PKI_AAA: pre-authorization chain validation status (0x4)
Dec 3 04:24:39.135: AAA/BIND(00000021): Bind i/f
Dec 3 04:24:39.135: AAA/AUTHOR (0x21): Pick method list 'CRL'
.
.
.

Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-serial-not" = "4ACA")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: cert-serial doesn't match ("4ACA" != "4ACA")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: post-authorization chain validation status (0x7)
Dec 3 04:24:39.175: CRYPTO_PKI: AAA authorization for list 'CRL', and user 'PKIAAA'
failed.
Dec 3 04:24:39.175: CRYPTO_PKI: chain cert was anchored to trustpoint CA1, and chain
validation result was: CRYPTO_PKI_CERT_NOT_AUTHORIZED
Dec 3 04:24:39.175: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.43 is
bad: certificate invalid
Dec 3 04:24:39.175: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed with peer
at 192.0.2.43
.
.
.

```

Configuring Certificate Chain Validation: Examples

This section contains the following configuration examples that can be used to specify the level of certificate chain processing for your device certificates:

- [Configuring Certificate Chain Validation from Peer to Root CA, page 38](#)
- [Configuring Certificate Chain Validation from Peer to Subordinate CA, page 39](#)
- [Configuring Certificate Chain Validation Through a Gap, page 39](#)

Configuring Certificate Chain Validation from Peer to Root CA

In the following configuration example, all of the certificates will be validated—the peer, SubCA11, SubCA1, and RootCA certificates.

```

crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
  rsakeypair RootCA

crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none

```

```
rsa keypair SubCA1

crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue SubCA1
  revocation-check none
  rsa keypair SubCA11
```

Configuring Certificate Chain Validation from Peer to Subordinate CA

In the following configuration example, the following certificates will be validated—the peer and SubCA1 certificates.

```
crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
  rsa keypair RootCA

crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
  rsa keypair SubCA1

crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue SubCA1
  revocation-check none
  rsa keypair SubCA11
```

Configuring Certificate Chain Validation Through a Gap

In the following configuration example, SubCA1 is not in the configured Cisco IOS hierarchy but is expected to have been supplied in the certificate chain presented by the peer.

If the peer supplies the SubCA1 certificate in the presented certificate chain, the following certificates will be validated—the peer, SubCA11, and SubCA1 certificates.

If the peer does not supply the SubCA1 certificate in the presented certificate chain, the chain validation will fail.

```
crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
  rsa keypair RootCA

crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
  rsa keypair SubCA11
```

Additional References

The following sections provide references related to PKI certificate authorization and revocation.

Related Documents

Related Topic	Document Title
PKI commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Security Command Reference
Overview of PKI, including RSA keys, certificate enrollment, and CAs	“Cisco IOS PKI Overview: Understanding and Planning a PKI” module
RSA key generation and deployment	“Deploying RSA Keys Within a PKI” module
Certificate enrollment: supported methods, enrollment profiles, configuration tasks	“Configuring Certificate Enrollment for a PKI” module
Cisco IOS certificate server overview information and configuration tasks	“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” module

Technical Assistance

Description	Link
The Cisco Technical Support Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Certificate Authorization and Revocation

[Table 2](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation. For information on a feature in this technology that is not documented here, see the Implementing and Managing PKI Features Roadmap.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

[Table 2](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 **Feature Information for PKI Certificate Authorization and Revocation**

Feature Name	Software Releases	Feature Configuration Information
Cache Control Enhancements for Certification Revocation Lists	12.4(9)T	<p>This feature provides users the ability to disable CRL caching or to specify the maximum lifetime for which a CRL will be cached in router memory. It also provides functionality to configure certificate serial number session control.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • What Is a CRL? • Configuring Certificate Authorization and Revocation Settings • Configuring Certificate Authorization and Revocation Settings: Examples <p>The following commands were introduced or modified by this feature: crl-cache delete-after, crl-cache none, crypto pki certificate map</p>
Certificate-Complete Chain Validation	12.4(6)T	<p>This feature provides users the ability to configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • PKI Certificate Chain Validation • Configuring Certificate Chain Validation • Configuring Certificate Chain Validation: Examples <p>The following command was introduced by this feature: chain-validation</p>
OCSP - Server Certification from Alternate Hierarchy	12.4(6)T	<p>This feature provides users with the flexibility to specify multiple OCSP servers, either per client certificate or per group of client certificates, and provides the capability for OCSP server validation based on external CA certificates or self-signed certificates.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • What Is OCSP? • Configuring Certificate Authorization and Revocation Settings <p>The following command was introduced by this feature: match certificate override ocsp</p>

Table 2 *Feature Information for PKI Certificate Authorization and Revocation (continued)*

Feature Name	Software Releases	Feature Configuration Information
Optional OCSP Nonce	12.2(33)SR 12.4(4)T	<p>This feature provides users with the ability to configure the sending of a nonce, or unique identifier for an OCSP request, during OCSP communications.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • What Is OCSP? • Configuring a Revocation Mechanism for PKI Certificate Status Checking • Disabling Nonces in Communications with the OCSP Server: Example
Certificate Security Attribute-Based Access Control	12.2(15)T	<p>Under the IPsec protocol, CA interoperability permits Cisco IOS devices and a CA to communicate so that the Cisco IOS device can obtain and use digital certificates from the CA. Certificates contain several fields that are used to determine whether a device or user is authorized to perform a specified action. This feature adds fields to the certificate that allow specifying an ACL, creating a certificate-based ACL.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • When to Use Certificate-Based ACLs for Authorization or Revocation • Configuring Certificate Authorization and Revocation Settings <p>The following commands were introduced or modified by this feature: crypto pki certificate map, crypto pki trustpoint, match certificate</p>
Online Certificate Status Protocol (OCSP)	12.3(2)T	<p>This feature allows users to enable OCSP instead of CRLs to check certificate status. Unlike CRLs, which provide only periodic certificate status, OCSP can provide timely information regarding the status of a certificate.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • CRLs or OCSP Server: Choosing a Certificate Revocation Mechanism • Configuring a Revocation Mechanism for PKI Certificate Status Checking <p>The following commands were introduced by this feature: ocsp url, revocation-check</p>

Table 2 **Feature Information for PKI Certificate Authorization and Revocation (continued)**

Feature Name	Software Releases	Feature Configuration Information
PKI AAA Authorization Using the Entire Subject Name	12.3(11)T	<p>This feature provides users with the ability to query the AAA server using the entire subject name from the certificate as a unique AAA username.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Attribute-Value Pairs for PKI and AAA Server Integration • Configuring PKI Integration with a AAA Server <p>The following command was modified by this feature: authorization username</p>
PKI Integration with AAA Server	12.3(1)	<p>This feature provides additional scalability for authorization by generating a AAA username from the certificate presented by the peer. A AAA server is queried to determine whether the certificate is authorized for use by the internal component. The authorization is indicated by a component-specified label that must be present in the AV pair for the user.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • PKI and AAA Server Integration for Certificate Status • Configuring PKI Integration with a AAA Server <p>The following commands were introduced by this feature: authorization list, authorization username</p>
PKI: Query Multiple Servers During Certificate Revocation Check	12.3(7)T	<p>This feature introduces the ability for Cisco IOS software to make multiple attempts to retrieve the CRL, allowing operations to continue when a particular server is not available. In addition, the ability to override the CDPs in a certificate with a manually configured CDP has been introduced. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for an extended period of time. The certificate's CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Querying All CDPs During Revocation Check • Manually Overriding CDPs in a Certificate <p>The following command was introduced by this feature: match certificate override cdp</p>

Table 2 *Feature Information for PKI Certificate Authorization and Revocation (continued)*

Feature Name	Software Releases	Feature Configuration Information
PKI: Query Multiple Servers During Certificate Revocation Check	12.3(7)T	<p>This feature introduces the ability for Cisco IOS software to make multiple attempts to retrieve the CRL, allowing operations to continue when a particular server is not available. In addition, the ability to override the CDPs in a certificate with a manually configured CDP has been introduced. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for an extended period of time. The certificate's CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Querying All CDPs During Revocation Check Manually Overriding CDPs in a Certificate <p>The following command was introduced by this feature: match certificate override cdp</p>
Using Certificate ACLs to Ignore Revocation Check and Expired Certificates	12.3(4)T	<p>This feature allows a certificate that meets specified criteria to be accepted regardless of the validity period of the certificate, or if the certificate meets the specified criteria, revocation checking does not have to be performed. Certificate ACLs are used to specify the criteria that the certificate must meet to be accepted or to avoid revocation checking. In addition, if AAA communication is protected by a certificate, this feature provides for the AAA checking of the certificate to be ignored.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Ignore Revocation Checks Using a Certificate-Based ACL Configuring Certificate-Based ACLs to Ignore Revocation Checks <p>The following command was modified by this feature: match certificate</p>
Certificate - Security Attribute-Based Access Control	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
OCSP (Online Certificate Status Protocol)	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Optional OCSP Nonce	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Table 2 **Feature Information for PKI Certificate Authorization and Revocation (continued)**

Feature Name	Software Releases	Feature Configuration Information
PKI AAA Authorization Using the Entire Subject Name	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
PKI Integration with AAA Server	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Query Mode Definition Per Trustpoint	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Query Multiple Servers during Certificate Revocation Check	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.



Configuring Certificate Enrollment for a PKI

First Published: May 2, 2005

Last Updated: August 21, 2007

Certificate enrollment, which is the process of obtaining a certificate from a certification authority (CA), occurs between the end host that requests the certificate and the CA. Each peer that participates in the public key infrastructure (PKI) must enroll with a CA. This module describes the different methods available for certificate enrollment and how to set up each method for a participating PKI peer.

Finding Feature Information in This Module

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for PKI Certificate Enrollment”](#) section on page 32.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Catalyst OS, and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for PKI Certificate Enrollment](#), page 2
- [Information About Certificate Enrollment for a PKI](#), page 2
- [How to Configure Certificate Enrollment for a PKI](#), page 6
- [Configuration Examples for PKI Certificate Enrollment Requests](#), page 24
- [Additional References](#), page 30
- [Feature Information for PKI Certificate Enrollment](#), page 32



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for PKI Certificate Enrollment

Before configuring peers for certificate enrollment, you should have the following items:

- A generated Rivest, Shamir, and Adelman (RSA) key pair to enroll and a PKI in which to enroll.
- Your CA should be authenticated.
- Familiarity with the module “Cisco IOS PKI Overview: Understanding and Planning a PKI.”

**Note**

As of Cisco IOS Release 12.3(7)T, all commands that begin with “**crypto ca**” have been changed to begin with “**crypto pki**.” Although the router will still accept **crypto ca** commands, all output will be read back as **crypto pki**.

Information About Certificate Enrollment for a PKI

Before configuring peers to request a certificate and enroll in the PKI, you should understand the following concepts:

- [What Are CAs?, page 2](#)
- [Authentication of the CA, page 3](#)
- [Supported Certificate Enrollment Methods, page 3](#)
- [Registration Authorities \(RA\), page 4](#)
- [Automatic Certificate Enrollment, page 4](#)
- [Certificate Enrollment Profiles, page 5](#)

What Are CAs?

A CA manages certificate requests and issues certificates to participating network devices. These services (managing certificate requests and issuing certificates) provide centralized key management for the participating devices to validate identities and to create digital certificates. Before any PKI operations can begin, the CA generates its own public key pair and creates a self-signed CA certificate; thereafter, the CA can sign certificate requests and begin peer enrollment for the PKI.

You can use the Cisco IOS certificate server or a CA provided by a third-party CA vendor.

Hierarchical PKI: Multiple CAs

A PKI can be set up in a hierarchical framework to support multiple CAs. At the top of the hierarchy is a root CA, which holds a self-signed certificate. The trust within the entire hierarchy is derived from the RSA key pair of the root CA. The subordinate CAs within the hierarchy can be enrolled with either the root CA or with another subordinate CA. Multiple tiers of CAs are configured by either the root CA or with another subordinate CA. Within a hierarchical PKI, all enrolled peers, can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA.

When to Use Multiple CAs

Multiple CAs provide users with added flexibility and reliability. For example, subordinate CAs can be placed in branch offices while the root CA is at the office headquarters. Also, different granting policies can be implemented per CA, so you can set up one CA to automatically grant certificate requests while another CA within the hierarchy requires each certificate request to be manually granted.

Scenarios in which at least a two-tier CA is recommended are as follows:

- Large and very active networks in which a large number of certificates are revoked and reissued. A multiple tier CA helps to control the size of the certificate revocation lists (CRLs).
- When online enrollment protocols are used, the root CA can be kept offline except to issue subordinate CA certificates. This scenario provides added security for the root CA.

Authentication of the CA

The certificate of the CA must be authenticated before the device will be issued its own certificate and before certificate enrollment can occur. Authentication of the CA typically occurs only when you initially configure PKI support at your router. To authenticate the CA, issue the **crypto pki authenticate** command, which authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA.

Authentication via the fingerprint Command

After Cisco IOS Release 12.3(12), you can issue the **fingerprint** command to preenter a fingerprint that can be matched against the fingerprint of a CA certificate during authentication.

If a fingerprint is not preentered for a trustpoint, and if the authentication request is interactive, you must verify the fingerprint that is displayed during authentication of the CA certificate. If the authentication request is noninteractive, the certificate will be rejected without a preentered fingerprint.



Note

If the authentication request is made using the command-line interface (CLI), the request is an interactive request. If the authentication request is made using HTTP or another management tool, the request is a noninteractive request.

Supported Certificate Enrollment Methods

Cisco IOS software supports the following methods to obtain a certificate from a CA:

- Simple Certificate Enrollment Protocol (SCEP)—A Cisco developed enrollment protocol that uses HTTP to communicate with the CA or registration authority (RA). SCEP is the most commonly used method for sending and receiving requests and certificates.



Note

To take advantage of automated certificate and key rollover functionality, you must be running a CA that supports rollover and SCEP must be used as your client enrollment method.

If you are running a Cisco IOS CA, you must be running Cisco IOS Release 12.4(2)T or a later release for rollover support.

- PKCS12—The router imports certificates in PKCS12 format from an external server.
- IOS File System (IFS)—The router uses any file system that is supported by Cisco IOS software (such as TFTP, FTP, flash, and NVRAM) to send a certificate request and to receive the issued certificate. Users may enable IFS certificate enrollment when their CA does not support SCEP.



Note Prior to Cisco IOS Release 12.3(4)T, only the TFTP file system is supported within IFS.

- Manual cut-and-paste—The router displays the certificate request on the console terminal, allowing the user to enter the issued certificate on the console terminal. A user may manually cut-and-paste certificate requests and certificates when there is no network connection between the router and CA.
- Enrollment profiles—The router sends HTTP-based enrollment requests directly to the CA server instead of to the RA-mode CS. Enrollment profiles can be used if a CA server does not support SCEP.
- Self-signed certificate enrollment for a trustpoint—The secure HTTP (HTTPS) server generates a self-signed certificate that is to be used during the secure socket layer (SSL) handshake, establishing a secure connection between the HTTPS server and the client. The self-signed certificate is then saved in the router's startup configuration (NVRAM). The saved, self-signed certificate can then be used for future SSL handshakes, eliminating the user intervention that was necessary to accept the certificate every time the router reloaded.



Note

To take advantage of autoenrollment and auto reenrollment, do not use either TFTP or manual cut-and-paste enrollment as your enrollment method. Both TFTP and manual cut-and-paste enrollment methods are manual enrollment processes, requiring user input.

Registration Authorities (RA)

A Cisco IOS certificate server can be configured to run in RA mode. An RA offloads authentication and authorization responsibilities from a CA. When the RA receives a SCEP or manual enrollment request, the administrator can either reject or grant it on the basis of local policy. If the request is granted, it will be forwarded to the issuing CA, and the CA can be configured to automatically generate the certificate and return it to the RA. The client can later retrieve the granted certificate from the RA.

Automatic Certificate Enrollment

Certificate autoenrollment allows the CA client to automatically request a certificate from its CA sever. This automatic router request eliminates the need for operator intervention when the enrollment request is sent to the CA server. Automatic enrollment is performed on startup for any trustpoint CA that is configured and that does not have a valid client certificate. When the certificate expires, a new certificate is automatically requested.



Note

When automatic enrollment is configured, clients automatically request client certificates. The CA server performs its own authorization checks; if these checks include a policy to automatically issue certificates, all clients will automatically receive certificates, which is not very secure. Thus, automatic certificate enrollment should be combined with additional authentication and authorization mechanisms (such as Secure Device Provisioning (SDP), leveraging existing certificates, and one-time passwords).

Automated Client Certificate and Key Rollover

By default, the automatic certificate enrollment function requests a new client certificate and keys from the CS before the client's current certificate expires. Certificate and key rollover allows the certificate renewal rollover request to be made before the certificate expires by retaining the current key and certificate until the new, or rollover, certificate is available. After a specified amount of time, the rollover certificate and keys will become the active certificate and keys. The expired certificate and keys are immediately deleted upon rollover and removed from the certificate chain and CRL.

The setup for automatic rollover is twofold: CA clients must be automatically enrolled and the client's CAs must be automatically enrolled and have the **auto-rollover** command enabled. For more information on configuring your CA servers for automatic certificate rollover see the section "Automatic CA Certificate and Key Rollover" in the chapter "[Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment](#)."

An optional renewal percentage parameter can be used with the **auto-enroll** command to allow a new certificate to be requested when a specified percentage of the lifetime of the certificate has passed. For example, if the renewal percentage is configured as 90 and the certificate has a lifetime of one year, a new certificate is requested 36.5 days before the old certificate expires. In order for automatic rollover to occur, the renewal percentage must be less than 100. The specified percent value must not be less than 10. If a client certificate is issued for less than the configured validity period due to the impending expiration of the CA certificate, the rollover certificate will be issued for the balance of that period. A minimum of 10 percent of the configured validity period, with an absolute minimum of 3 minutes, is required to allow rollover enough time to function.



Tip

If CA autoenrollment is not enabled, you may manually initiate rollover on an existing client with the **crypto pki enroll** command if the expiration time of the current client certificate is equal to or greater than the expiration time of the corresponding CA certificate.

The client will initiate the rollover process, which only occurs if the server is configured for automated rollover and has an available rollover server certificate.



Note

A key pair is also sent if configured by the **auto-enroll re-generate** command and keyword. It is recommended that a new key pair be issued for security reasons.

Certificate Enrollment Profiles

Enrollment profiles allow users to specify certificate authentication, enrollment, and reenrollment parameters when prompted. The values for these parameters are referenced by two templates that make up the profile. One template contains parameters for the HTTP request that is sent to the CA server to obtain the certificate of the CA (also known as certificate authentication); the other template contains parameters for the HTTP request that is sent to the CA for certificate enrollment.

Configuring two templates enables users to specify different URLs or methods for certificate authentication and enrollment; for example, authentication (getting the certificate of the CA) can be performed via TFTP (using the **authentication url** command) while enrollment can be performed manually (using the **enrollment terminal** command).

Prior to Cisco IOS Release 12.3(11)T, certificate requests could be sent only in a PKCS10 format; however, an additional parameter has now been added to the profile, allowing users to specify the PKCS7 format for certificate renewal requests.

**Note**

A single enrollment profile can have up to three separate sections for each task—certificate authentication, enrollment, and reenrollment.

How to Configure Certificate Enrollment for a PKI

This section contains the following enrollment option procedures. If you configure enrollment or autoenrollment (the first task), you cannot configure manual certificate enrollment. Also, if you configure TFTP or manual cut-and-paste certificate enrollment, you cannot configure autoenrollment, auto reenrollment, an enrollment profile, nor can you utilize the automated CA certificate rollover capability.

- [Configuring Certificate Enrollment or Autoenrollment, page 6](#)
- [Configuring Manual Certificate Enrollment, page 11](#)
- [Configuring a Persistent Self-Signed Certificate for Enrollment via SSL, page 16](#)
- [Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment, page 20](#)

Configuring Certificate Enrollment or Autoenrollment

Perform this task to configure certificate enrollment for clients participating in your PKI.

Prerequisites for Autoenrollment

Before configuring automatic certificate enrollment requests, you should ensure that all necessary enrollment information is configured.

Prerequisites for Enabling Automated Client Certificate and Key Rollover

CA client support for certificate rollover is automatically enabled when using autoenrollment. For automatic CA certificate rollover to run successfully, the following prerequisites are applicable:

- Your network devices must support shadow PKI.
- Your clients must be running Cisco IOS Release 12.4(2)T or a later release.
- The client's CS must support automatic rollover. See the section “Automatic CA Certificate and Key Rollover” in the chapter “[Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment](#)” for more information on CA server automatic rollover configuration.

Prerequisites for Specifying Autoenrollment Initial Key Generation Location

To specify the location of the autoenrollment initial key generation, you must be running Cisco IOS Release 12.4(11)T or a later release.

Restrictions for Autoenrollment

RSA Key Pair Restriction for Autoenrollment

Trustpoints configured to generate a new key pair using the **regenerate** command or the **regenerate** keyword of the **auto-enroll** command must not share key pairs with other trustpoints. To give each trustpoint its own key pair, use the **rsakeypair** command in ca-trustpoint configuration mode. Sharing key pairs among regenerating trustpoints is not supported and will cause loss of service on some of the trustpoints because of key and certificate mismatches.

Restrictions for Automated Client Certificate and Key Rollover

In order for clients to run automatic CA certificate rollover successfully, the following restrictions are applicable:

- SCEP must be used to support rollover. Any device that enrolls with the PKI using an alternative to SCEP as the certificate management protocol or mechanism (such as enrollment profiles, manual enrollment, or TFTP enrollment) will not be able to take advantage of the rollover functionality provided by SCEP.
- If the configuration cannot be saved to the startup configuration after a shadow certificate is generated, rollover will not occur.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]
5. **subject-name** [*x.500-name*]
6. **ip address** {*ip address* | *interface* | **none**}
7. **serial-number** [**none**]
8. **auto-enroll** [*percent*] [**regenerate**]
9. **usage** *method1* [*method2* [*method3*]]
10. **password** *string*
11. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
12. **fingerprint** *ca-fingerprint*
13. **on** *devicename*:
14. **exit**
15. **crypto pki authenticate** *name*
16. **exit**
17. **copy system:running-config nvram:startup-config**
18. **show crypto pki certificates**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint name Example: Router(config)# crypto pki trustpoint mytp	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 4	enrollment [mode] [retry period minutes] [retry count number] url url [pem] Example: Router(ca-trustpoint)# enrollment url http://cat.example.com	Specifies the URL of the CA on which your router should send certificate requests. <ul style="list-style-type: none"> mode—Specifies RA mode if your CA system provides an RA. retry period minutes—Specifies the wait period between certificate request retries. The default is 1 minute between retries. retry count number— Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. (Specify from 1 to 100 retries.) url url—URL of the file system where your router should send certificate requests. For enrollment method options, see the enrollment command in the Cisco IOS Security Command Reference. pem—Adds privacy-enhanced mail (PEM) boundaries to the certificate request. <p>Note An enrollment method other than TFTP or manual cut-and-paste must be configured to support autoenrollment.</p>
Step 5	subject-name [x.500-name] Example: Router(ca-trustpoint)# subject-name cat	(Optional) Specifies the requested subject name that will be used in the certificate request. <ul style="list-style-type: none"> x.500-name—If it is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.
Step 6	ip address {ip address interface none} Example: Router(ca-trustpoint)# ip address 192.168.1.66	(Optional) Includes the IP address of the specified interface in the certificate request. <p>Issue the none keyword if no IP address should be included.</p> <p>Note If this command is enabled, you will not be prompted for an IP address during enrollment for this trustpoint.</p>

	Command or Action	Purpose
Step 7	serial-number [none] Example: Router(ca-trustpoint)# serial-number	(Optional) Specifies the router serial number in the certificate request, unless the none keyword is issued.
Step 8	auto-enroll [<i>percent</i>] [regenerate] Example: Router(ca-trustpoint)# auto-enroll regenerate	<p>(Optional) Enables autoenrollment, allowing the client to automatically request a rollover certificate from the CA. If autoenrollment is not enabled, the client must be manually reenrolled in your PKI upon certificate expiration.</p> <ul style="list-style-type: none"> By default, only the Domain Name System (DNS) name of the router is included in the certificate. Use the <i>percent</i> argument to specify that a new certificate will be requested after the percentage of the lifetime of the current certificate is reached. Use the regenerate keyword to generate a new key for the certificate even if a named key already exists. <p>Note If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable: “! RSA key pair associated with trustpoint is exportable.”</p> <p>Note It is recommended that a new key pair be generated for security reasons.</p>
Step 9	usage <i>method1</i> [<i>method2</i> [<i>method3</i>]] Example: Router(ca-trustpoint)# usage ssl-client	<p>(Optional) Specifies the intended use for the certificate.</p> <p>Available options are ike, ssl-client, and ssl-server; the default is ike.</p>
Step 10	password <i>string</i> Example: Router(ca-trustpoint)# password string1	<p>(Optional) Specifies the revocation password for the certificate. If this command is enabled, you will not be prompted for a password during enrollment for this trustpoint.</p> <p>Note When SCEP is used, this password can be used to authorize the certificate request—often via a one-time password or similar mechanism.</p>
Step 11	rsakeypair <i>key-label</i> [<i>key-size</i> [<i>encryption-key-size</i>]] Example: Router(ca-trustpoint)# rsakeypair cat	<p>(Optional) Specifies which key pair to associate with the certificate.</p> <ul style="list-style-type: none"> A key pair with <i>key-label</i> will be generated during enrollment if it does not already exist or if the auto-enroll regenerate command was issued. Specify the <i>key-size</i> argument for generating the key, and specify the <i>encryption-key-size</i> argument to request separate encryption, signature keys, and certificates. <p>Note If this command is not enabled, the FQDN key pair is used.</p>

	Command or Action	Purpose
Step 12	fingerprint <i>ca-fingerprint</i> Example: Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E	(Optional) Specifies a fingerprint that can be matched against the fingerprint of a CA certificate during authentication. Note If the fingerprint is not provided and authentication of the CA certificate is interactive, the fingerprint will be displayed for verification.
Step 13	on <i>devicename:</i> Example: Router(ca-trustpoint)# on usbtokens0:	(Optional) Specifies that RSA keys will be created on the specified device upon autoenrollment initial key generation. Devices that may be specified include NVRAM, local disks, and USB tokens. USB tokens may be used as cryptographic devices in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication to be performed on the token.
Step 14	exit Example: Router(ca-trustpoint)# exit	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 15	crypto pki authenticate <i>name</i> Example: Router(config)# crypto pki authenticate mytp	Retrieves the CA certificate and authenticates it. <ul style="list-style-type: none"> Check the certificate fingerprint if prompted. Note This command is optional if the CA certificate is already loaded into the configuration.
Step 16	exit Example: Router(config)# exit	Exits global configuration mode.
Step 17	copy system:running-config nvram:startup-config Example: Router# copy system:running-config nvram:startup-config	(Optional) Copies the running configuration to the NVRAM startup configuration. Note Autoenrollment will not update NVRAM if the running configuration has been modified but not written to NVRAM.
Step 18	show crypto pki certificates Example: Router# show crypto pki certificates	(Optional) Displays information about your certificates, including any rollover certificates.

Examples

The following example shows the configuration for the “mytp-A” certificate server and its associated trustpoint, where RSA keys generated by the initial autoenrollment for the trustpoint will be stored on a USB token, “usbtokens0”:

```
crypto pki server mytp-A
  database level complete
  issuer-name CN=company, L=city, C=country
  grant auto
! Specifies that certificate requests will be granted automatically.
```

```
!  
  
crypto pki trustpoint mytp-A  
    revocation-check none  
    rsakeypair myTP-A  
    storage usbtoken0:  
! Specifies that keys will be stored on usbtoken0:.  
    on usbtoken0:  
! Specifies that keys generated on initial auto enroll will be generated on and stored on  
! usbtoken0:
```

Configuring Manual Certificate Enrollment

Manual certificate enrollment can be set up via TFTP or the manual cut-and-paste method. Both options can be used if your CA does not support SCEP or if a network connection between the router and CA is not possible. Perform one of the following tasks to set up manual certificate enrollment:

- [Configuring Cut-and-Paste Certificate Enrollment, page 11](#)
- [Configuring TFTP Certificate Enrollment, page 13](#)

PEM-Formatted Files for Certificate Enrollment Request

Using PEM-formatted files for certificate requests can be helpful for customers who are using terminal or profile-based enrollment to request certificates from their CA server. Customers using PEM-formatted files can directly use existing certificates on their Cisco IOS routers.

Restrictions for Manual Certificate Enrollment

Switching Enrollment URLs When Using SCEP

We do not recommend switching URLs if SCEP is used; that is, if the enrollment URL is “http://myca,” do not change the enrollment URL after getting the CA certificate and before enrolling the certificate. A user can switch between TFTP and manual cut-and-paste

Key Regeneration Restriction

Do not regenerate the keys manually using the **crypto key generate** command; key regeneration will occur when the **crypto pki enroll** command is issued if the **regenerate** keyword is specified.

Configuring Cut-and-Paste Certificate Enrollment

Perform this task to configure manual certificate enrollment via the cut-and-paste method for peers participating in your PKI.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment terminal** [*pem*]
5. **fingerprint** *ca-fingerprint*

6. **exit**
7. **crypto pki authenticate** *name*
8. **crypto pki enroll** *name*
9. **crypto pki import** *name* **certificate**
10. **exit**
11. **show crypto pki certificates**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint <i>name</i> Example: Router(config)# crypto pki trustpoint mytp	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 4	enrollment terminal [pem] Example: Router(ca-trustpoint)# enrollment terminal	Specifies manual cut-and-paste certificate enrollment method. The certificate request will be displayed on the console terminal so that you may manually copied (or cut). <ul style="list-style-type: none">pem—Configures the trustpoint to generate PEM-formatted certificate requests to the console terminal.
Step 5	fingerprint <i>ca-fingerprint</i> Example: Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E	(Optional) Specifies a fingerprint that can be matched against the fingerprint of a CA certificate during authentication. Note If the fingerprint is not provided, it will be displayed for verification.
Step 6	exit Example: Router(config)# exit	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 7	crypto pki authenticate <i>name</i> Example: Router(config)# crypto pki authenticate mytp	Retrieves the CA certificate and authenticates it.

	Command or Action	Purpose
Step 8	crypto pki enroll <i>name</i> Example: Router(config)# crypto pki enroll mytp	Generates certificate request and displays the request for copying and pasting into the certificate server. You are prompted for enrollment information, such as whether to include the router FQDN and IP address in the certificate request. You are also given the choice about displaying the certificate request to the console terminal. The base-64 encoded certificate with or without PEM headers as requested is displayed.
Step 9	crypto pki import <i>name</i> certificate Example: Router(config)# crypto pki import mytp certificate	Imports a certificate manually at the console terminal (pasting). The base-64 encoded certificate is accepted from the console terminal and inserted into the internal certificate database. Note You must enter this command twice if usage keys, a signature key and an encryption key, are used. The first time the command is entered, one of the certificates is pasted into the router. The second time the command is entered, the other certificate is pasted into the router. It does not matter which certificate is pasted first. Note Some CAs ignore the usage key information in the certificate request and issue general purpose usage certificates. If this applies to the certificate authority you are using, import the general purpose certificate. The router will not use one of the two key pairs generated.
Step 10	exit Example: Router(config)# exit	Exits global configuration mode.
Step 11	show crypto pki certificates Example: Router# show crypto pki certificates	(Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.

Configuring TFTP Certificate Enrollment

Perform this task to configure manual certificate enrollment using a TFTP server.

Prerequisites for TFTP Certificate Enrollment

- You must know the correct URL to use if you are configuring certificate enrollment via TFTP.
- The router must be able to write a file to the TFTP server for the **crypto pki enroll** command.
- If using a file specification with the **enrollment** command, the file must contain the CA certificate either in binary format or be base-64 encoded.

- You must know if your CA ignores key usage information in a certificate request and issues only a general purpose usage certificate.

**Caution**

Some TFTP servers require that the file must exist on the server before it can be written.

Most TFTP servers require that the file be “write-able” by the world. This requirement may pose a risk because any router or other device may write or overwrite the certificate request; thus, the replacement certificate request will not be used by the CA administrator, who must first check the enrollment request fingerprint before granting the certificate request.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]
5. **fingerprint** *ca-fingerprint*
6. **exit**
7. **crypto pki authenticate** *name*
8. **crypto pki enroll** *name*
9. **crypto pki import** *name* **certificate**
10. **exit**
11. **show crypto pki certificates**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint name Example: Router(config)# crypto pki trustpoint mytp	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 4	enrollment [mode] [retry period minutes] [retry count number] url url [pem] Example: Router(ca-trustpoint)# enrollment url tftp://certserver/file_specification	Specifies TFTP as the enrollment method to send the enrollment request and to retrieve the CA certificate and router certificate and any optional parameters. Note For TFTP enrollment, the url must be configured as a TFTP url, tftp://example_tftp_url. An optional file specification filename may be included in the TFTP url. If the file specification is not included, the FQDN will be used. If the file specification is included, the router will append the extension “.ca” to the specified file name.
Step 5	fingerprint ca-fingerprint Example: Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E	(Optional) Specifies the fingerprint of the CA certificate received via an out-of-band method from the CA administrator. Note If the fingerprint is not provided, it will be displayed for verification.
Step 6	exit Example: Router(config)# exit	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 7	crypto pki authenticate name Example: Router(config)# crypto pki authenticate mytp	Retrieves the CA certificate and authenticates it from the specified TFTP server.

	Command or Action	Purpose
Step 8	crypto pki enroll <i>name</i> Example: Router(config)# crypto pki enroll mytp	Generates certificate request and writes the request out to the TFTP server. You are prompted for enrollment information, such as whether to include the router FQDN and IP address in the certificate request. You are queried about whether or not to display the certificate request to the console terminal. The filename to be written is appended with the extension “.req”. For usage keys, a signature key and an encryption key, two requests are generated and sent. The usage key request filenames are appended with the extensions “-sign.req” and “-encr.req” respectively.
Step 9	crypto pki import <i>name</i> certificate Example: Router(config)# crypto pki import mytp certificate	Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate. The router will attempt to retrieve the granted certificate via TFTP using the same filename used to send the request, except the extension is changed from “.req” to “.crt”. For usage key certificates, the extensions “-sign.crt” and “-encr.crt” are used. The router will parse the received files, verify the certificates, and insert the certificates into the internal certificate database on the router. Note Some CAs ignore the usage key information in the certificate request and issue general purpose usage certificates. If your CA ignores the usage key information in the certificate request, only import the general purpose certificate. The router will not use one of the two keypairs generated.
Step 10	exit Example: Router(config)# exit	Exits global configuration mode.
Step 11	show crypto pki certificates Example: Router# show crypto pki certificates	(Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.

Configuring a Persistent Self-Signed Certificate for Enrollment via SSL

This section contains the following tasks:

- [Configuring a Trustpoint and Specifying Self-Signed Certificate Parameters, page 17](#)
- [Enabling the HTTPS Server, page 19](#)



Note

These tasks are optional because if you enable the HTTPS server, it generates a self-signed certificate automatically using default values.

Persistent Self-Signed Certificates Overview

The SSL protocol can be used to establish a secure connection between an HTTPS server and a client (web browser). During the SSL handshake, the client expects the SSL server's certificate to be verifiable using a certificate the client already possesses.

If Cisco IOS software does not have a certificate that the HTTPS server can use, the server generates a self-signed certificate by calling a PKI application programming interface (API). When the client receives this self-signed certificate and is unable to verify it, intervention is needed. The client asks you if the certificate should be accepted and saved for future use. If you accept the certificate, the SSL handshake continues.

Future SSL handshakes between the same client and the server use the same certificate. However, if the router is reloaded, the self-signed certificate is lost. The HTTPS server must then create a new self-signed certificate. This new self-signed certificate does not match the previous certificate so you are once again asked to accept it.

Requesting acceptance of the router's certificate each time that the router reloads may present an opportunity for an attacker to substitute an unauthorized certificate when you are being asked to accept the certificate. Persistent self-signed certificates overcome all these limitations by saving a certificate in the router's startup configuration.

Restrictions

You can configure only one trustpoint for a persistent self-signed certificate.



Note

Do not change the IP domain name or the hostname of the router after creating the self-signed certificate. Changing either name triggers the regeneration of the self-signed certificate and overrides the configured trustpoint. WebVPN ties the SSL trustpoint name to the WebVPN gateway configuration. If a new self-signed certificate is triggered, then the new trustpoint name does not match the WebVPN configuration, causing the WebVPN connections to fail.

Configuring a Trustpoint and Specifying Self-Signed Certificate Parameters

Perform the following task to configure a trustpoint and specify self-signed certificate parameters.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment selfsigned**
5. **subject-name** [*x.500-name*]
6. **rsa***keypair* *key-label* [*key-size* [*encryption-key-size*]]
7. **crypto pki enroll** *name*
8. **end**
9. **show crypto pki certificates** [*trustpoint-name* [*verbose*]]
10. **show crypto pki trustpoints** [*status* | *label* [*status*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint name Example: Router(config)# crypto pki trustpoint local	Declares the CA that your router should use and enters ca-trustpoint configuration mode. Note Effective with Cisco IOS Release 12.3(8)T, the crypto pki trustpoint command replaced the crypto ca trustpoint command.
Step 4	enrollment selfsigned Example: Router(ca-trustpoint)# enrollment selfsigned	Specifies self-signed enrollment.
Step 5	subject-name [x.500-name] Example: Router(ca-trustpoint)# subject-name	(Optional) Specifies the requested subject name to be used in the certificate request. <ul style="list-style-type: none"> If the <i>x-500-name</i> argument is not specified, the FQDN, which is the default subject name, is used.
Step 6	rsa keypair key-label [key-size [encryption-key-size]] Example: Router(ca-trustpoint)# rsa keypair examplekeys 1024 1024	(Optional) Specifies which key pair to associate with the certificate. <ul style="list-style-type: none"> The <i>key-label</i> argument will be generated during enrollment if it does not already exist or if the auto-enroll regenerate command was issued. Specify the <i>key-size</i> argument for generating the key, and specify the <i>encryption-key-size</i> argument to request separate encryption, signature keys, and certificates. Note If this command is not enabled, the FQDN key pair is used.
Step 7	crypto pki enroll name Example: Router(ca-trustpoint)# crypto pki enroll local	Tells the router to generate the persistent self-signed certificate.
Step 8	end Example: Router(ca-trustpoint)# end Example: Router(config)# end	(Optional) Exits ca-trustpoint configuration mode and global configuration mode.

	Command or Action	Purpose
Step 9	show crypto pki certificates [<i>trustpoint-name</i>] [<i>verbose</i>]] Example: Router# show crypto pki certificates local verbose	Displays information about your certificate, the certification authority certificate, and any registration authority certificates.
Step 10	show crypto pki trustpoints [<i>status</i> <i>label</i>] [<i>status</i>]] Example: Router# show crypto pki trustpoints status	Displays the trustpoints that are configured in the router.

Enabling the HTTPS Server

Perform the following task to enable the HTTPS server.

Prerequisites

To specify parameters, you must create a trustpoint and configure it. To use default values, delete any existing self-signed trustpoints. Deleting all self-signed trustpoints causes the HTTPS server to generate a persistent self-signed certificate using default values as soon as the server is enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http secure-server**
4. **end**
5. **copy system:running-config nvram: startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip http secure-server Example: Router(config)# ip http secure-server	Enables the secure HTTP web server. Note A key pair (modulus 1024) and a certificate are generated.
Step 4	end Example: Router(config)# end	Exits global configuration mode.
Step 5	copy system:running-config nvram:startup-config Example: Router# copy system:running-config nvram:startup-config	Saves the self-signed certificate and the HTTPS server in enabled mode.

Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment

Perform this task to configure an enrollment profile for certificate enrollment or reenrollment of a router with a Cisco IOS CA that is already enrolled with a third-party vendor CA.

Enable a router that is enrolled with a third-party vendor CA to use its existing certificate to enroll with the Cisco IOS certificate server so the enrollment request is automatically granted. To enable this functionality, you must issue the **enrollment credential** command. Also, you cannot configure manual certificate enrollment.

Prerequisites

Before configuring a certificate enrollment profile for the client router that is already enrolled with a third party vendor CA so that the router can reenroll with a Cisco IOS certificate server, you should have already performed the following tasks at the client router:

- Defined a trustpoint that points to the third-party vendor CA.
- Authenticated and enrolled the client router with the third-party vendor CA.

Restrictions

- To use certificate profiles, your network must have an HTTP interface to the CA.

- If an enrollment profile is specified, an enrollment URL may not be specified in the trustpoint configuration. Although both commands are supported, only one command can be used at a time in a trustpoint.
- Because there is no standard for the HTTP commands used by various CAs, the user is required to enter the command that is appropriate to the CA that is being used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment profile** *label*
5. **exit**
6. **crypto pki profile enrollment** *label*
7. **authentication url** *url*
or
authentication terminal
8. **authentication command**
9. **enrollment url** *url*
or
enrollment terminal
10. **enrollment credential** *label*
11. **enrollment command**
12. **parameter** *number* {**value** *value* | **prompt** *string*}
13. **exit**
14. **show crypto pki certificates**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint name Example: Router(config)# crypto pki trustpoint Entrust	Declares the trustpoint and a given name and enter ca-trustpoint configuration mode.
Step 4	enrollment profile label Example: Router(ca-trustpoint)# enrollment profile E	Specifies that an enrollment profile is to be used for certificate authentication and enrollment.
Step 5	exit Example: Router(ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.
Step 6	crypto pki profile enrollment label Example: Router(config)# crypto pki profile enrollment E	Defines an enrollment profile and enters ca-profile-enroll configuration mode. <ul style="list-style-type: none"> label—Name for the enrollment profile; the enrollment profile name must match the name specified in the enrollment profile command.
Step 7	authentication url url Example: Router(ca-profile-enroll)# authentication url http://entrust:81 or authentication terminal Example: Router(ca-profile-enroll)# authentication terminal	Specifies the URL of the CA server to which to send certificate authentication requests. <ul style="list-style-type: none"> url—URL of the CA server to which your router should send authentication requests. <p>If using HTTP, the URL should read “http://CA_name,” where CA_name is the host DNS name or IP address of the CA.</p> <p>If using TFTP, the URL should read “tftp://certserver/file_specification.” (If the URL does not include a file specification, the FQDN of the router will be used.)</p> <p>Specifies manual cut-and-paste certificate authentication.</p>

	Command or Action	Purpose
Step 8	authentication command Example: Router(ca-profile-enroll)# authentication command	(Optional) Specifies the HTTP command that is sent to the CA for authentication. This command should be used after the authentication url command has been entered.
Step 9	enrollment url url Example: Router(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/clientcgi.exe or enrollment terminal Example: Router(ca-profile-enroll)# enrollment terminal	Specifies the URL of the CA server to which to send certificate enrollment requests via HTTP or TFTP. Specifies manual cut-and-paste certificate enrollment.
Step 10	enrollment credential label Example: Router(ca-profile-enroll)# enrollment credential Entrust	(Optional) Specifies the third-party vendor CA trustpoint that is to be enrolled with the Cisco IOS CA. Note This command cannot be issued if manual certificate enrollment is being used.
Step 11	enrollment command Example: Router(ca-profile-enroll)# enrollment command	(Optional) Specifies the HTTP command that is sent to the CA for enrollment.
Step 12	parameter number {value value prompt string} Example: Router(ca-profile-enroll)# parameter 1 value aaaa-bbbb-cccc	(Optional) Specifies parameters for an enrollment profile. This command can be used multiple times to specify multiple values.
Step 13	exit Example: Router(ca-profile-enroll)# exit Router(config)# exit	Enter this command two times—one time to exit ca-profile-enroll configuration mode and the second time to exit global configuration mode.
Step 14	show crypto pki certificates Example: Router# show crypto pki certificates	(Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.

What to Do Next

If you configured the router to reenroll with a Cisco IOS CA, you should configure the Cisco IOS certificate server to accept enrollment requests only from clients already enrolled with the specified third-party vendor CA trustpoint to take advantage of this functionality. For more information, see the module “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment.”

Configuration Examples for PKI Certificate Enrollment Requests

This section contains the following configuration examples:

- [Configuring Autoenrollment: Example, page 24](#)
- [Configuring Certificate Autoenrollment with Key Regeneration: Example, page 25](#)
- [Configuring Cut-and-Paste Certificate Enrollment: Example, page 25](#)
- [Configuring Manual Certificate Enrollment with Key Regeneration: Example, page 28](#)
- [Creating and Verifying a Persistent Self-Signed Certificate: Example, page 28](#)
- [Configuring Direct HTTP Enrollment: Example, page 30](#)

Configuring Autoenrollment: Example

The following example shows how to configure the router to automatically enroll with a CA on startup, enabling automatic rollover, and how to specify all necessary enrollment information in the configuration:

```
crypto pki trustpoint trustpt1
 enrollment url http://trustpt1.company.com//
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 serial-number none
 usage ike
 auto-enroll regenerate
 password revokeme
 rsa-key trustpt1 2048
!
crypto pki certificate chain trustpt1
certificate pki 0B
30820293 3082023D A0030201 0202010B 300D0609 2A864886 F70D0101 04050030
79310B30 09060355 04061302 5553310B 30090603 55040813 02434131 15301306
0355040A 130C4369 73636F20 53797374 656D3120 301E0603 55040B13 17737562
6F726420 746F206B 6168756C 75692049 50495355 31243022 06035504 03131B79
6E692D75 31302043 65727469 66696361 7465204D 616E6167 6572301E 170D3030
30373134 32303536 32355A17 0D303130 37313430 31323834 335A3032 310E300C
06035504 0A130543 6973636F 3120301E 06092A86 4886F70D 01090216 11706B69
2D343562 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
4B003048 024100B3 0512A201 3B4243E1 378A9703 8AC5E3CE F77AF987 B5A422C4
15E947F6 70997393 70CF34D6 63A86B9C 4347A81A 0551FC02 ABA62360 01EF7DD2
6C136AEB 3C6C3902 03010001 A381F630 81F3300B 0603551D 0F040403 02052030
1C060355 1D110415 30138211 706B692D 3435622E 63697363 6F2E636F 6D301D06
03551D0E 04160414 247D9558 169B9A21 23D289CC 2DDA2A9A 4F77C616 301F0603
551D2304 18301680 14BD742C E892E819 1D551D91 683F6DB2 D8847A6C 73308185
0603551D 1F047E30 7C307AA0 3CA03AA4 38303631 0E300C06 0355040A 13054369
73636F31 24302206 03550403 131B796E 692D7531 30204365 72746966 69636174
65204D61 6E616765 72A23AA4 38303631 0E300C06 0355040A 13054369 73636F31
24302206 03550403 131B796E 692D7531 30204365 72746966 69636174 65204D61
6E616765 72300D06 092A8648 86F70D01 01040500 03410015 BC7CECF9 696697DF
E887007F 7A8DA24F 1ED5A785 C5C60452 47860061 0C18093D 08958A77 5737246B
0A25550A 25910E27 8B8B428E 32F8D948 3DD1784F 954C70
quit
```



Note

In this example, keys are neither regenerated nor rolled over.

Configuring Certificate Autoenrollment with Key Regeneration: Example

The following example shows how to configure the router to automatically enroll with the CA named “trustme1” on startup and enable automatic rollover. The **regenerate** keyword is issued, so a new key will be generated for the certificate and reissued when the automatic rollover process is initiated. The renewal percentage is configured as 90 so if the certificate has a lifetime of one year, a new certificate is requested 36.5 days before the old certificate expires. The changes made to the running configuration are saved to the NVRAM startup configuration because autoenrollment will not update NVRAM if the running configuration has been modified but not written to NVRAM.

```
crypto pki trustpoint trustme1
  enrollment url http://trustme1.company.com/
  subject-name OU=Spiral Dept., O=tiedye.com
  ip-address ethernet0
  serial-number none
  auto-enroll 90 regenerate
  password revokeme
  rsa-keypair trustme1 2048
  exit
crypto pki authenticate trustme1
copy system:running-config nvram:startup-config
```

Configuring Cut-and-Paste Certificate Enrollment: Example

The following example shows how to configure certificate enrollment using the manual cut-and-paste enrollment method:

```
Router(config)# crypto pki trustpoint TP
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# crypto pki authenticate TP
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIICNDCCAd6gAwIBAgIQOsCmXpVHwodKryRoqULV7jANBgkqhkiG9w0BAQUFADA5
MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJ
bXNjYSl1b290MB4XDTAyMDIxNDAwNDYwMVoXDTA3MDIxNDAwNTQ0FowOTELMAkG
A1UEBhMCVVMxMjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
cm9vdDBCA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCix8nIGFg+wvy3BjFbVi25wYoG
K2N0HWWHpgxqFuFhgyBnIC0OshIn9CtdN3JvUNHr0N1KocEwNKUGYmPwWGTfAgMB
AAGjgcEwgb4wCwYDVROPAQDAAGHMA8GA1UdEwEB/wQFMAMBAf8wHQYDVRO0BBYE
FKIacsl6dKAfuNDVQymlSp7esf8jMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9t
c2NhLXJvb3QvQ2VydEVucm9sbC9tc2NhLXJvb3QvY3J5SMDGgG6AthitmaWxloi8v
XFxtc2NhLXJvb3RcQ2VydEVucm9sbC9tc2NhLXJvb3QvY3J5SMBAGCSsGAQQBgjcV
AQQDAgEAMA0GCSqGSIb3DQEBAQUAA0EauZkZMX9qkoLHfETYPVWjZPQbBmwNRA
oJDSdYdtL3BcI/uLL5q7EmODyGfLyMGxuhQYx5r/40aSQgLCqBq+yg==
-----END CERTIFICATE-----
```

Certificate has the following attributes:

Fingerprint: D6C12961 CD78808A 4E02193C 0790082A

% Do you accept this certificate? [yes/no]: **y**

Trustpoint CA certificate accepted.

% Certificate successfully imported

```
Router(config)# crypto pki enroll TP
% Start certificate enrollment..
```

% The subject name in the certificate will be: **Router.company.com**

% Include the router serial number in the subject name? [yes/no]: **n**

```
% Include an IP address in the subject name? [no]: n
Display Certificate Request to terminal? [yes/no]: y
Signature key certificate request -
Certificate Request follows:

MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxdhXFDiWAn/hIZs9zf0tssKA
daoWYu0ms9Fe/Pew01dh14vXdxgacstOs2Pr5wk6jLOPxpvxOJPWyQM6ipLmyVxv
ojhyLTrVohrh6Dngcvk+G/5ohss9o9RxxvONwx042pQchFnx9EkMuZC7evwRxJEQR
mBHXBZ8GmP3jYQsjs8MCaWEAAAhMB8GCSqGSib3DQEJDjESMBaWdGyDVR0PAQH/
BAQDAgeAMA0GCSqGSib3DQEBAUAA4GBAMT6WtyFw95POY7UtF+YIYHiVRUf4SCq
hRIAGrljUePLo9iTqyPU1Pnt8JnIZ5P5BHU3MfgP8sqodaWub6mubkzaohJ1qD06
O87fnLCnid5Tov5jKogFHIki2EGGZxBosUw91JlenQdNdDpbJc5LIWdfDvcia6jO
Nl8rOtKnt8Q+
!
!
!
Redisplay enrollment request? [yes/no]:
Encryption key certificate request -
Certificate Request follows:

MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwG60QoJpDbzbKnyj8FyTiOcv
THkDP7XD4vLT1XaJ409z0gSioGnIcdFtXhV1BWtpq3/09zYFXr1tH+BMCRQi3Lts
0IpxYa3D9iFPgev7SPXpsAIsY8a6FMq7TiWlObqiQjLKL4cbuV0Frj10Yuv5A/Z+
kqMOM7c+pWNWfDL9lsCAwEAAAhMB8GCSqGSib3DQEJDjESMBaWdGyDVR0PAQH/
BAQDAgUgMA0GCSqGSib3DQEBAUAA4GBACF7feURj/fJMoJPBLR6fa9BrlMJx+2F
H91YM/CIiz2n4mHteWTWKhLot8wUfa9NGOk7yi+nF/F7035twLfq6n2bSCTW4aem
8jLMMaeFwxkrV/ceQKrucmNcluVx+fBy9rhnKx8j60XE25tnplU08r6om/pBQABU
eNPFhoczcaQ/2
!
!
!
Redisplay enrollment request? [yes/no]: n
Router(config)# crypto pki import TP certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

MIIDajCCAxSgAwIBAgIKFN7C6QAAAAAMRzANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1y
b290MB4XDTAyMDYwODAxMTY0M1oXDTAzMjY0M1owJTEjMCEGCSqGSib3
DQEJAhMUU2FuZEJhZ2dlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMXYVxQ4lgJ/4SGbPc3zrbLCgHWqFmLrPRXvz3sNNXYdeL13cYgnLL
TrNj6+cJOoyzj8ab8TiT1skDOoqS5slcb6I4ci061aIa4eg56nL5Phv+aIbLPaPU
cbzjcMdonQUHIRZ8fRJDLMQu3r8EcSRKkZgR1wWfBpj942ELI0vDAGMBAAGjggHM
MIIBYDALBgNVHQ8EBAMCB4AwHQYDVR0OBBYEFL8Quz8dyz4EGIEKx9A8UMNHLE4s
MHAGA1UdIwRpmGGeAFKIAcsl6dKAfuNDVQym1Sp7esf8joT2kOzA5MQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yY290
ghA6wKZelUfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFNhbmcYCYWdnZXIuY2l2
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QvY3J5MDGgG6AthitmaWxloI8vXFxtc2NhLXJvb3RcQ2Vy
dEVucm9sbFxtc2NhLXJvb3QvY3J5SMIGUBggrBgEFBQcBAQSBhzbCBhDA/BggrBgEF
BQcwAoYzahr0cDovL2l2Y2Etcm9vdC9DZXJ0RW5yb2xsL2l2Y2Etcm9vdF9tc2Nh
LXJvb3QvY3J0MEEGCCSGAQUFBzAChjVmaWxloI8vXFxtc2NhLXJvb3RcQ2VydeVucm
9sbFxtc2NhLXJvb3RfbXNjYS1yY290LmNydDANBgkqhkiG9w0BAQUFAANBAJo2
r6sHPGBdTQX2EDoJpR/A2UHXxRYqVSHkFKZw0z31r5JzUM0oPNUETV7mnZlYNVRZ
CSEX/G8boi3W0jz9wZo=

% Router Certificate successfully imported

Router(config)# crypto pki import TP cert

Enter the base 64 encoded certificate.
```

End with a blank line or the word "quit" on a line by itself

```
MIIDajCCAxsGAWIBAgIKFN7OBQAAAAAMSDANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1y
b290MB4XDTAyMDYwODAxMTY0NVoxDTAzMDYwODAxMjY0NVowJTEjMCEGCSqGSIb3
DQEJAhMUU2FuZEJhZ2dldci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMButEKI6Q282yp8o/Bck4jnL0x5Az+lw+Ly09V2ieNpc9IEiKBpyHHR
bV4VZQVraat/zvc2BV69bR/gTAKUITy7bNCKcWGtw/YhT6nr+0j16bACLGPgUhtK
u04sCzm6okIyyi+HG7ldBa45dGLr+QP2fpKjDpu3PqVjVhXS3vZbAgMBAAGjggHM
MIIBYDALBgNVHQ8EBAMCBSAwHQYDVR0OBBYEFDO29oRdlEUSgBMg6jZR+YFRWlj
MHAGA1UdIwRPMGeAFKIacs16dKAfuNDVQym1Sp7esf8joT2kOzA5MQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yb290
ghA6wKZelUfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFFNhbmcRCYwdnZXIuY2l2
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QuY3JsMDGgLG6AthitmaWxlOi8vXFxtc2NhLXJvb3RcQ2Vy
dEVucm9sbFxtc2NhLXJvb3QuY3JsMIGUBggrBgEFBQcBAQSBhzCBhDA/BggrBgEF
BQcAwAoYzaHR0cDovL2l2Y2Etc9vdC9DZXJ0RW5yb2xsL2l2Y2Etc9vdF9tc2Nh
LXJvb3QuY3J0MEEGCCsGAQUFBzAChjVmaWxlOi8vXFxtc2NhLXJvb3RcQ2VydeVU
cm9sbFxtc2NhLXJvb3RfbXNjYS1yb290LmNydDANBgkqhkiG9w0BAQUFAANBAHaU
hyCwLirUghNxcmLzXRG7C3W1j0kSX7a4fX9OxKR/Z2SoMjdMNPpyApuh8SoT2zBP
ZKjZU2WjcZG/nZF4W5k=
```

```
% Router Certificate successfully imported
```

You can verify that the certificate was successfully imported by issuing the **show crypto pki certificate** command.

```
Router# show crypto pki certificate
Certificate
  Status: Available
  Certificate Serial Number: 14DECE050000000000C48
  Certificate Usage: Encryption
  Issuer:
    CN = TPCA-root
    O = Company
    C = US
  Subject:
    Name: Router.company.com
    OID.1.2.840.113549.1.9.2 = Router.company.com
  CRL Distribution Point:
    http://tpca-root/CertEnroll/tpca-root.crl
  Validity Date:
    start date: 18:16:45 PDT Jun 7 2002
    end date: 18:26:45 PDT Jun 7 2003
    renew date: 16:00:00 PST Dec 31 1969
  Associated Trustpoints: TP
```

```
Certificate
  Status: Available
  Certificate Serial Number: 14DEC2E90000000000C47
  Certificate Usage: Signature
  Issuer:
    CN = tpca-root
    O = company
    C = US
  Subject:
    Name: Router.company.com
    OID.1.2.840.113549.1.9.2 = Router.company.com
  CRL Distribution Point:
    http://tpca-root/CertEnroll/tpca-root.crl
  Validity Date:
    start date: 18:16:42 PDT Jun 7 2002
    end date: 18:26:42 PDT Jun 7 2003
```

```

    renew date: 16:00:00 PST Dec 31 1969
    Associated Trustpoints: TP

CA Certificate
  Status: Available
  Certificate Serial Number: 3AC0A65E9547C2874AAF2468A942D5EE
  Certificate Usage: Signature
  Issuer:
    CN = tpca-root
    O = Company
    C = US
  Subject:
    CN = tpca-root
    O = company
    C = US
  CRL Distribution Point:
    http://tpca-root/CertEnroll/tpca-root.crl
  Validity Date:
    start date: 16:46:01 PST Feb 13 2002
    end   date: 16:54:48 PST Feb 13 2007
  Associated Trustpoints: TP

```

Configuring Manual Certificate Enrollment with Key Regeneration: Example

The following example shows how to regenerate new keys with a manual certificate enrollment from the CA named “trustme2”:

```

crypto pki trustpoint trustme2
  enrollment url http://trustme2.company.com/
  subject-name OU=Spiral Dept., O=tiedye.com
  ip-address ethernet0
  serial-number none
  regenerate
  password revokeme
  rsakeypair trustme2 2048s
  exit
crypto pki authenticate trustme2
crypto pki enroll trustme2

```

Creating and Verifying a Persistent Self-Signed Certificate: Example

The following example shows how to declare and enroll a trustpoint named “local” and generate a self-signed certificate with an IP address:

```

crypto pki trustpoint local
  enrollment selfsigned
  end
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

crypto pki enroll local
Nov 29 20:51:13.067: %SSH-5-ENABLED: SSH 1.99 has been enabled
Nov 29 20:51:13.267: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: ethernet 0
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created

```


**Note**

A router can have only one self-signed certificate. If you attempt to enroll a trustpoint configured for a self-signed certificate and one already exists, you receive a notification and are asked if you want to replace it. If so, a new self-signed certificate is generated to replace the existing one.

Enabling the HTTPS Server: Example

The following example shows how to enable the HTTPS server and generate a default trustpoint because one was not previously configured:

```
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

ip http secure-server
% Generating 1024 bit RSA keys ...[OK]
*Dec 21 19:14:15.421:%PKI-4-NOAUTOSAVE:Configuration was modified.  Issue "write memory"
to save new certificate
Router(config)#
```

**Note**

You need to save the configuration to NVRAM if you want to keep the self-signed certificate and have the HTTPS server enabled following router reloads.

The following message also appears:

```
*Dec 21 19:14:10.441:%SSH-5-ENABLED:SSH 1.99 has been enabled
```

**Note**

Creation of the key pair used with the self-signed certificate causes the Secure Shell (SSH) server to start. This behavior cannot be suppressed. You may want to modify your access control lists (ACLs) to permit or deny SSH access to the router.

Verifying the Self-Signed Certificate Configuration: Example

The following example displays information about the self-signed certificate that you just created:

```
Router# show crypto pki certificates

Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: General Purpose
  Issuer:
    cn=IOS-Self-Signed-Certificate-3326000105
  Subject:
    Name: IOS-Self-Signed-Certificate-3326000105
    cn=IOS-Self-Signed-Certificate-3326000105
  Validity Date:
    start date: 19:14:14 GMT Dec 21 2004
    end   date: 00:00:00 GMT Jan 1 2020
  Associated Trustpoints: TP-self-signed-3326000105
```

**Note**

The number 3326000105 above is the router's serial number and varies depending on the router's actual serial number.

The following example displays information about the key pair corresponding to the self-signed certificate:

```
Router# show crypto key mypubkey rsa
```

```
% Key pair was generated at: 19:14:10 GMT Dec 21 2004
Key name: TP-self-signed-3326000105
Usage: General Purpose Key
Key is not exportable.
Key Data:
 30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B88F70
 6BC78B6D 67D6CFF3 135C1D91 8F360292 CA44A032 5AC1A8FD 095E4865 F8C95A2B
 BFD1C2B7 E64A3804 9BBD7326 207BD456 19BAB78B D075E78E 00D2560C B09289AE
 6DECB8B0 6672FB3A 5CDAEE92 9D4C4F71 F3BCB269 214F6293 4BA8FABF 9486BCFC
 2B941BCA 550999A7 2EFE12A5 6B7B669A 2D88AB77 39B38E0E AA23CB8C B7020301 0001
% Key pair was generated at: 19:14:13 GMT Dec 21 2004
Key name: TP-self-signed-3326000105.server
Usage: Encryption Key
Key is not exportable.
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00C5680E 89777B42
 463E5783 FE96EA9E F446DC7B 70499AF3 EA266651 56EE29F4 5B003D93 2FC9F81D
 8A46E12F 3FBAC2F3 046ED9DD C5F27C20 1BBA6B9B 08F16E45 C34D6337 F863D605
 34E30F0E B4921BC5 DAC9EBBA 50C54AA0 BF551BDD 88453F50 61020301 0001
```

**Note**

The second key pair with the name TP-self-signed-3326000105.server is the SSH key pair and is generated when any key pair is created on the router and SSH starts up.

The following example displays information about the trustpoint named “local”:

```
Router# show crypto pki trustpoints
```

```
Trustpoint local:
  Subject Name:
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.company.com
    Serial Number: 01
  Persistent self-signed certificate trust point
```

Configuring Direct HTTP Enrollment: Example

The following example show how to configure an enrollment profile for direct HTTP enrollment with a CA server:

```
crypto pki trustpoint Entrust
 enrollment profile E
 serial

crypto pki profile enrollment E
 authentication url http://entrust:81
 authentication command GET /certs/cacert.der
 enrollment url http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command POST reference_number=$P2&authcode=$P1
 &retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Additional References

The following sections provide references related to certificate enrollment for a PKI.

Related Documents

Related Topic	Document Title
USB Token RSA Operations: Benefits of using USB tokens	“ Storing PKI Credentials ” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
USB Token RSA Operations: Certificate server configuration	<p>“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” chapter in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i></p> <p>See the “Generating a Certificate Server RSA Key Pair” section, the “Configuring a Certificate Server Trustpoint” section, and related examples.</p>
Overview of PKI, including RSA keys, certificate enrollment, and CAs	“ Cisco IOS PKI Overview: Understanding and Planning a PKI ” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
Secure Device Provisioning: functionality overview and configuration tasks	“ Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI ” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
RSA key generation and deployment	“ Deploying RSA Keys Within a PKI ” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
Cisco IOS certificate server overview information and configuration tasks	“ Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment ” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
Setting up and using a USB token	“ Storing PKI Credentials ” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for PKI Certificate Enrollment

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Implementing and Managing PKI Features Roadmap](#).”

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, Catalyst OS, and Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 **Feature Information for PKI Certificate Enrollment**

Feature Name	Releases	Feature Information
Cisco IOS USB Token PKI Enhancements—Phase 2	12.4(11)T	<p>This feature enhances USB token functionality by using the USB token as a cryptographic device. USB tokens may be used for RSA operations such as key generation, signing, and authentication.</p> <p>The following sections in this document provide information about this feature:</p> <ul style="list-style-type: none"> • Configuring Certificate Enrollment or Autoenrollment <p>Note This document covers the use of utilizing USB tokens for RSA operations during initial autoenrollment for a trustpoint. For other documents on this topic, see the “Related Documents” section.</p>
Certificate Authority (CA) Key Rollover	12.4(2)T	<p>This feature introduces the ability for root CAs to roll over expiring CA certificates and keys and to have these changes propagate through the PKI network without manual intervention.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Automatic Certificate Enrollment • Configuring Certificate Enrollment or Autoenrollment <p>The following commands were introduced or modified by this feature: auto-rollover, crypto pki certificate chain, crypto pki export pem, crypto pki server, crypto pki server info request, show crypto pki certificates, show crypto pki server, and show crypto pki trustpoint</p>
Certificate Autoenrollment	12.2(8)T Cisco IOS XE Release 2.1	<p>This feature introduces certificate autoenrollment, which allows the router to automatically request a certificate from the CA that is using the parameters in the configuration.</p> <p>In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR series routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Automatic Certificate Enrollment • Configuring Certificate Enrollment or Autoenrollment <p>The following commands were introduced by this feature: auto-enroll, rsakeypair, show crypto ca timers</p>

Table 1 *Feature Information for PKI Certificate Enrollment (continued)*

Feature Name	Releases	Feature Information
Certificate Enrollment Enhancements	12.2(8)T Cisco IOS XE Release 2.1	<p>This feature introduces five new crypto ca trustpoint subcommands that provide new options for certificate requests and allow users to specify fields in the configuration instead of having to go through prompts.</p> <p>In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR series routers.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Configuring Certificate Enrollment or Autoenrollment <p>The following commands were introduced by this feature: ip-address (ca-trustpoint), password (ca-trustpoint), serial-number, subject-name, usage</p>
Direct HTTP Enrollment with CA Servers	12.3(4)T Cisco IOS XE Release 2.1	<p>This feature allows users to configure an enrollment profile if their CA server does not support SCEP and they do not want to use an RA-mode CS. The enrollment profile allows users to send HTTP requests directly to the CA server instead of to an RA-mode CS.</p> <p>In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR series routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Certificate Enrollment Profiles • Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment <p>The following commands were introduced by this feature: authentication command, authentication terminal, authentication url, crypto ca profile enrollment, enrollment command, enrollment profile, enrollment terminal, enrollment url, parameter</p>
Import of RSA Key Pair and Certificates in PEM Format	12.3(4)T	<p>This feature allows customers to issue certificate requests and receive issued certificates in PEM-formatted files.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Configuring Manual Certificate Enrollment <p>The following commands were modified by this feature: enrollment, enrollment terminal</p>

Table 1 *Feature Information for PKI Certificate Enrollment (continued)*

Feature Name	Releases	Feature Information
Key Rollover for Certificate Renewal	12.3(7)T Cisco IOS XE Release 2.1	<p>This feature allows the certificate renewal request to be made before the certificate expires and retains the old key and certificate until the new certificate is available.</p> <p>In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR series routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Automatic Certificate Enrollment • Configuring Certificate Enrollment or Autoenrollment • Configuring Manual Certificate Enrollment <p>The following commands were introduced or modified by this feature: auto-enroll, regenerate</p>
Manual Certificate Enrollment (TFTP Cut-and-Paste)	12.2(13)T Cisco IOS XE Release 2.1	<p>This feature allows users to generate a certificate request and accept CA certificates as well as the router's certificates via a TFTP server or manual cut-and-paste operations.</p> <p>In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR series routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Supported Certificate Enrollment Methods • Configuring Manual Certificate Enrollment <p>The following commands were introduced or modified by this feature: crypto ca import, enrollment, enrollment terminal</p>
Multiple-Tier CA Hierarchy ¹	12.2(15)T	<p>This enhancement enables users to set up a PKI in a hierarchical framework to support multiple CAs. Within a hierarchical PKI, all enrolled peers can validate the certificate of one another as long as the peers share a trusted root CA certificate or a common subordinate CA.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none"> • Hierarchical PKI: Multiple CAs

Table 1 *Feature Information for PKI Certificate Enrollment (continued)*

Feature Name	Releases	Feature Information
Persistent Self-Signed Certificates	12.2(33)SXH 12.2(33)SRA 12.3(14)T Cisco IOS XE Release 2.1	<p>This feature allows the HTTPS server to generate and save a self-signed certificate in the router startup configuration. Thus, future SSL handshakes between the client and the HTTPS server can use the same self-signed certificate without user intervention.</p> <p>In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR series routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Supported Certificate Enrollment Methods • Configuring a Persistent Self-Signed Certificate for Enrollment via SSL <p>The following commands were introduced or modified by this feature: enrollment selfsigned, show crypto pki certificates, show crypto pki trustpoints</p>
PKI Status ¹	12.3(11)T	<p>This enhancement added the status keyword to the show crypto pki trustpoints command, which allows you to view the current status of the trustpoint. Prior to this enhancement, you had to issue the show crypto pki certificates and the show crypto pki timers commands for the current status.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none"> • How to Configure Certificate Enrollment for a PKI
Reenroll Using Existing Certificates	12.3(11)T Cisco IOS XE Release 2.1	<p>This feature allows users to reenroll a router with a Cisco IOS CA via existing certificates from a third-party vendor CA.</p> <p>In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR series routers.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none"> • Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment <p>The following commands were introduced by this feature: enrollment credential, grant auto trustpoint</p>
Trustpoint CLI	12.2(8)T	<p>This feature introduces the crypto pki trustpoint command, which adds support for trustpoint CAs.</p>

1. This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.

PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005–2007 Cisco Systems, Inc. All rights reserved.



Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment

First Published: May 2, 2005

Last Updated: March 9, 2009

This module describes how to set up and manage a Cisco IOS certificate server for public key infrastructure (PKI) deployment. A certificate server embeds a simple certificate server, with limited certification authority (CA) functionality, into the Cisco IOS software. Thus, the following benefits are provided to the user:

- Easier PKI deployment by defining default behavior. The user interface is simpler because default behaviors are predefined. That is, you can leverage the scaling advantages of PKI without all of the certificate extensions that a CA provides, thereby allowing you to easily enable a basic PKI-secured network.
- Direct integration with Cisco IOS software.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for the Cisco IOS Certificate Server” section on page 50](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Configuring a Cisco IOS Certificate Server, page 2](#)
- [Restrictions for Configuring a Cisco IOS Certificate Server, page 3](#)
- [Information About Cisco IOS Certificate Servers, page 3](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2005–2009 Cisco Systems, Inc. All rights reserved.

- [How to Set Up and Deploy a Cisco IOS Certificate Server, page 10](#)
- [Configuration Examples for Using a Certificate Server, page 36](#)
- [Where to Go Next, page 48](#)
- [Additional References, page 48](#)
- [Feature Information for the Cisco IOS Certificate Server, page 50](#)

Prerequisites for Configuring a Cisco IOS Certificate Server

Planning Your PKI Before Configuring the Certificate Server

Before configuring a Cisco IOS certificate server, it is important that you have planned for and chosen appropriate values for the settings you intend to use within your PKI (such as certificate lifetimes and certificate revocation list (CRL) lifetimes). After the settings have been configured in the certificate server and certificates have been granted, settings cannot be changed without having to reconfigure the certificate server and reenrolling the peers. For information on certificate server default settings and recommended settings, see the section “[Certificate Server Default Values and Recommended Values](#).”

Enabling an HTTP Server

The certificate server supports Simple Certificate Enrollment Protocol (SCEP) over HTTP. The HTTP server must be enabled on the router for the certificate server to use SCEP. (To enable the HTTP server, use the **ip http server** command.) The certificate server will automatically enable or disable SCEP services after the HTTP server is enabled or disabled. If the HTTP server is not enabled, only manual PKCS10 enrollment is supported.



Note

To take advantage of automatic CA certificate and key pair rollover functionality for all types of certificate servers, Cisco IOS Release 12.4(4)T or a later release must be used and SCEP must be used as the enrollment method.

Configuring Reliable Time Services

Time services must be running on the router because the certificate server must have reliable time knowledge. If a hardware clock is unavailable, the certificate server will depend on manually configured clock settings, such as Network Time Protocol (NTP). If there is not a hardware clock or the clock is invalid, the following message will be displayed at bootup:

```
% Time has not been set. Cannot start the Certificate server.
```

After the clock has been set, the certificate server will automatically switch to running status.

For information on manually configuring clock settings, see the section “Setting Time and Calendar Services” in the chapter “Performing Basic System Management” of the *Cisco IOS Network Management Configuration Guide*.

“crypto ca” to “crypto pki” CLI Change

As of Cisco IOS Release 12.3(7)T, all commands that begin as “crypto ca” have been changed to begin as “crypto pki.” Although the router will still accept crypto ca commands, all output will be read back as crypto pki.

Restrictions for Configuring a Cisco IOS Certificate Server

The certificate server does not provide a mechanism for modifying the certificate request that is received from the client; that is, the certificate that is issued from the certificate server matches the requested certificate without modifications. If a specific certificate policy, such as name constraints, must be issued, the policy must be reflected in the certificate request.

Information About Cisco IOS Certificate Servers

Before setting up and deploying a certificate server in your PKI, you should understand the following concepts:

- [RSA Key Pair and Certificate of the Certificate Server, page 3](#)
- [Certificate Server Database, page 4](#)
- [Trustpoint of the Certificate Server, page 6](#)
- [Certificate Revocation Lists \(CRLs\), page 6](#)
- [Certificate Server Error Conditions, page 7](#)
- [Certificate Enrollment Using a Certificate Server, page 8](#)
- [Types of CA Servers: Subordinate and Registration Authorities \(RAs\), page 8](#)
- [Automatic CA Certificate and Key Rollover, page 9](#)

RSA Key Pair and Certificate of the Certificate Server

The certificate server automatically generates a 1024-bit Rivest, Shamir, and Adelman (RSA) key pair. You must manually generate an RSA key pair if you prefer a different key pair modulus. For information on completing this task, see the section “[Generating a Certificate Server RSA Key Pair.](#)”

**Note**

The recommended modulus for a certificate server key pair is 2048 bits.

The certificate server will use a regular Cisco IOS RSA key pair as its CA key. This key pair must have the same name as the certificate server. If you do not generate the key pair before the certificate server is created on the router, a general-purpose key pair will be automatically generated during the configuration of the certificate server.

As of Cisco IOS Release 12.3(11)T and later releases, the CA certificate and CA key can be backed up automatically one time after they are generated by the certificate server. As a result, it is not necessary to generate an exportable CA key for backup purposes.

What to Do with Automatically Generated Key Pairs in Cisco IOS Software Prior to Release 12.3(11)T

If the key pair is automatically generated, it will not be marked as exportable. Thus, you must manually generate the key pair as exportable if you want to back up the CA key. For information on how to complete this task, see the section “[Generating a Certificate Server RSA Key Pair.](#)”

How the CA Certificate and CA Key Are Automatically Archived

At initial certificate server setup, you can enable the CA certificate and the CA key to be automatically archived so that they may be restored later if either the original copy or the original configuration is lost.

When the certificate server is turned on the first time, the CA certificate and CA key will be generated. If automatic archive is also enabled, the CA certificate and the CA key will be exported (archived) to the server database. The archive can be in PKCS12 or privacy-enhanced mail (PEM) format.

**Note**

- This CA key backup file is extremely important and should be moved immediately to another secured place.
- This archiving action occurs only one time. Only the CA key that is (1) manually generated and marked exportable or (2) automatically generated by the certificate server will be archived (this key will be marked nonexportable).
- Autoarchiving will not occur if you generate the CA key manually and mark it “nonexportable.”
- In addition to the CA certificate and CA key archive file, you should also regularly back up the serial number file (.ser) and the CRL file (.crl). The serial file and the CRL file are both critical for CA operation if you need to restore your certificate server.
- It is not possible to manually back up a server that uses nonexportable RSA keys or manually generated, nonexportable RSA keys. Although automatically generated RSA keys are marked as nonexportable, they are automatically archived once.

Certificate Server Database

The Cisco IOS certificate server stores files for its own use and may publish files for other processes to use. Critical files generated by the certificate server that are needed for its ongoing operation are stored to only one location per file type for its exclusive use. The certificate server reads from and writes to these files. The critical certificate server files are the serial number file (.ser) and the CRL storage location file (.crl). Files that the certificate server writes to, but does not read from again, may be published and available for use by other processes. An example of a file that may be published is the issued certificates file (.crt).

Performance of your certificate server may be affected by the following factors, which should be considered when you choose storage options and publication options for your certificate server files.

- The storage or publish locations you choose may affect your certificate server performance. Reading from a network location takes more time than reading directly from a router’s local storage device.
- The number of files you choose to store or publish to a specific location may affect your certificate server performance. The local Cisco IOS file system may not always be suitable for a large number of files.
- The file types you choose to store or publish may affect your certificate server performance. Certain files, such as the .crl files, can become very large.

**Note**

It is recommended that you store .ser and .crl files to your local Cisco IOS file system and publish your .crt files to a remote file system.

Certificate Server Database File Storage

The certificate server allows the flexibility to store different critical file types to different storage locations depending on the database level set (see the **database level** command for more information). When choosing storage locations, consider the file security needed and server performance. For instance, serial number files and archive files (.p12 or .pem) might have greater security restrictions than the issued certificates file storage location (.crt) or the name file storage location (.cnm).

Table 1 shows the critical certificate server file types by file extension that may be stored to a specific location.

Table 1 Certificate Server Storage Critical File Types

File Extension	File Type
.ser	The main certificate server database file.
.crl	The CRL storage location.
.crt	The issued certificates storage location.
.cnm	The certificate name and expiration file storage location.
.p12	The certificate server certificate archive file location in PKCS12 format.
.pem	The certificate server certificate archive file location in PEM format.

Cisco IOS certificate server files may be stored to three levels of specificity:

- Default location, NVRAM
- Specified primary storage location for all critical files
- Specified storage location for specific critical file(s).

A more specific storage location setting overrides a more general storage location setting. For instance, if you have not specified any certificate server file storage locations, all certificate server files will be stored to NVRAM. If you specify a storage location for the name file, only the name file will be stored there; all other files will still be stored to NVRAM. If you then specify a primary location, all files except the name file will now be stored to this location, instead of NVRAM.

**Note**

You may specify either .p12 or .pem; you cannot specify both types of archive files.

Certificate Server Database File Publication

A publish file is a copy of the original file and is available for other processes to use or for your use. If the certificate server fails to publish a file, it does cause the server to shut down. You may specify one publish location for the issued certificates file and name file and multiple publish locations for the CRL file. See Table 2 for files types available for publication. You may publish files regardless of the database level that is set.

Table 2 Certificate Server Publish File Types

File Extension	File Type
.crl	The CRL publish location.
.crt	The issued certificates publish location.
.cnm	The certificate name and expiration file publish location.

Trustpoint of the Certificate Server

The certificate server will also have an automatically generated trustpoint of the same name; the trustpoint will store the certificate of the certificate server. After the router detects that a trustpoint is being used to store the certificate of the certificate server, the trustpoint will be locked so that it cannot be modified.

Before configuring the certificate server you can perform the following:

- Manually create and set up this trustpoint (using the **crypto pki trustpoint** command), which allows you to specify an alternative RSA key pair (using the **rsa keypair** command).
- Specify that the initial autoenrollment key pair will be generated on a specific device, such as a configured and available USB token, using the **on** command.

**Note**

The automatically generated trustpoint and the certificate server certificate are not available for the certificate server device identity. Thus, any command-line interface (CLI) (such as the **ip http secure-trustpoint** command) that is used to specify the CA trustpoint to obtain certificates and authenticate the connecting client's certificate must point to an additional trustpoint configured on the certificate server device.

If the server is a root certificate server, it will use the RSA key pairs and several other attributes to generate a self-signed certificate. The associated CA certificate will have the following key usage extensions—Digital Signature, Certificate Sign, and CRL Sign.

After the CA certificate is generated, attributes can be changed only if the certificate server is destroyed.

**Note**

A certificate server trustpoint must not be automatically enrolled using the **auto-enroll** command. Initial enrollment of the certificate server must be initiated manually and ongoing automatic rollover functionality may be configured with the **auto-rollover** command. For more information on automatic rollover functionality, see the section [“Automatic CA Certificate and Key Rollover.”](#)

Certificate Revocation Lists (CRLs)

By default, CRLs are issued once every 168 hours (1 calendar week). To specify a value other than the default value for issuing the CRL, execute the **lifetime crl** command. After the CRL is issued, it is written to the specified database location as *ca-label.crl*, where *ca-label* is the name of the certificate server.

CRLs can be distributed via SCEP, which is the default method, or a CRL distribution point (CDP), if configured and available. If you set up a CDP, use the **cdp-url** command to specify the CDP location. If the **cdp-url** command is not specified, the CDP certificate extension will not be included in the

certificates that are issued by the certificate server. If the CDP location is not specified, Cisco IOS PKI clients will automatically request a CRL from the certificate server with a SCEP GetCRL message. The CA then returns the CRL in a SCEP CertRep message to the client. Because all SCEP messages are enveloped and signed PKCS#7 data, the SCEP retrieval of the CRL from the certificate server is costly and not highly scalable. In very large networks, an HTTP CDP provides better scalability and is recommended if you have many peer devices that will be checking CRLs. You may specify the CDP location by a simple HTTP URL string for example,

```
cdp-url http://my-cdp.company.com/filename.crl
```

The certificate server supports only one CDP; thus, all certificates that are issued include the same CDP.

If you have PKI clients that are not running Cisco IOS software and that do not support a SCEP GetCRL request and wish to use a CDP you may set up an external server to distribute CRLs and configure the CDP to point to that server. Or, you can specify a non-SCEP request for the retrieval of the CRL from the certificate server by specifying the **cdp-url** command with the URL in the following format where *cs-addr* is the location of the certificate server:

```
cdp-url http://cs-addr/cgi-bin/pkiclient.exe?operation=GetCRL
```

**Note**

If your Cisco IOS CA is also configured as your HTTP CDP server, specify your CDP with the **cdp-url** `http://cs-addr/cgi-bin/pkiclient.exe?operation=GetCRL` command syntax.

It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified via the **cdp-url** command.

In order to force the parser to retain the embedded question mark within the specified location, enter Ctrl-v prior to the question mark. If this action is not taken, CRL retrieval via HTTP will return an error message.

The CDP location may be changed after the certificate server is running via the **cdp-url** command. New certificates will contain the updated CDP location, but existing certificates will not be reissued with the newly specified CDP location. When a new CRL is issued, the certificate server uses its current cached CRL to generate a new CRL. (When the certificate server is rebooted, it reloads the current CRL from the database.) A new CRL cannot be issued unless the current CRL has expired. After the current CRL expires, a new CRL is issued only after a certificate is revoked from the CLI.

Certificate Server Error Conditions

At startup, the certificate server checks the current configuration before issuing any certificates. It reports the last known error conditions via the **show crypto pki server** command output. Example errors can include any of the following conditions:

- Storage inaccessible
- Waiting for HTTP server
- Waiting for time setting

If the certificate server experiences a critical failure at any time, such as failing to publish a CRL, the certificate server will automatically enter a disabled state. This state allows the network administrator to fix the condition; thereafter, the certificate server will return to the previous normal state.

Certificate Enrollment Using a Certificate Server

A certificate enrollment request functions as follows:

- The certificate server receives the enrollment request from an end user, and the following actions occur:
 - A request entry is created in the enrollment request database with the initial state. (See [Table 3](#) for a complete list of certificate enrollment request states.)
 - The certificate server refers to the CLI configuration (or the default behavior any time a parameter is not specified) to determine the authorization of the request. Thereafter, the state of the enrollment request is updated in the enrollment request database.
- At each SCEP query for a response, the certificate server examines the current request and performs one of the following actions:
 - Responds to the end user with a “pending” or “denied” state.
 - Generates and signs the appropriate certificate and stores the certificate in the enrollment request database.

If the connection of the client has closed, the certificate server will wait for the client to request another certificate.

All enrollment requests transition through the certificate enrollment states that are defined in [Table 3](#). To see current enrollment requests, use the **crypto pki server request pkcs10** command.

Table 3 *Certificate Enrollment Request State Descriptions*

Certificate Enrollment State	Description
authorized	The certificate server has authorized the request.
denied	The certificate server has denied the request for policy reasons.
granted	The CA core has generated the appropriate certificate for the certificate request.
initial	The request has been created by the SCEP server.
malformed	The certificate server has determined that the request is invalid for cryptographic reasons.
pending	The enrollment request must be manually accepted by the network administrator.

SCEP Enrollment

All SCEP requests are treated as new certificate enrollment requests, even if the request specifies a duplicate subject name or public key pair as a previous certificate request.

Types of CA Servers: Subordinate and Registration Authorities (RAs)

CA servers have the flexibility to be configured as a subordinate certificate server or an RA-mode certificate server.

Why Configure a Subordinate CA?

A subordinate certificate server provides all the same features as a root certificate server. The root RSA key pairs are extremely important in a PKI hierarchy, and it is often advantageous to keep them offline or archived. To support this requirement, PKI hierarchies allow for subordinate CAs that have been signed by the root authority. In this way, the root authority can be kept offline (except to issue occasional CRL updates), and the subordinate CA can be used during normal operation.

Why Configure an RA-Mode Certificate Server?

A Cisco IOS certificate server can be configured to run in RA mode. An RA offloads authentication and authorization responsibilities from a CA. When the RA receives a SCEP or manual enrollment request, the administrator can either reject or grant it on the basis of local policy. If the request is granted, it will be forwarded to the issuing CA, and the CA will automatically generate the certificate and return it to the RA. The client can later retrieve the granted certificate from the RA.

An RA is the authority charged with recording or verifying some or all of the data required for the CA to issue certificates. In many cases the CA will undertake all of the RA functions itself, but where a CA operates over a wide geographical area or when there is security concern over exposing the CA to direct network access, it may be administratively advisable to delegate some of the tasks to an RA and leave the CA to concentrate on its primary tasks of signing certificates and CRLs.

Automatic CA Certificate and Key Rollover

CAs—root CAs, subordinate CAs, and RA-mode CAs—like their clients, have certificates and key pairs with expiration dates that need to be reissued when the current certificate and key pair are about to expire. When a root CA's certificate and key pair are expiring it must generate a self-signed rollover certificate and key pair. If a subordinate CA or an RA-mode CA's certificate and key pair are expiring, it will request a rollover certificate and key pair from its superior CA, obtaining the superior CA's new self-signed rollover certificates at the same time. The CA must distribute the new CA rollover certificate and keys too all its peers. This process, called rollover, allows for continuous operation of the network while the CAs and their clients are switching from an expiring CA certificate and key pair to a new CA certificate and key pair.

Rollover relies on the PKI infrastructure requirements of trust relationships and synchronized clocks. The PKI trust relationships allow (1) the new CA certificate to be authenticated, and (2) the rollover to be accomplished automatically without the loss of security. Synchronized clocks allow the rollover to be coordinated throughout your network.

Automatic CA Certificate Rollover: How It Works

The CA server must have rollover configured. All levels of CAs must be automatically enrolled and have **auto-rollover** enabled. CA clients support rollover automatically when automatically enrolled. For more information about clients and automatic rollover, see the section “[Automatic Certificate Enrollment](#)” in the chapter “Configuring Certificate Enrollment for a PKI”.

After CAs have rollover enabled and their clients are automatically enrolled, there are three stages to the automatic CA certificate rollover process.

Stage One: Active CA Certificate and Key Pair Only

In stage one, there is an active CA certificate and key pair only.

Stage Two: Rollover CA Certificate and Key Pair Generation and Distribution

In stage two, the rollover CA certificate and key pair are generated and distributed. The superior CA generates a rollover certificate and key pair. After the CA successfully saves its active configuration, the CA is ready to respond to client requests for the rollover certificate and key pair. When the superior CA receives a request for the new CA certificate and key pair from a client, the CA responds by sending the new rollover CA certificate and key pair to the requesting client. The clients store the rollover CA certificate and key pair.

**Note**

When a CA generates its rollover certificate and key pair, it must be able to save its active configuration. If the current configuration has been altered, saving of the rollover certificate and key pair will not happen automatically. In this case, the administrator must save the configuration manually or rollover information will be lost.

Stage Three: Rollover CA Certificate and Key Pair Become the Active CA Certificate and Key Pair

In stage three, the rollover CA certificate and key pair become the active CA certificate and key pair. All devices that have stored a valid rollover CA certificate rename the rollover certificate to the active certificate and the once-active certificate and key pair are deleted.

How to Set Up and Deploy a Cisco IOS Certificate Server

This section contains the following procedures:

- [Generating a Certificate Server RSA Key Pair, page 10](#)
- [Configuring Certificate Servers, page 13](#)
- [Configuring Certificate Server Functionality, page 24](#)
- [Working with Automatic CA Certificate Rollover, page 28](#)
- [Maintaining, Verifying, and Troubleshooting the Certificate Server, Certificates, and the CA, page 30](#)

Generating a Certificate Server RSA Key Pair

Perform this task to manually generate an RSA key pair for the certificate server. Manually generating a certificate server RSA key pair allows you to specify the type of key pair you want to generate, to create an exportable key pair for backup purposes, to specify the key pair storage location, or to specify the key generation location.

If you are running Cisco IOS Release 12.3(8)T or earlier releases, you may want to create an exportable certificate server key pair for backup, or archive purposes. If this task is not performed, the certificate server will automatically generate a key pair, which will not be marked as exportable. Automatic CA certificate archiving was introduced in Cisco IOS Release 12.3(11)T.

As of Cisco IOS Release 12.4(11)T and later releases, if your router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication of credentials to be performed on a USB token. The private key never leaves the USB token and is not exportable. The public key is exportable. For titles of specific documents about configuring a USB token and making it available to use as a cryptographic device, see the “Related Documents” section.

**Note**

It is recommended that the private key be kept in a secure location and that you regularly archive the certificate server database.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename:*] [**on** *devicename:*]
4. **crypto key export rsa** *key-label* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*
5. **crypto key import rsa** *key-label* **pem** [**usage-keys** | **signature** | **encryption**] {**terminal** | **url** *url*} [**exportable**] [**on** *devicename:*] *passphrase*
6. **exit**
7. **show crypto key mypubkey rsa**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto key generate rsa [general-keys usage-keys signature encryption] [label <i>key-label</i>] [exportable] [modulus <i>modulus-size</i>] [storage <i>devicename:</i>] [on <i>devicename:</i>] Example: Router (config)# crypto key generate rsa label mycs exportable modulus 2048	Generates the RSA key pair for the certificate server. When specifying a label name, you must use the same name for the label that you plan to use for the certificate server (via the crypto pki server cs-label command). By default, the fully qualified domain name (FQDN) of the router is used for the key label. If you manually generate the exportable RSA key pair but wait until after the CA certificate has been generated before issuing the no shutdown command, you can use the crypto ca export pkcs12 command to export a PKCS12 file that contains the certificate server certificate and the private key. By default, the modulus size of a CA key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range for a CA key is from 350 to 2048 bits.

	Command or Action	Purpose
Step 4	crypto key export rsa <i>key-label</i> pem [terminal url <i>url</i>] { 3des des } <i>passphrase</i> Example: Router (config)# crypto key export rsa mycs pem url nvram: 3des PASSWORD	(Optional) Exports the generated RSA key pair. Allows you to export the generated keys.
Step 5	crypto key import rsa <i>key-label</i> pem [usage-keys signature encryption] { terminal url <i>url</i> } [exportable] [on <i>devicename:</i>] <i>passphrase</i> Example: Router (config)# crypto key import rsa mycs2 pem url nvram:mycs PASSWORD	(Optional) Imports RSA key pair. To create the imported keys on a USB token, use the on keyword and specify the appropriate device location. If you exported the RSA keys using the exportable keyword and you want to change the RSA key pair to nonexportable, import the key back to the certificate server without the exportable keyword. The key cannot be exported again.
Step 6	exit Example: Router (config)# exit	Exits global configuration.
Step 7	show crypto key mypubkey rsa Example: Router# show crypto key mypubkey rsa	Displays the RSA public keys of your router.

Examples

The following example generates a general usage 1024-bit RSA key pair on a USB token with the label “ms2” with crypto engine debugging messages shown:

```
Router(config)# crypto key generate rsa on usbtoken0 label ms2 modulus 1024
The name for the keys will be: ms2
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw) (ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw) (ipsec)
```

Now, the on-token keys labeled “ms2” may be used for enrollment.

The following example shows the successful import of an encryption key to a configured and available USB tokens:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# crypto key import rsa encryption on usbtoken0 url nvram:e password
% Importing public Encryption key or certificate PEM file...
filename [e-encr.pub]?
Reading file from nvram:e-encr.pub
% Importing private Encryption key PEM file...
Source filename [e-encr.prv]?
Reading file from nvram:e-encr.prv
% Key pair import succeeded.
```

Configuring Certificate Servers

The following tasks explain how to configure a certificate server, a subordinate certificate server, or an RA-mode certificate server, and how to enable automatic rollover.

- [Configuring a Certificate Server, page 13](#)
- [Configuring a Subordinate Certificate Server, page 15](#)
- [Configuring a Certificate Server to Run in RA Mode, page 21](#)
- [Configuring the Root Certificate Server to Delegate Enrollment Tasks to the RA Mode Certificate Server, page 23](#)

Prerequisites for Automatic CA Certificate Rollover

When configuring a certificate server, for automatic CA certificate rollover to run successfully, the following prerequisites are applicable for your CA servers:

- You must be running Cisco IOS Release 12.4(2)T or a later release on your CA servers.
- Your CA server must be enabled and fully configured with a reliable time of day, an available key pair, a self-signed, valid CA certificate associated with the key pair, a CRL, an accessible storage device, and an active HTTP/SCEP server.
- CA clients must have successfully completed automatic enrollment and have autoenrollment enabled with the same certificate server.

**Note**

If you are running Cisco IOS 12.4(2)T or earlier releases, only your root CA will support automatic CA certificate rollover functionality. Cisco IOS 12.4(4)T or later releases support all CAs—root CAs, subordinate CAs, and RA-mode CAs.

Restrictions for Automatic CA Certificate Rollover

When configuring a certificate server, in order for automatic CA certificate rollover to run successfully, the following restrictions are applicable:

- SCEP must be used to support rollover. Any device that enrolls with the PKI using an alternative to SCEP as the certificate management protocol or mechanism (such as enrollment profiles, manual enrollment, or TFTP enrollment) will not be able to take advantage of the rollover functionality provided by SCEP.
- If you have automatic archive configured on your network and the archive fails, rollover will not occur because the certificate server will not enter the rollover state, and the rollover certificate and key pair will not be automatically saved.

Configuring a Certificate Server

Perform this task to configure a Cisco IOS certificate server and enable automatic rollover.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **ip http server**
4. **crypto pki server** *cs-label*
5. **no shutdown**
6. **auto-rollover** [*time-period*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip http server Example: Router(config)# ip http server	Enables the HTTP server on your system.
Step 4	crypto pki server <i>cs-label</i> Example: Router(config)# crypto pki server server-pki	Defines a label for the certificate server and enters certificate server configuration mode. <p>Note If you manually generated an RSA key pair, the <i>cs-label</i> argument must match the name of the key pair.</p>
Step 5	no shutdown Example: Router(cs-server)# no shutdown	(Optional) Enables the certificate server. <p>Note Only use this command at this point if you want to use the preconfigured default functionality. That is, do not issue this command just yet if you plan to change any of the default settings as shown in the task “Configuring Certificate Server Functionality.”</p>
Step 6	auto-rollover [<i>time-period</i>] Example: Router(cs-server)# auto-rollover 90	(Optional) Enables the automated CA certificate rollover functionality. <ul style="list-style-type: none"> <i>time-period</i>—default is 30 days.

Examples

The following example shows how to configure the certificate server “ca”:

```
Router(config)# crypto pki server ca
Router(cs-server)# no shutdown
```

```
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: yes
% Generating 1024 bit RSA keys ...[OK]
```



```
% Certificate Server enabled.
Router(cs-server)# end
!
Router# show crypto pki server

Certificate Server ca:
  Status: enabled, configured
  CA cert fingerprint: 5A856122 4051347F 55E8C246 866D0AC3
  Granting mode is: manual
  Last certificate issued serial number: 0x1
  CA certificate expiration timer: 19:44:57 GMT Oct 14 2006
  CRL NextUpdate timer: 19:45:25 GMT Oct 22 2003
  Current storage dir: nvram:
  Database Level: Complete - all issued certs written as <serialnum>.cer
```

The following example shows how to enable automated CA certificate rollover on the server mycs with the **auto-rollover** command. The **show crypto pki server** command shows that the automatic rollover has been configured on the server mycs with an overlap period of 25 days.

```
Router(config)# crypto pki server mycs
Router(cs-server)# auto-rollover 25
Router(cs-server)# no shut

%Some server settings cannot be changed after CA certificate generation.
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% Exporting Certificate Server signing certificate and keys...

% Certificate Server enabled.
Router(cs-server)#

Router# show crypto pki server

Certificate Server mycs:
  Status:enabled
  Server's configuration is locked (enter "shut" to unlock it)
  Issuer name:CN=mycs
  CA cert fingerprint:70AFECA9 211CDDCC 6AA9D7FF 3ADB03AE
  Granting mode is:manual
  Last certificate issued serial number:0x1
  CA certificate expiration timer:00:49:26 PDT Jun 20 2008
  CRL NextUpdate timer:00:49:29 PDT Jun 28 2005
  Current storage dir:nvram:
  Database Level:Minimum - no cert data written to storage
  Auto-Rollover configured, overlap period 25 days
  Autorollover timer:00:49:26 PDT May 26 2008
```

Configuring a Subordinate Certificate Server

Perform this task to configure a subordinate certificate server to grant all or certain SCEP or manual certificate requests and to enable automatic rollover.

Restrictions

- You must be running Cisco IOS Release 12.3(14)T or a later release. (Versions prior to Cisco IOS software Release 12.3(14)T support only one certificate server and no hierarchy; that is, subordinate certificate servers are not supported.)
- The root certificate server should be a Cisco IOS certificate server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **exit**
6. **crypto pki server** *cs-label*
7. **issuer name** *DN-string*
8. **mode sub-cs**
9. **auto-rollover** [*time-period*]
10. **grant auto rollover** {*ca-cert* | *ra-cert*}
11. **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint <i>name</i> Example: Router (config)# crypto pki trustpoint sub	Declares the trustpoint that your subordinate certificate server should use and enters ca-trustpoint configuration mode.
Step 4	enrollment url <i>url</i> Example: Router (ca-trustpoint)# enrollment url http://192.0.2.6	Specifies the enrollment URL of the issuing CA certificate server (root certificate server).
Step 5	exit Example: Router (ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.
Step 6	crypto pki server <i>cs-label</i> Example: Router(config)# crypto pki server sub	Enables a Cisco IOS certificate server and enters cs-server configuration mode. Note The subordinate server must have the same name as the trustpoint that was created in Step 3 above.

	Command or Action	Purpose
Step 7	issuer name <i>DN-string</i> Example: Router(cs-server)# issuer-name CN=sub CA, O=Cisco, C=us	(Optional) Specifies the DN as the CA issuer name for the certificate server.
Step 8	mode sub-cs Example: Router(cs-server)# mode sub-cs	Places the PKI server into sub-certificate server mode.
Step 9	auto-rollover [<i>time-period</i>] Example: Router(cs-server)# auto-rollover 90	(Optional) Enables the automated CA certificate rollover functionality. <ul style="list-style-type: none"> <i>time-period</i>—default is 30 days.
Step 10	grant auto rollover { ca-cert ra-cert } Example: Router(cs-server)# grant auto rollover ca-cert	(Optional) Automatically grants reenrollment requests for subordinate CAs and RA-mode CAs without operator intervention. <ul style="list-style-type: none"> ca-cert—Specifies that the subordinate CA rollover certificate will be automatically granted. ra-cert—Specifies that the RA-mode CA rollover certificate will be automatically granted. Note If this is the first time that a subordinate certificate server is enabled and enrolled, the certificate request must be manually granted.
Step 11	no shutdown Example: Router(cs-server)# no shutdown	Enables or reenables the certificate server. If this is the first time that a subordinate certificate server is enabled, the certificate server will generate the key and obtain its signing certificate from the root certificate server.

Examples

If the certificate server fails to enable or if the certificate server has trouble handling the request that has been configured, you can use the **debug crypto pki server** command to troubleshoot your configuration as shown in the following examples (Clock Not Set and Trustpoint Not Configured):

```
Router# debug crypto pki server
```

Clock Not Set

```
Router (config)# crypto pki server sub
Router (cs-server)# mode sub-cs
Router (cs-server)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key % or type Return to exit
Password:
*Jan  6 20:57:37.667: CRYPTO_CS: enter FSM: input state initial, input signal no shut

Re-enter password:
% Generating 1024 bit RSA keys ...
```

```
*Jan  6 20:57:45.303: CRYPTO_CS: starting enabling checks
*Jan  6 20:57:45.303: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]
% Time has not been set. Cannot start the Certificate server
```

Trustpoint Not Configured

```
Router (config)# crypto pki server sub
Router (cs-server)# mode sub-cs
Router (cs-server)# no shutdown

%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key or type Return to exit
Password:
Jan  6 21:00:15.961: CRYPTO_CS: enter FSM: input state initial, input signal no shut.
Jan  6 21:03:34.309: CRYPTO_CS: enter FSM: input state initial, input signal time set.
Jan  6 21:03:34.313: CRYPTO_CS: exit FSM: new state initial.
Jan  6 21:03:34.313: CRYPTO_CS: cs config has been unlocked
Re-enter password:
% Generating 1024 bit RSA keys ...
Jan  6 21:03:44.413: CRYPTO_CS: starting enabling checks
Jan  6 21:03:44.413: CRYPTO_CS: associated trust point 'sub' does not exist; generated
automatically
Jan  6 21:03:44.417: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]

Jan  6 21:04:03.993: CRYPTO_CS: nvram filesystem
Jan  6 21:04:04.077: CRYPTO_CS: serial number 0x1 written.
You must specify an enrollment URL for this CA before you can authenticate it.
% Failed to authenticate the Certificate Authority
```

If the certificate server fails to obtain its signing certificate from the root certificate server, you can use the **debug crypto pki transactions** command to troubleshoot your configuration as shown in the following example:

```
Router# debug crypto pki transactions

Jan  6 21:07:00.311: CRYPTO_CS: enter FSM: input state initial, input signal time set
Jan  6 21:07:00.311: CRYPTO_CS: exit FSM: new state initial
Jan  6 21:07:00.311: CRYPTO_CS: cs config has been unlocked no sh
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key % or type Return to exit
Password:
Jan  6 21:07:03.535: CRYPTO_CS: enter FSM: input state initial, input signal no shut
Re-enter password:
% Generating 1024 bit RSA keys ...
Jan  6 21:07:10.619: CRYPTO_CS: starting enabling checks
Jan  6 21:07:10.619: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]

Jan  6 21:07:20.535: %SSH-5-ENABLED: SSH 1.99 has been enabled
Jan  6 21:07:25.883: CRYPTO_CS: nvram filesystem
Jan  6 21:07:25.991: CRYPTO_CS: serial number 0x1 written.
Jan  6 21:07:27.863: CRYPTO_CS: created a new serial file.
Jan  6 21:07:27.863: CRYPTO_CS: authenticating the CA 'sub'
Jan  6 21:07:27.867: CRYPTO_PKI: Sending CA Certificate Request:
GET /cgi-bin/pkiclient.exe?operation=GetCACert&message=sub HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)

Jan  6 21:07:27.867: CRYPTO_PKI: can not resolve server name/IP address
Jan  6 21:07:27.871: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6 Certificate has the
following attributes:
    Fingerprint MD5: 328ACC02 52B25DB8 22F8F104 B6055B5B
    Fingerprint SHA1: 02FD799D DD40C7A8 61DC53AB 1E89A3EA 2A729EE2

% Do you accept this certificate? [yes/no]:
Jan  6 21:07:30.879: CRYPTO_PKI: http connection opened
```

```
Jan 6 21:07:30.903: CRYPTO_PKI: HTTP response header:
  HTTP/1.1 200 OK
Date: Thu, 06 Jan 2005 21:07:30 GMT
Server: server-IOS
Content-Type: application/x-x509-ca-cert
Expires: Thu, 06 Jan 2005 21:07:30 GMT
Last-Modified: Thu, 06 Jan 2005 21:07:30 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none

Content-Type indicates we have received a CA certificate.

Jan 6 21:07:30.903: Received 507 bytes from server as CA certificate:
Jan 6 21:07:30.907: CRYPTO_PKI: transaction GetCACert completed
Jan 6 21:07:30.907: CRYPTO_PKI: CA certificate received.
Jan 6 21:07:30.907: CRYPTO_PKI: CA certificate received.
Jan 6 21:07:30.927: CRYPTO_PKI: crypto_pki_authenticate_tp_cert()

Jan 6 21:07:30.927: CRYPTO_PKI: trustpoint sub authentication status = 0 y Trustpoint CA
certificate accepted.%

% Certificate request sent to Certificate Authority

% Enrollment in progress...
Router (cs-server)#
Jan 6 21:07:51.772: CRYPTO_CA: certificate not found
Jan 6 21:07:51.772: CRYPTO_CA: certificate not found
Jan 6 21:07:52.460: CRYPTO_CS: Publishing 213 bytes to crl file nvram:sub.crl
Jan 6 21:07:54.348: CRYPTO_CS: enrolling the server's trustpoint 'sub'
Jan 6 21:07:54.352: CRYPTO_CS: exit FSM: new state check failed
Jan 6 21:07:54.352: CRYPTO_CS: cs config has been locked
Jan 6 21:07:54.356: CRYPTO_PKI: transaction PKCSReq completed
Jan 6 21:07:54.356: CRYPTO_PKI: status:
Jan 6 21:07:55.016: CRYPTO_PKI: Certificate Request Fingerprint MD5: 1BA027DB 1C7860C7
EC188F65 64356C80
Jan 6 21:07:55.016: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 840DB52C E17614CB
0C7BE187 0DFC884D D32CAA75
Jan 6 21:07:56.508: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:07:56.508: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6
Jan 6 21:07:56.516: CRYPTO_PKI: http connection opened
Jan 6 21:07:59.136: CRYPTO_PKI: received msg of 776 bytes
Jan 6 21:07:59.136: CRYPTO_PKI: HTTP response header:
  HTTP/1.1 200 OK
Date: Thu, 06 Jan 2005 21:07:57 GMT
Server: server-IOS
Content-Type: application/x-pki-message
Expires: Thu, 06 Jan 2005 21:07:57 GMT
Last-Modified: Thu, 06 Jan 2005 21:07:57 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none

Jan 6 21:07:59.324: The PKCS #7 message has 1 verified signers.
Jan 6 21:07:59.324: signing cert: issuer=cn=root1
Jan 6 21:07:59.324: Signed Attributes:

Jan 6 21:07:59.328: CRYPTO_PKI: status = 102: certificate request pending
Jan 6 21:08:00.788: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:08:00.788: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6
Jan 6 21:08:00.796: CRYPTO_PKI: http connection opened
Jan 6 21:08:11.804: CRYPTO_PKI: received msg of 776 bytes
Jan 6 21:08:11.804: CRYPTO_PKI: HTTP response header: HTTP/1.1 200 OK
```

```

Date: Thu, 06 Jan 2005 21:08:01 GMT
Server: server-IOS
Content-Type: application/x-pki-message
Expires: Thu, 06 Jan 2005 21:08:01 GMT
Last-Modified: Thu, 06 Jan 2005 21:08:01 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none

```

```

Jan 6 21:08:11.992: The PKCS #7 message has 1 verified signers.
Jan 6 21:08:11.992: signing cert: issuer=cn=root1
Jan 6 21:08:11.996: Signed Attributes:

```

```

Jan 6 21:08:11.996: CRYPTO_PKI: status = 102: certificate request pending
Jan 6 21:08:21.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:08:31.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:08:41.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:08:51.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:09:01.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:09:11.996: CRYPTO_PKI: resend GetCertInitial, 1
Jan 6 21:09:11.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:09:11.996: CRYPTO_PKI: resend GetCertInitial for session: 0
Jan 6 21:09:11.996: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:09:11.996: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6
Jan 6 21:09:12.024: CRYPTO_PKI: http connection opened% Exporting Certificate Server
signing certificate and keys...

```

```

Jan 6 21:09:14.784: CRYPTO_PKI: received msg of 1611 bytes
Jan 6 21:09:14.784: CRYPTO_PKI: HTTP response header:
HTTP/1.1 200 OK
Date: Thu, 06 Jan 2005 21:09:13 GMT
Server: server-IOS
Content-Type: application/x-pki-message
Expires: Thu, 06 Jan 2005 21:09:13 GMT
Last-Modified: Thu, 06 Jan 2005 21:09:13 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none

```

```

Jan 6 21:09:14.972: The PKCS #7 message has 1 verified signers.
Jan 6 21:09:14.972: signing cert: issuer=cn=root1
Jan 6 21:09:14.972: Signed Attributes:

```

```

Jan 6 21:09:14.976: CRYPTO_PKI: status = 100: certificate is granted
Jan 6 21:09:15.668: The PKCS #7 message contains 1 certs and 0 crls.
Jan 6 21:09:15.688: Newly-issued Router Cert: issuer=cn=root serial=2
Jan 6 21:09:15.688: start date: 21:08:03 GMT Jan 6 2005
Jan 6 21:09:15.688: end date: 21:08:03 GMT Jan 6 2006
Jan 6 21:09:15.688: Router date: 21:09:15 GMT Jan 6 2005
Jan 6 21:09:15.692: Received router cert from CA
Jan 6 21:09:15.740: CRYPTO_CA: certificate not found
Jan 6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan 6 21:09:15.744: %PKI-6-CERTRET: Certificate received from Certificate Authority
Jan 6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan 6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan 6 21:09:15.748: CRYPTO_CS: enter FSM: input state check failed, input signal cert
configured
Jan 6 21:09:15.748: CRYPTO_CS: starting enabling checks
Jan 6 21:09:15.748: CRYPTO_CS: nvram filesystem
Jan 6 21:09:15.796: CRYPTO_CS: found existing serial file.
Jan 6 21:09:15.820: CRYPTO_CS: old router cert flag 0x4
Jan 6 21:09:15.820: CRYPTO_CS: new router cert flag 0x44

```

```

Jan  6 21:09:18.432: CRYPTO_CS: DB version 1
Jan  6 21:09:18.432: CRYPTO_CS: last issued serial number is 0x1
Jan  6 21:09:18.480: CRYPTO_CS: CRL file sub.crl exists.
Jan  6 21:09:18.480: CRYPTO_CS: Read 213 bytes from crl file sub.crl.
Jan  6 21:09:18.532: CRYPTO_CS: SCEP server started
Jan  6 21:09:18.532: CRYPTO_CS: exit FSM: new state enabled
Jan  6 21:09:18.536: CRYPTO_CS: cs config has been locked
Jan  6 21:09:18.536: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.

```

If the certificate server fails to enable or if the certificate server has trouble handling the request that has been configured, you can use the **debug crypto pki server** command to troubleshoot the progress of an enrollment. This command can also be used to debug the root CA (turn it on at the root CA).

Configuring a Certificate Server to Run in RA Mode

Restrictions for Configuring a Certificate Server for RA Mode

When the Cisco IOS certificate server is acting as an RA, the issuing CA should be a Cisco IOS certificate server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **subject-name** *x.500-name*
6. **exit**
7. **crypto pki server** *cs-label*
8. **mode ra**
9. **auto-rollover** [*time-period*]
10. **grant auto rollover** {*ca-cert* | *ra-cert*}
11. **no shutdown**
12. **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	crypto pki trustpoint <i>name</i> Example: Router (config)# crypto pki trustpoint ra-server	Declares the trustpoint that your RA mode certificate server should use and enters ca-trustpoint configuration mode.
Step 4	enrollment url <i>url</i> Example: Router (ca-trustpoint)# enrollment url http://ca-server.company.com	Specifies the enrollment URL of the issuing CA certificate server (root certificate server).
Step 5	subject-name <i>x.500-name</i> Example: Router (ca-trustpoint)# subject-name cn=ioscs RA	(Optional) Specifies the subject name the RA will use. Note Include “cn=ioscs RA” or “ou=ioscs RA” in the subject name so that the issuing CA certificate server can recognize the RA (see Step 7 below).
Step 6	exit Example: Router (ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.
Step 7	crypto pki server <i>cs-label</i> Example: Router(config)# crypto pki server ra-server	Enables a Cisco IOS certificate server and enters cs-server configuration mode. Note The certificate server must have the same name as the trustpoint that was created in Step 3 above.
Step 8	mode ra Example: Router(cs-server)# mode ra	Places the PKI server into RA certificate server mode.
Step 9	auto-rollover [<i>time-period</i>] Example: Router(cs-server)# auto-rollover 90	(Optional) Enables the automatic CA certificate rollover functionality. <ul style="list-style-type: none"> <i>time-period</i>—default is 30 days.
Step 10	grant auto rollover { ca-cert ra-cert } Example: Router(cs-server)# grant auto rollover ra-cert	(Optional) Automatically grants reenrollment requests for subordinate CAs and RA-mode CAs without operator intervention. <ul style="list-style-type: none"> ca-cert—Specifies that the subordinate CA rollover certificate will be automatically granted. ra-cert—Specifies that the RA-mode CA rollover certificate will be automatically granted. If this is the first time that a subordinate certificate server is enabled and enrolled, the certificate request must be manually granted.

	Command or Action	Purpose
Step 11	no shutdown Example: Router(cs-server)# no shutdown	Enables the certificate server. Note After this command is issued, the RA will automatically enroll with the root certificate server. After the RA certificate has been successfully received, you must issue the no shutdown command again, which reenables the certificate server.
Step 12	no shutdown Example: Router(cs-server)# no shutdown	Reenables the certificate server.

Configuring the Root Certificate Server to Delegate Enrollment Tasks to the RA Mode Certificate Server

Perform the following steps on the router that is running the issuing certificate server; that is, configure the root certificate server that is delegating enrollment tasks to the RA mode certificate server.



Note

Granting enrollment requests for an RA is essentially the same process as granting enrollment requests for client devices—except that enrollment requests for an RA are displayed in the section “RA certificate requests” of the command output for the **crypto pki server info-requests** command.

SUMMARY STEPS

1. **enable**
2. **crypto pki server** *cs-label* **info requests**
3. **crypto pki server** *cs-label* **grant req-id**
4. **configure terminal**
5. **crypto pki server** *cs-label*
6. **grant ra-auto**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	crypto pki server <i>cs-label</i> info requests Example: Router# crypto pki server root-server info requests	Displays the outstanding RA certificate request. Note This command is issued on the router that is running the issuing certificate server.

	Command or Action	Purpose
Step 3	crypto pki server <i>cs-label</i> grant <i>req-id</i> Example: Router# crypto pki server root-server grant 9	Grants the pending RA certificate request. Note Because the issuing certificate server will delegate the enrollment request verification task to the RA, you must pay extra attention to the RA certificate request before granting it.
Step 4	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 5	crypto pki server <i>cs-label</i> Example: Router (config)# crypto pki server root-server	Enables a Cisco IOS certificate server and enters cs-server configuration mode.
Step 6	grant ra-auto Example: Router(cs-server)# grant ra-auto	(Optional) Specifies that all enrollment requests from an RA are to be granted automatically. Note For the grant ra-auto command to work, you have to include “cn=ioscs RA” or “ou=ioscs RA” in the subject name of the RA certificate. (See Step 2 above.)

What to Do Next

After you have configured a certificate server, you can use the preconfigured default values or specify values via the CLI for the functionality of the certificate server. If you choose to specify values other than the defaults, see the following section, “[Configuring Certificate Server Functionality](#).”

Configuring Certificate Server Functionality

After you have enabled a certificate server and are in certificate server configuration mode, use any of the steps in this task to configure basic certificate server functionality values other than the default values.

Certificate Server Default Values and Recommended Values

The default values for a certificate server are intended to address a relatively small network (of about ten devices). For example, the database settings are minimal (via the **database level minimal** command) and the certificate server handles all CRL requests via SCEP. For larger networks, it is recommended that you use either the database setting “names” or “complete” (as described in the **database level** command) for possible audit and revocation purposes. Depending on the CRL checking policy, you should also use an external CDP in a larger network.

Certificate Server File Storage and Publication Locations

You have the flexibility to store file types to different storage and publication locations.

SUMMARY STEPS

1. **database url** *root-url*
2. **database url** {*cnm* | *crl* | *crt* | **p12** | **pem** | **ser**} *root-url*
3. **database url** {*cnm* | *crl* | *crt*} **publish** *root-url*
4. **database level** {*minimal* | *names* | **complete**}
5. **database username** *username* [**password** [*encr-type*] *password*]
6. **database archive** {**pkcs12** | **pem**} [**password** [*encr-type*] *password*]
7. **issuer-name** *DN-string*
8. **lifetime** {*ca-certificate* | *certificate*} *time*
9. **lifetime crl** *time*
10. **lifetime enrollment-request** *time*
11. **cdp-url** *url*
12. **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	database url <i>root-url</i> Example: Router (cs-server)# database url tftp://cert-svr-db.company.com	Specifies the primary location where database entries for the certificate server will be written out. If this command is not specified, all database entries will be written to NVRAM.
Step 2	database url { <i>cnm</i> <i>crl</i> <i>crt</i> p12 pem ser } <i>root-url</i> Example: Router (cs-server)# database url ser nvram:	Specifies certificate server critical file storage location by file type. Note If this command is not specified, all critical files will be stored to the primary location if specified. If the primary location is not specified, all critical files will be stored to NVRAM.
Step 3	database url { <i>cnm</i> <i>crl</i> <i>crt</i> } publish <i>root-url</i> Example: Router (cs-server)# database url crl publish tftp://csdb_specific_crl_files.company.com	Specifies certificate server publish location by file type. Note If this command is not specified, all publish files will be stored to the primary location if specified. If the primary location is not specified, all publish files will be stored to NVRAM.

	Command or Action	Purpose
Step 4	<p>database level {minimal names complete}</p> <p>Example: Router (cs-server)# database level complete</p>	<p>Controls what type of data is stored in the certificate enrollment database.</p> <ul style="list-style-type: none"> • minimal—Enough information is stored only to continue issuing new certificates without conflict; the default value. • names—In addition to the information given in the minimal level, the serial number and subject name of each certificate. • complete—In addition to the information given in the minimal and names levels, each issued certificate is written to the database. <p>Note The complete keyword produces a large amount of information; if it is issued, you should also specify an external TFTP server in which to store the data via the database url command.</p>
Step 5	<p>database username <i>username</i> [password [<i>encr-type</i>] <i>password</i>]</p> <p>Example: Router (cs-server)# database username user password PASSWORD</p>	<p>(Optional) Sets a username and password when a user is required to access a primary certificate enrollment database storage location.</p>
Step 6	<p>database archive {pkcs12 pem} [password [<i>encr-type</i>] <i>password</i>]</p> <p>Example: Router (cs-server)# database archive pem</p>	<p>(Optional) Sets the CA key and CA certificate archive format and password to encrypt the file.</p> <p>The default value is pkcs12, so if this subcommand is not configured, autoarchiving will still be done, and the PKCS12 format will be used.</p> <ul style="list-style-type: none"> • The password is optional. If it is not configured, you will be prompted for the password when the server is turned on for the first time. <p>Note It is recommended that you remove the password from the configuration after the archive is finished.</p>
Step 7	<p>issuer-name <i>DN-string</i></p> <p>Example: Router (cs-server)# issuer-name my-server</p>	<p>(Optional) Sets the CA issuer name to the specified distinguished name (<i>DN-string</i>). The default value is as follows: issuer-name cn={cs-label}.</p>
Step 8	<p>lifetime {ca-certificate certificate} <i>time</i></p> <p>Example: Router (cs-server)# lifetime certificate 888</p>	<p>(Optional) Specifies the lifetime, in days, of a CA certificate or a certificate.</p> <p>Valid values range from 1 day to 1825 days. The default CA certificate lifetime is 3 years; the default certificate lifetime is 1 year. The maximum certificate lifetime is 1 month less than the lifetime of the CA certificate.</p>
Step 9	<p>lifetime crl <i>time</i></p> <p>Example: Router (cs-server)# lifetime crl 333</p>	<p>(Optional) Defines the lifetime, in hours, of the CRL that is used by the certificate server.</p> <p>Maximum lifetime value is 336 hours (2 weeks). The default value is 168 hours (1 week).</p>

	Command or Action	Purpose
Step 10	lifetime enrollment-request <i>time</i> Example: Router (cs-server)# lifetime enrollment-request 888	(Optional) Specifies how long an enrollment request should stay in the enrollment database before being removed. Maximum lifetime is 1000 hours.
Step 11	cdp-url <i>url</i> Example: Router (cs-server)# cdp-url http://my-cdp.company.com	(Optional) Defines the CDP location to be used in the certificates that are issued by the certificate server. <ul style="list-style-type: none"> The URL must be an HTTP URL. If you have PKI clients that are not running Cisco IOS software and that do not support a SCEP GetCRL request, use the following URL format: <pre>http://server.company.com/certEnroll/filename.crl</pre> Or, if your Cisco IOS certificate server is also configured as your CDP, use the following URL format <pre>http://cs-addr/cgi-bin/pkiclient.exe?operation=GetCRL</pre> where <i>cs-addr</i> is the location of the certificate server. <p>In order to force the parser to retain the embedded question mark within the specified location, enter Ctrl-v prior to the question mark. If this action is not taken, CRL retrieval via HTTP will return an error message.</p> <p>Note Although this command is optional, it is strongly recommended for any deployment scenario.</p>
Step 12	no shutdown Example: Router (cs-server)# no shutdown	Enables the certificate server. You should issue this command only after you have completely configured your certificate server.

Examples

The following example shows how to configure a CDP location where the PKI clients do not support SCEP GetCRL requests:

```
Router(config)# crypto pki server aaa
Router(cs-server)# database level minimum
Router(cs-server)# database url tftp://10.1.1.1/username1/
Router(cs-server)# issuer-name CN=aaa
Router(cs-server)# cdp-url http://server.company.com/certEnroll/aaa.crl
```

After a certificate server has been enabled on a router, the **show crypto pki server** command displays the following output:

```
Router# show crypto pki server

Certificate Server status:enabled, configured
Granting mode is:manual
Last certificate issued serial number:0x1
CA certificate expiration timer:19:31:15 PST Nov 17 2006
CRL NextUpdate timer:19:31:15 PST Nov 25 2003
Current storage dir:nvram:
Database Level:Minimum - no cert data written to storage
```

Working with Automatic CA Certificate Rollover

This section describes different methods of initiating automatic CA certificate rollover on the server and obtaining rollover certificates. Use the following tasks as appropriate:

- [Starting Automated CA Certificate Rollover Immediately, page 28](#)
- [Requesting a Certificate Server Client's Rollover Certificate, page 28](#)
- [Exporting a CA Rollover Certificate, page 29](#)

Starting Automated CA Certificate Rollover Immediately

Use this task to initiate the automated CA certificate rollover process immediately on your root CA server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki server *cs-label* [rollover [cancel]]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki server <i>cs-label</i> [rollover [cancel]] Example: Router(config)# crypto pki server mycs rollover	Immediately starts the CA certificate rollover process by generating a shadow CA certificate. To delete the CA certificate rollover certificate and keys, use the cancel keyword.

Requesting a Certificate Server Client's Rollover Certificate

Use this task to request a certificate server client's rollover certificate.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki server *cs-label* [rollover request pkcs10 terminal]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki server cs-label [rollover request pkcs10 terminal] Example: Router(config)# crypto pki server mycs rollover request pkcs10 terminal	Requests a client rollover certificate from the server.

Examples

The following example shows a rollover certificate request being inputted into the server:

```
Router# crypto pki server mycs rollover request pkcs10 terminal

% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.

% End with a blank line or "quit" on a line by itself.

-----BEGIN CERTIFICATE REQUEST-----

MIIBUTCBuwIBADASMRawDgYDVQQDEwdOZXdsb290MIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDMHeev1ERSs320zbLQQk+3lhV/R2HpYQ/im6uT1jkJf5iy0UPR
wF/Xl6yUNmG+ObiGiW9fsASF0nxZw+fO7d2X2yh1PakfvF2wbP27C/sgJNOw9uPf
sBxEc40Xe0d5FMh0YKOSASHfZYKOflnyQR2Drmm2x/33QGo15QyRvjkeWQIDAQAB
oAAwDQYJKoZIhvcNAQEEBQADgYEALM90r4d79X6vxhD0qjuYJXfBCOvv4FNyFsjr
aBS/y6CnNVYySF8UBUohXYIGTWf4I4+sJ6i8gYfoFUW1/L82djs18TLrUr6wpCOs
RqfAfps7HW1e4cizOfjAUU+C7lNcobCAhwF1o6q2nIEjpQ/2yfk907sb3SCJZBfe
eW3tyCo=

-----END CERTIFICATE REQUEST-----
```

Exporting a CA Rollover Certificate

Use this task to export a CA rollover certificate.

SUMMARY STEPS

1. enable
2. configure terminal
3. crypto pki export trustpoint pem {terminal | url url} [rollover]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki export trustpoint pem {terminal url url} [rollover] Example: Router(config)# crypto pki export mycs pem terminal rollover	Exports a CA shadow certificate.

Maintaining, Verifying, and Troubleshooting the Certificate Server, Certificates, and the CA

Use the tasks in this section to help maintain, verify, and troubleshoot the certificate server, certificates and the CA as appropriate:

- [Managing the Enrollment Request Database, page 30](#)
- [Removing Enrollment Requests from the Enrollment Request Database: Examples, page 38](#)
- [Deleting a Certificate Server, page 33](#)
- [Verifying and Troubleshooting Certificate Server and CA Status, page 34](#)
- [Verifying CA Certificate Information, page 34](#)

Managing the Enrollment Request Database

SCEP supports two client authentication mechanisms—manual and preshared key. Manual enrollment requires the administrator at the CA server to specifically authorize the enrollment requests; enrollment using preshared keys allows the administrator to preauthorize enrollment requests by generating a one-time password (OTP).

Use any of the optional steps within this task to help manage the enrollment request database by performing functions such as specifying enrollment processing parameters that are to be used by SCEP and by controlling the run-time behavior or the certificate server.

SUMMARY STEPS

1. **enable**
2. **crypto pki server *cs-label* grant {all | *req-id*}**
3. **crypto pki server *cs-label* reject {all | *req-id*}**
4. **crypto pki server *cs-label* password generate [*minutes*]**

5. **crypto pki server** *cs-label* **revoke** *certificate-serial-number*
6. **crypto pki server** *cs-label* **request pkcs10** {*url* | **terminal**} [**base64** | **pem**]
7. **crypto pki server** *cs-label* **info** **crl**
8. **crypto pki server** *cs-label* **info** **requests**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	crypto pki server <i>cs-label</i> grant { all <i>req-id</i> } Example: Router# crypto pki server mycs grant all	Grants all or specific SCEP requests.
Step 3	crypto pki server <i>cs-label</i> reject { all <i>req-id</i> } Router# crypto pki server mycs reject all	Rejects all or specific SCEP requests.
Step 4	crypto pki server <i>cs-label</i> password generate [<i>minutes</i>] Example: Router# crypto pki server mycs password generate 75	Generates a OTP for SCEP requests. <ul style="list-style-type: none"> <i>minutes</i>—Length of time, in minutes, that the password is valid. Valid values range from 1 to 1440 minutes. The default is 60 minutes. Note Only one OTP is valid at a time; if a second OTP is generated, the previous OTP is no longer valid.
Step 5	crypto pki server <i>cs-label</i> revoke <i>certificate-serial-number</i> Example: Router# crypto pki server mycs revoke 3	Revokes a certificate on the basis of its serial number. <ul style="list-style-type: none"> <i>certificate-serial-number</i>—One of the following options: <ul style="list-style-type: none"> A string with a leading 0x, which is treated as a hexadecimal value A string with a leading 0 and no x, which is treated as octal All other strings, which are treated as decimal

	Command or Action	Purpose
Step 6	<pre>crypto pki server cs-label request pkcs10 {url terminal} [base64 pem]</pre> <p>Example: Router# crypto pki server mycs request pkcs10 terminal pem</p>	<p>Manually adds either a base64-encoded or PEM-formatted PKCS10 certificate enrollment request to the request database.</p> <p>After the certificate is granted, it will be displayed on the console terminal using base64 encoding.</p> <ul style="list-style-type: none"> • pem—Specifies the certificate will be returned <i>with</i> PEM headers automatically added to the certificate after the certificate is granted, regardless of whether PEM headers were used in the request. • base64—Specifies the certificate will be returned <i>without</i> privacy-enhanced mail (PEM) headers, regardless of whether PEM headers were used in the request.
Step 7	<pre>crypto pki server cs-label info crl</pre> <p>Example: Router# crypto pki server mycs info crl</p>	Displays information regarding the status of the current CRL.
Step 8	<pre>crypto pki server cs-label info requests</pre> <p>Example: Router# crypto pki server mycs info requests</p>	Displays all outstanding certificate enrollment requests.

Removing Requests from the Enrollment Request Database

After the certificate server receives an enrollment request, the server can leave the request in a pending state, reject it, or grant it. The request stays in the enrollment request database for 1 week until the client polls the certificate server for the result of the request. If the client exits and never polls the certificate server, you can remove either individual requests or all requests from the database.

Use this task to remove requests from the database and allow the server to be returned to a clean slate with respect to the keys and transaction IDs. Also, you can use this task to help troubleshoot a SCEP client that may not be behaving properly.

SUMMARY STEPS

1. **enable**
2. **crypto pki server cs-label remove {all | req-id}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	crypto pki server <i>cs-label</i> remove {all <i>req-id</i>} Example: Router# crypto pki server mycs remove 15	Removes enrollment requests from the enrollment request database.

Deleting a Certificate Server

Users can delete a certificate server from the PKI configuration if they no longer want it on the configuration. Typically, a subordinate certificate server or an RA is being deleted. However, users may delete a root certificate server if they are moving it to another device via the archived RSA keys.

Perform this task to delete a certificate server from your PKI configuration.



Note

When a certificate server is deleted, the associated trustpoint and key are also deleted.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no crypto pki server *cs-label***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	no crypto pki server <i>cs-label</i> Example: Router (config)# no crypto pki server mycs	Deletes a certificate server and associated trustpoint and key.

Verifying and Troubleshooting Certificate Server and CA Status

Use any of the following optional steps to verify the status of the certificate server or the CA.

SUMMARY STEPS

1. **enable**
2. **debug crypto pki server**
3. **dir filesystem:**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	debug crypto pki server Example: Router# debug crypto pki server	Enables debugging for a crypto PKI certificate server. <ul style="list-style-type: none">• This command can be used for monitoring the progress of an enrollment and for troubleshooting if the certificate server fails to respond or if the certificate server has trouble handling the request that has been configured.
Step 3	dir filesystem: Example: Router# dir slot0:	Displays a list of files on a file system. <ul style="list-style-type: none">• This command can be used to verify the certificate server autoarchived file if the database url command was entered to point to a local file system. You should be able to at least see “<i>cs-label.ser</i>” and “<i>cs-label.crl</i>” files in the database.

Verifying CA Certificate Information

To obtain information relating to the CA certificates including the certificate server rollover process, rollover certificates, and timers, you may use any of the following commands.



Note

These commands are not exclusive to shadow certificate information. If no shadow certificate exists, the following commands will simply display the active certificate information.

SUMMARY STEPS

1. **crypto pki certificate chain** *name*
2. **crypto pki server** *cs-label* **info requests**
3. **show crypto pki certificates**
4. **show crypto pki server**
5. **show crypto pki trustpoints**

DETAILED STEPS

- Step 1** The **crypto pki certificate chain** command can be used to view the certificate chain details and to distinguish the current active certificate from the rollover certificate in the certificate chain. The following example shows a certificate chain with an active CA certificate and a shadow, or rollover, certificate:

```
Router(config)# crypto pki certificate chain mica

certificate 06
certificate ca 01
! This is the peer's shadow PKI certificate.
certificate rollover 0B
! This is the CA shadow PKI certificate
certificate rollover ca 0A
```

- Step 2** The **crypto pki server info requests** command displays all outstanding certificate enrollment requests. The following example shows the output for shadow PKI certificate information requests:

```
Router# crypto pki server myca info requests

Enrollment Request Database:
RA certificate requests:

  ReqID  State      Fingerprint                               SubjectName
-----
RA rollover certificate requests:

  ReqID  State      Fingerprint                               SubjectName
-----

Router certificates requests:

  ReqID  State      Fingerprint                               SubjectName
-----
1       pending   A426AF07FE3A4BB69062E0E47198E5BF hostname=client

Router rollover certificates requests:

  ReqID  State      Fingerprint                               SubjectName
-----
2       pending   B69062E0E47198E5BFA426AF07FE3A4B hostname=client
```

- Step 3** The **show crypto pki certificates** command displays information about your certificate, the certification authority certificate, shadow certificates, and any registration authority certificates. The following example displays the certificate of the router and the certificate of the CA. There is no shadow certificate available. A single, general-purpose RSA key pair was previously generated, and a certificate was requested but not received for that key pair. Note that the certificate status of the router shows “Pending.” After the router receives its certificate from the CA, the Status field changes to “Available” in the **show** output.

```
Router# show crypto pki certificates

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 192.0.2.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
```

```

Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000
CA Certificate
Status: Available
Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
Key Usage: Not Set

```

- Step 4** The **show crypto pki server** command displays the current state and configuration of the certificate server. The following example shows that the certificate server “routercs” has rollover configured. The CA auto-rollover time has occurred and the rollover, or shadow, PKI certificate is available. The status shows the rollover certificate fingerprint and rollover CA certificate expiration timer information.

```

Router# show crypto pki server

Certificate Server routercs:
  Status: enabled, configured
  Issuer name: CN=walnutcs
  CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
  Granting mode is: auto
  Last certificate issued serial number: 0x7
  CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
  CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
  Current storage dir: nvram:
  Database Level: Minimum - no cert data written to storage
Rollover status: available for rollover
  Rollover CA cert fingerprint: 6AAF5944 74227A5B 23DF3E52 9A7F1FEF
  Rollover CA certificate expiration timer: 22:10:29 GMT Jan 29 2017

```

- Step 5** The **show crypto pki trustpoints** command displays the trustpoints that are configured in the router. The following output shows that a shadow CA certificate is available and shows the SCEP capabilities reported during the last enrollment operation:

```

Router# show crypto pki trustpoints

Trustpoint vpn:
  Subject Name:
  cn=Cisco SSL CA
  o=Cisco Systems
  Serial Number: 0FFEBCDC1B6F6D9D0EA7875875E4C695
  Certificate configured.
  Rollover certificate configured.
  Enrollment Protocol:
  SCEPv1, PKI Rollover

```

Configuration Examples for Using a Certificate Server

This section contains the following configuration examples:

- [Configuring Specific Storage and Publication Locations: Examples, page 37](#)
- [Removing Enrollment Requests from the Enrollment Request Database: Examples, page 38](#)
- [Autoarchiving the Certificate Server Root Keys: Examples, page 39](#)
- [Restoring a Certificate Server from Certificate Server Backup Files: Examples, page 41](#)
- [Subordinate Certificate Server: Example, page 43](#)
- [RA Mode Certificate Server: Example, page 45](#)
- [Enabling CA Certificate Rollover to Start Immediately: Example, page 47](#)

Configuring Specific Storage and Publication Locations: Examples

The following example shows the configuration of a minimal local file system, so that the certificate server can respond quickly to certificate requests. The .ser and .crl files are stored on the local Cisco IOS file system for fast access, and a copy of all of the .crt files are published to a remote location for long-term logging.

```
crypto pki server myserver
  !Pick your database level.
  database level minimum
  !Specify a location for the .crt files that is different than the default local
  !Cisco IOS file system.
  database url crt publish http://url username user1 password secret
```



Note

Free space on the local file system should be monitored, in case the .crl file becomes too large.

The following example shows the configuration of a primary storage location for critical files, a specific storage location for the critical file serial number file, the main certificate server database file, and a password protected file publication location for the CRL file:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://cs-db.company.com
!
% Server database url was changed. You need to move the
% existing database to the new location.
!
Router(cs-server)# database url ser nvram:
Router(cs-server)# database url crt publish ftp://crl.company.com username myname password
mypassword
Router(cs-server)# end
```

The following output displays the specified primary storage location and critical file storage locations specified:

```
Router# show
```

```
Sep  3 20:19:34.216: %SYS-5-CONFIG_I: Configured from console by user on console
```

```
Router# show crypto pki server
```

```
Certificate Server mycs:
  Status: disabled
  Server's configuration is unlocked (enter "no shut" to lock it)
  Issuer name: CN=mycs
  CA cert fingerprint: -Not found-
  Granting mode is: manual
  Last certificate issued serial number: 0x0
  CA certificate expiration timer: 00:00:00 GMT Jan 1 1970
  CRL not present.
  Current primary storage dir: ftp://cs-db.company.com
  Current storage dir for .ser files: nvram:
  Database Level: Minimum - no cert data written to storage
The following output displays all storage and publication locations. The serial number file (.ser) is stored in NVRAM. The CRL file will be published to ftp://crl.company.com with a username and password. All other critical files will be stored to the primary location, ftp://cs-db.company.com.
```

```
Router# show running-config
```

```
section crypto pki server
crypto pki server mycs shutdown database url ftp://cs-db.company.com
```

```

database url crl publish ftp://crl.company.com username myname password 7
12141C0713181F13253920
database url ser nvram:
Router#

```

Removing Enrollment Requests from the Enrollment Request Database: Examples

The following examples show both the enrollment requests that are currently in the enrollment request database and the result after one of the enrollment requests has been removed from the database.

Enrollment Request Currently in the Enrollment Request Database

The following example shows that the **crypto pki server info requests** command has been used to display the enrollment requests that are currently in the Enrollment Request Database:

```
Router# crypto pki server myserver info requests
```

Enrollment Request Database:

```

RA certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----

```

```

Router certificates requests:
ReqID      State      Fingerprint                               SubjectName
-----
2          pending  1B07F3021DAAB0F19F35DA25D01D8567       hostname=host1.company.com
1          denied   5322459D2DC70B3F8EF3D03A795CF636       hostname=host2.company.com

```

crypto pki server remove Command Used to Remove One Enrollment Request

The following example shows that the **crypto pki server remove** command has been used to remove Enrollment Request 1:

```
Router# crypto pki server myserver remove 1
```

Enrollment Request Database After the Removal of One Enrollment Request

The following example shows the result of the removal of Enrollment Request 1 from the Enrollment Request Database:

```
Router# crypto pki server mycs info requests
```

Enrollment Request Database:

```

RA certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----

```

```

Router certificates requests:
ReqID      State      Fingerprint                               SubjectName
-----
2          pending  1B07F3021DAAB0F19F35DA25D01D8567       hostname=host1.company.com

```


Autoarchiving the Certificate Server Root Keys: Examples

The following output configurations and examples show what you might see if the **database archive** command has not been configured (that is, configured using the default value); if the **database archive** command has been configured to set the CA certificate and CA key archive format as PEM, without configuring a password; and if the **database archive** command has been configured to set the CA certificate and CA key archive format as PKCS12, with a password configured. The last example is sample content of a PEM-formatted archive file.

database archive Command Not Configured



Note

The default is PKCS12, and the prompt for the password appears after the **no shutdown** command has been issued.

```
Router (config)# crypto pki server myserver
Router (cs-server)# no shutdown

% Generating 1024 bit RSA keys ...[OK]
% Ready to generate the CA certificate.
%Some server settings cannot be changed after CA certificate generation.

Are you sure you want to do this? [yes/no]: y
% Exporting Certificate Server signing certificate and keys...
! Note the next two lines, which are asking for a password.
% Please enter a passphrase to protect the private key.
Password:
% Certificate Server enabled.
Router (cs-server)# end

Router# dir nvram:

Directory of nvram:/

 125  -rw-          1693          <no date>  startup-config
 126  ----           5          <no date>  private-config
   1  -rw-           32          <no date>  myserver.ser
   2  -rw-          214          <no date>  myserver.crl
! Note the next line, which indicates PKCS12 format.
   3  -rw-         1499          <no date>  myserver.p12
```

database archive Command and pem Keyword Configured



Note

The prompt for the password appears after the **no shutdown** command has been issued.

```
Router (config)# crypto pki server myserver
Router (cs-server)# database archive pem
Router (cs-server)# no shutdown

% Generating 1024 bit RSA keys ...[OK]
% Ready to generate the CA certificate.
%Some server settings cannot be changed after CA certificate generation.

Are you sure you want to do this? [yes/no]: y
% Exporting Certificate Server signing certificate and keys...
!Note the next two lines, which are asking for a password.
% Please enter a passphrase to protect the private key.
Password:
```

```
% Certificate Server enabled.
Router (cs-server)# end

Router# dir nvram

Directory of nvram:/

 125  -rw-          1693          <no date>  startup-config
 126  ----           5          <no date>  private-config
   1  -rw-          32          <no date>  myserver.ser
   2  -rw-         214          <no date>  myserver.crl
! Note the next line showing that the format is PEM.
   3  -rw-         1705          <no date>  myserver.pem
```

database archive Command and pkcs12 Keyword (and Password) Configured



Note

When the password is entered, it will be encrypted. However, it is recommended that you remove the password from the configuration after the archive has finished.

```
Router (config)# crypto pki server myserver
Router (cs-server)# database archive pkcs12 password cisco123
Router (cs-server)# no shutdown

% Generating 1024 bit RSA keys ...[OK]
% Ready to generate the CA certificate.
% Some server settings cannot be changed after CA certificate generation.

Are you sure you want to do this? [yes/no]: y
% Exporting Certificate Server signing certificate and keys...
! Note that you are not being prompted for a password.
% Certificate Server enabled.
Router (cs-server)# end
Router# dir nvram:
Directory of nvram:/

 125  -rw-          1693          <no date>  startup-config
 126  ----           5          <no date>  private-config
   1  -rw-          32          <no date>  myserver.ser
   2  -rw-         214          <no date>  myserver.crl
! Note that the next line indicates that the format is PKCS12.
   3  -rw-         1499          <no date>  myserver.p12
```

PEM-Formatted Archive

The following sample output shows that autoarchiving has been configured in PEM file format. The archive consists of the CA certificate and the CA private key. To restore the certificate server using the backup, you would have to import the PEM-formatted CA certificate and CA key individually.



Note

In addition to the CA certificate and CA key archive files, you should also back up the serial file (.ser) and the CRL file (.crl) regularly. The serial file and the CRL file are both critical for CA operation if you need to restore your certificate server.

```
Router# more nvram:mycs.pem

-----BEGIN CERTIFICATE-----
MIIB9zCCAWCgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDgyNzAyMzI0N1oXDTA3MDgyNzAyMzI0N1owDzENMAAGAlUEAxMEbXlj
czCBNzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1lZpKP4nGDJHgPkpYSkix7ld
nr23aMlZ9Kz5oo/qTBxeZ8mujpjYcZ0T8AZvoOiCuDnYMl796ZwpkMgjz1aZZbL+
```

```
BtuVvllsEOfhC+u/Ol/vxfGG5xpshoz/F5J3xdg5ZZuWwuIDAUYu9+QbI5feuG04
Z/BiPIb4AmGTP4B2MM0CAwEAAAnjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAYYwHwYDVR0jBBgwFoAUKi/cuK6wkz+ZswVtb06vUJboEeEwHQYDVR0O
BBYEFcov3LiusJM/mbMFbW9Or1CW6BHhMA0GCSqGSIb3DQEBBAUAA4GBAKLOmoE2
4+NeOKEXMCXG1jcohK7O2HrkFfl/vpK0+q92PTnMUFhxL0qI8pWIq5CCgC7heace
OrTv2zcUAoH4rzx3Rc2USIxkDokWWQMLujsMm/SLIeHit0G5uj//GCcbgK20MAW6
ymf7+Tmb1SFljWzstoUXC2hLnsJIMq/KffaD
-----END CERTIFICATE-----
```

!The private key is protected by the password that is configured in "database archive pem password pwd" or that is entered when you are prompted for the password.

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4, ENCRYPTED

DEK-Info: DES-EDE3-CBC,106CE91FFD0A075E

```
zyiFC8rKv8Cs+IKsQG2QpsVpVDBHqZqBSM4D528bvZv7jzr6WuHj8E6zo+6G8R/A
zjsfTALo+e+ZDg7KMzbryHARvjSkbqFdOMLlVIYBhCeSElKsskWB6chOuyPHJInW
JwC5YzZdZwOqcyLBP/xOYXcvjzzNfPAXZzN12VR8vWDNq/kHT+3Lplc8hY++ABMI
M+C9FB3dpNZu501BZCJg46bqbkuLaCCmScIDaVt0zDFZwWTSufiemmnXZBG4xS8
t5t+FEhmSfv8DAmwg4f/KVRFtm10phUArcLxQ038A10W5YHHORdACnuzVUvHgc07
VT4XUTj07qMhmJgFNWylpu49fbdS2NnOn5IoIyAq51k1KUPrz/WABWiCvLMy1GnZ
kyMCWoaMtG5/vdx74BBCj09yRZJnLmLi6SDofjCNTDhfMFEVg4LsSWCd41P9OP8
0MghP1D5VIx6PbMnwKWW121pBbCCdesFRGHjZD2dOu96kHD7ItErX34CC8W04aG4
b7DLktUu6WNV6M8g3CAqJiC0V8ATlp+kvdHZVXovgND5IU00Jpsj0HhGzKAGpOY
KTGTUekUboISjVVkI6efp1v06temVL3Txg3KGhzWMJGrq1snghE0KnV8tkddv/9N
d/t1l+we9mrccTq50WNDnKEi/cwHI/0PKXg+NDNH3k3QGpAprsqGQmMPdqc5ut0P
86i4cF9078QwWg4Tpay3uqNH1Zz6UN0tcarVvNmDupFESUxYw10qJrrEYVRadu74
rKAU4Ey4xkAftB2kuqvr21Av/L+jne4kkGIozYdB+p/M98pQRgkYyg==
-----END RSA PRIVATE KEY-----
```

Restoring a Certificate Server from Certificate Server Backup Files: Examples

The following example shows that restoration is from a PKCS12 archive and that the database URL is NVRAM (the default).

```
Router# copy tftp://192.0.2.71/backup.ser nvram:mycs.ser
Destination filename [mycs.ser]?
```

32 bytes copied in 1.320 secs (24 bytes/sec)

```
Router# copy tftp://192.0.2.71/backup.crl nvram:mycs.crl
Destination filename [mycs.crl]?
```

214 bytes copied in 1.324 secs (162 bytes/sec)

```
Router# configure terminal
```

```
Router (config)# crypto pki import mycs pkcs12 tftp://192.0.2.71/backup.p12 cisco123
Source filename [backup.p12]?
```

CRYPTO_PKI: Imported PKCS12 file successfully.

```
Router (config)# crypto pki server mycs
```

! fill in any certificate server configuration here

```
Router (cs-server)# no shutdown
```

% Certificate Server enabled.

```
Router (cs-server)# end
```

```
Router# show crypto pki server
```

Certificate Server mycs:

Status: enabled

Server's current state: enabled

Issuer name: CN=mycs

CA cert fingerprint: 34885330 B13EAD45 196DA461 B43E813F

Granting mode is: manual

Last certificate issued serial number: 0x1

```

CA certificate expiration timer: 01:49:13 GMT Aug 28 2007
CRL NextUpdate timer: 01:49:16 GMT Sep 4 2004
Current storage dir: nvram:
Database Level: Minimum - no cert data written to storage

```

The following example shows that restoration is from a PEM archive and that the database URL is flash:

```

Router# copy tftp://192.0.2.71/backup.ser flash:mycs.ser
Destination filename [mycs.ser]?
32 bytes copied in 1.320 secs (24 bytes/sec)
Router# copy tftp://192.0.2.71/backup.crl flash:mycs.crl
Destination filename [mycs.crl]?
214 bytes copied in 1.324 secs (162 bytes/sec)
Router# configure terminal
! Because CA cert has Digital Signature usage, you need to import using the "usage-keys"
keyword
Router (config)# crypto ca import mycs pem usage-keys terminal cisco123
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
! Paste the CA cert from .pem archive.
-----BEGIN CERTIFICATE-----
MIIB9zCCAwwGAgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDkwMjIxMDI1N1oXDTA3MDkwMjIxMDI1N1owDzENMAAGA1UEAxMEbXl1j
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGykCgYEAuGnnDXJbpdDQwCuKGS5Zg2rc
K7ZJauSUotTmWYQvNx+ZmWrUs5/j9Ee5FV2YonirGBQ9mc6u163kNlrIPFck062L
GpahBhNmKDgod1o2PHTnRlZpEZNDIqU2D3hACgByxPjY4vUnccV36ewLnQnYpp8
szEu7PYTJr5dU5ltAekCAwEAAANjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAAYwHwYDVR0jBBgwFoAUaEEQwYKCQ1dm9+wLYBKRTlZxaDIwHQYDVR0O
BBYEFGBBEMGCGkNXZvfcS2ASKU5c8WgyMA0GCSqSIB3DQEBBAUAA4GBAHyhiV2C
mH+vsWkbJRA1FzZk8ttu9s5kwqG0dXp25QRUWsgLr9nsKPNdVKt3P7p0A/KochHe
eNiygIv+hDQ3FVnzsNv983le605jvAPxc17RO1BbfNhhqEWMSXdnjHocUy7XerCo
+bdPcUf/eCiZueH/BEy/SZhd7yovzn2cdzBN
-----END CERTIFICATE-----

% Enter PEM-formatted encrypted private SIGNATURE key.
% End with "quit" on a line by itself.
! Paste the CA private key from .pem archive.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC,5053DC842B04612A

1Cn1F5Pqvd0zp2NLZ7iosxzTy6nDeXPPNyJpXB5q+V29IuY8Apb6TlJCU7YrsEB/
nBTk7K76DCeGPlLpcuyEI171QmkQJ2gA0QhC0LrRo09WrINVH+b4So/y7nffZkVb
p2yDpZwqoJ8cmRH94Tie0YmzBtEh6ayOud1lZ53qbrsCnfSEwszt1xrWlMKrFZrk
/fTy6loHzGFz13BDj4r5gBecExwcPp74ldHO+Ld4Nc9egG8BYkeBCsZZOQNvHXLN
I0tODos6hP915zb6OrZFVYv0NK6grTBO9D8hjNZ3U79jJzsSP7UNzIYHNTzRjIAyu
i56Oy/iHvkCSNUIK6zeIJQnW4bSoM1BqrbVPwHU6QaXUqlNzZ8SDtw7ZRZ/rHuiD
RTJMPbKquAzeuBss1132OaAUJRStjPXgyZTUbc+cWb6zATNws2yijPDTR6sRHoQL
47wHMr2Yj80VZGgkCSLAKL88ACz9TfUiVFhtf16xMC2yuF1+WRk1XfF5VtWe5Zer
3Fn1DcBmlF7086XUkiSHP4EV0cI6n5ZMzVLx0XAUTdA1lgD94y1V+6p9PcQHLYQA
pGRmj51lSfw90aLafgCTbRbmC0ChIqHy91UFa1ub0130+yu7LsLGRlPmJ9NE61JR
bjRh1UXItRYWY7C4M3m/0wz6fmVQNSumJM08RHq61UB3olZigGIz1ZkoaESrLG0p
qq2AENFemCPF0uhyVS2humMHjWuRr+jedfc/IM17sLEgAdqCVCfV3RZVEaNXBud1
4QjkuTrwaTcRXVfbtrVioT/puyVULpA7+k7w+F5TZwUV08mwvUEqDw==
-----END RSA PRIVATE KEY-----
quit
% Enter PEM-formatted SIGNATURE certificate.
% End with a blank line or "quit" on a line by itself.
! Paste the CA cert from .pem archive again.
-----BEGIN CERTIFICATE-----
MIIB9zCCAwwGAgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDkwMjIxMDI1N1oXDTA3MDkwMjIxMDI1N1owDzENMAAGA1UEAxMEbXl1j
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGykCgYEAuGnnDXJbpdDQwCuKGS5Zg2rc
K7ZJauSUotTmWYQvNx+ZmWrUs5/j9Ee5FV2YonirGBQ9mc6u163kNlrIPFck062L

```

```
GpahBhNmKDgod1o2PHTnRlZpEZNDIqU2D3hACgByxPjrY4vUnccV36ewLnQnYpp8
szEu7PYTJr5dU5ltAekCAwEAAANjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAYYwHwYDVR0jBBgwFoAUaEEQwYKCQ1dm9+wLYBKRTlzxADIwHQYDVR0O
BBYEFghBEMGCgkNXZvfsC2AskU5c8WgyMA0GCSqGSIb3DQEBAUAA4GBAHyhiV2C
mH+vswkBjRA1Fzzk8ttu9s5kwqG0dXp25QRUWsGlr9nsKPNdVKt3P7p0A/KochHe
eNiygivi+hdQ3FVnzsNv9831e605jvAPxc17R01BbfNhgqEWMsXdnjH0cUy7XerCo
+bdPcUf/eCiZueH/BEy/SZhD7yovzn2cdzBN
-----END CERTIFICATE-----

% Enter PEM-formatted encrypted private ENCRYPTION key.
% End with "quit" on a line by itself.
! Because the CA cert only has Digital Signature usage, skip the encryption part.
quit
% PEM files import succeeded.
Router (config)# crypto pki server mycs
Router (cs-server)# database url flash:
! Fill in any certificate server configuration here.
Router (cs-server)# no shutdown
% Certificate Server enabled.
Router (cs-server)# end

Router # show crypto pki server

Certificate Server mycs:
  Status: enabled
  Server's current state: enabled
  Issuer name: CN=mycs
  CA cert fingerprint: F04C2B75 E0243FBC 19806219 B1D77412
  Granting mode is: manual
  Last certificate issued serial number: 0x2
  CA certificate expiration timer: 21:02:55 GMT Sep 2 2007
  CRL NextUpdate timer: 21:02:58 GMT Sep 9 2004
  Current storage dir: flash:
  Database Level: Minimum - no cert data written to storage
```

Subordinate Certificate Server: Example

The following configuration and output is typical of what you might see after configuring a subordinate certificate server:

```
Router (config)# crypto pki trustpoint sub
Router (ca-trustpoint)# enrollment url http://192.0.2.6
Router (ca-trustpoint)# exit

Router (config)# crypto pki server sub
Router (cs-server)# mode sub-cs
Router (ca-server)# no shutdown

%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:
Jan  6 22:32:22.698: CRYPTO_CS: enter FSM: input state initial, input signal no shut

Re-enter password:
% Generating 1024 bit RSA keys ...
Jan  6 22:32:30.302: CRYPTO_CS: starting enabling checks
Jan  6 22:32:30.306: CRYPTO_CS: key 'sub' does not exist; generated automatically [OK]

Jan  6 22:32:39.810: %SSH-5-ENABLED: SSH 1.99 has been enabled
Certificate has the following attributes:
  Fingerprint MD5: 328ACC02 52B25DB8 22F8F104 B6055B5B
```

```

Fingerprint SHA1: 02FD799D DD40C7A8 61DC53AB 1E89A3EA 2A729EE2

% Do you accept this certificate? [yes/no]:
Jan  6 22:32:44.830: CRYPTO_CS: nvram filesystem
Jan  6 22:32:44.922: CRYPTO_CS: serial number 0x1 written.
Jan  6 22:32:46.798: CRYPTO_CS: created a new serial file.
Jan  6 22:32:46.798: CRYPTO_CS: authenticating the CA 'sub'y
Trustpoint CA certificate accepted.%

% Certificate request sent to Certificate Authority

% Enrollment in progress...
Router (cs-server)#
Jan  6 22:33:30.562: CRYPTO_CS: Publishing 213 bytes to crl file nvram:sub.crl
Jan  6 22:33:32.450: CRYPTO_CS: enrolling the server's trustpoint 'sub'
Jan  6 22:33:32.454: CRYPTO_CS: exit FSM: new state check failed
Jan  6 22:33:32.454: CRYPTO_CS: cs config has been locked
Jan  6 22:33:33.118: CRYPTO_PKI: Certificate Request Fingerprint MD5: CED89E5F 53B9C60E
> AA123413 CDDAD964
Jan  6 22:33:33.118: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 70787C76 ACD7E67F
7D2C8B23 98CB10E7 718E84B1
% Exporting Certificate Server signing certificate and keys...

Jan  6 22:34:53.839: %PKI-6-CERTRET: Certificate received from Certificate Authority
Jan  6 22:34:53.843: CRYPTO_CS: enter FSM: input state check failed, input signal cert
configured
Jan  6 22:34:53.843: CRYPTO_CS: starting enabling checks
Jan  6 22:34:53.843: CRYPTO_CS: nvram filesystem
Jan  6 22:34:53.883: CRYPTO_CS: found existing serial file.
Jan  6 22:34:53.907: CRYPTO_CS: old router cert flag 0x4
Jan  6 22:34:53.907: CRYPTO_CS: new router cert flag 0x44
Jan  6 22:34:56.511: CRYPTO_CS: DB version
Jan  6 22:34:56.511: CRYPTO_CS: last issued serial number is 0x1
Jan  6 22:34:56.551: CRYPTO_CS: CRL file sub.crl exists.
Jan  6 22:34:56.551: CRYPTO_CS: Read 213 bytes from crl file sub.crl.
Jan  6 22:34:56.603: CRYPTO_CS: SCEP server started
Jan  6 22:34:56.603: CRYPTO_CS: exit FSM: new state enabled
Jan  6 22:34:56.603: CRYPTO_CS: cs config has been locked
Jan  6 22:35:02.359: CRYPTO_CS: enter FSM: input state enabled, input signal time set
Jan  6 22:35:02.359: CRYPTO_CS: exit FSM: new state enabled
Jan  6 22:35:02.359: CRYPTO_CS: cs config has been locked

```

Root Certificate Server Differentiation: Example

When issuing certificates, the root certificate server (or parent subordinate certificate server) will differentiate the certificate request from “Sub CA,” “RA,” and peer requests, as shown in the following sample output:

```

Router# crypto pki server server1 info req

Enrollment Request Database:
RA certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----
Subordinate CS certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----
1          pending    CB9977AD8A73B146D3221749999B0F66  hostname=host-subcs.company.com

```

```

RA certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----
Router certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----

```

Show Output for a Subordinate Certificate Server: Example

The following **show crypto pki server** command output indicates that a subordinate certificate server has been configured:

```

Router# show crypto pki server

Certificate Server sub:
  Status: enabled
  Server's configuration is locked (enter "shut" to unlock it)
  Issuer name: CN=sub
  CA cert fingerprint: 11B586EE 3B354F33 14A25DDD 7BD39187
  Server configured in subordinate server mode
  Upper CA cert fingerprint: 328ACC02 52B25DB8 22F8F104 B6055B5B
  Granting mode is: manual
  Last certificate issued serial number: 0x1
  CA certificate expiration timer: 22:33:44 GMT Jan 6 2006
  CRL NextUpdate timer: 22:33:29 GMT Jan 13 2005
  Current storage dir: nvram:
  Database Level: Minimum - no cert data written to storage

```

RA Mode Certificate Server: Example

The following output is typical of what you might see after having configured an RA mode certificate server:

```

Router-ra (config)# crypto pki trustpoint myra
Router-ra (ca-trustpoint)# enrollment url http://192.0.2.17
! Include "cn=ioscs RA" or "ou=ioscs RA" in the subject-name.
Router-ra (ca-trustpoint)# subject-name cn=myra, ou=ioscs RA, o=company, c=us
Router-ra (ca-trustpoint)# exit
Router-ra (config)# crypto pki server myra
Router-ra (cs-server)# mode ra
Router-ra (cs-server)# no shutdown
% Generating 1024 bit RSA keys ...[OK]

Certificate has the following attributes:
Fingerprint MD5: 32661452 0DDA3CE5 8723B469 09AB9E85
Fingerprint SHA1: 9785BBCE 6C67D27C C950E8D0 718C7A14 C0FE9C38
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Ready to request the CA certificate.
%Some server settings cannot be changed after the CA certificate has been requested.

Are you sure you want to do this? [yes/no]: yes
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

```

```

Password:
Re-enter password:

% The subject name in the certificate will include: cn=myra, ou=ioscs RA, o=company, c=us
% The subject name in the certificate will include: Router-ra.company.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.

% Enrollment in progress...
Router-ra (cs-server)#
Sep 15 22:32:40.197: CRYPTO_PKI: Certificate Request Fingerprint MD5: 82B41A76 AF4EC87D
AAF093CD 07747D3A
Sep 15 22:32:40.201: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 897CDF40 C6563EAA
0FED05F7 0115FD3A 4FFC5231
Sep 15 22:34:00.366: %PKI-6-CERTRET: Certificate received from Certificate Authority
Router-ra (cs-server)#
Router-ra(cs-server)# end

```

```
Router-ra# show crypto pki server
```

```

Certificate Server myra:
  Status: enabled
  Issuer name: CN=myra
  CA cert fingerprint: 32661452 0DDA3CE5 8723B469 09AB9E85
  ! Note that the certificate server is running in RA mode
  Server configured in RA mode
  RA cert fingerprint: C65F5724 0E63B3CC BE7AE016 BE0D34FE
  Granting mode is: manual
  Current storage dir: nvram:
  Database Level: Minimum - no cert data written to storage

```

The following output shows the enrollment request database of the issuing certificate server after the RA has been enabled:



Note

The RA certificate request is recognized by the issuing certificate server because "ou=ioscs RA" is listed in the subject name.

```

Router-ca# crypto pki server mycs info request
Enrollment Request Database:

Subordinate CA certificate requests:
ReqID  State      Fingerprint                               SubjectName
-----
! The request is identified as RA certificate request.
RA certificate requests:
ReqID  State      Fingerprint                               SubjectName
-----
12     pending   88F547A407FA0C90F97CDE8900A30CB0
hostname=Router-ra.company.com,cn=myra,ou=ioscs RA,o=company,c=us

```



```
Router certificates requests:
ReqID    State    Fingerprint                               SubjectName
-----
```

```
! Issue the RA certificate.
Router-ca# crypto pki server mycs grant 12
```

The following output shows that the issuing certificate server is configured to issue a certificate automatically if the request comes from an RA:

```
Router-ca(config)# crypto pki server mycs
Router-ca (cs-server)# grant ra-auto
% This will cause all certificate requests already authorized by known RAs to be
automatically granted.

Are you sure you want to do this? [yes/no]: yes
Router-ca (cs-server)# end
Router-ca# show crypto pki server

Certificate Server mycs:
  Status: enabled
  Server's current state: enabled
  Issuer name: CN=mycs
  CA cert fingerprint: 32661452 0DDA3CE5 8723B469 09AB9E85
  ! Note that the certificate server will issue certificate for requests from the RA.
  Granting mode is: auto for RA-authorized requests, manual otherwise
  Last certificate issued serial number: 0x2
  CA certificate expiration timer: 22:29:37 GMT Sep 15 2007
  CRL NextUpdate timer: 22:29:39 GMT Sep 22 2004
  Current storage dir: nvram:
  Database Level: Minimum - no cert data written to storage
```

The following example shows the configuration of “myra”, an RA server, configured to support automatic rollover from “myca”, the CA. After the RA server is configured, automatic granting of certificate reenrollment requests is enabled:

```
crypto pki trustpoint myra
  enrollment url http://myca
  subject-name ou=iosca RA
  rsakeypair myra
crypto pki server myra
  mode ra
  auto-rollover

crypto pki server mycs
  grant auto rollover ra-cert
  auto-rollover 25
```

Enabling CA Certificate Rollover to Start Immediately: Example

The following example shows how to enable automated CA certificate rollover on the server mycs with the **crypto pki server** command. The **show crypto pki server** command then shows the current state of the mycs server and that the rollover certificate is currently available for rollover.

```
Router(config)# crypto pki server mycs rollover

Jun 20 23:51:21.211:%PKI-4-NOSHADOWAUTOSAVE:Configuration was
modified. Issue "write memory" to save new IOS CA certificate

! The config has not been automatically saved because the config has been changed.
```

```
Router# show crypto pki server
```

```
Certificate Server mycs:
  Status:enabled
  Server's configuration is locked (enter "shut" to unlock it)
  Issuer name:CN=mycs
  CA cert fingerprint:E7A5FABA 5D7AA26C F2A9F7B3 03CE229A
  Granting mode is:manual
  Last certificate issued serial number:0x2
  CA certificate expiration timer:00:49:26 PDT Jun 20 2008
  CRL NextUpdate timer:00:49:29 PDT Jun 28 2005
  Current storage dir:nvram:
  Database Level:Minimum - no cert data written to storage
  Rollover status:available for rollover
  ! Rollover certificate is available for rollover.
  Rollover CA certificate fingerprint:9BD7A443 00A6DD74 E4D9ED5F B7931BE0
  Rollover CA certificate expiration time:00:49:26 PDT Jun 20 2011
  Auto-Rollover configured, overlap period 25 days
```

Where to Go Next

After the certificate server is successfully running, you can either begin enrolling clients via manual mechanisms (as explained in the module “Configuring Certificate Enrollment for a PKI”) or begin configuring SDP, which is a web-based enrollment interface, (as explained in the module “Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI.”)

Additional References

The following sections provide references related to Cisco IOS certificate server:

Related Topic	Document Title
USB Token RSA Operations: Using the RSA keys on a USB token for initial autoenrollment	“Configuring Certificate Enrollment for a PKI” chapter in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i> . See the “Configuring Certificate Servers” section.
USB Token RSA Operations: Benefits of using USB tokens	“Storing PKI Credentials” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i> .
Certificate server client certificate enrollment, autoenrollment, and automatic rollover	“Configuring Certificate Enrollment for a PKI” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i> .
Setting up and logging into a USB token	“Storing PKI Credentials” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i> .
Web-based certificate enrollment	“Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i> .
RSA keys in PEM formatted files	“Deploying RSA Keys Within a PKI” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i> .
Choosing a certificate revocation mechanism	“Configuring Authorization and Revocation of Certificates in a PKI” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i> .

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for the Cisco IOS Certificate Server

Table 4 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Implementing and Managing PKI Features Roadmap](#).”

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 4 Feature Information for the Cisco IOS Certificate Server

Feature Name	Releases	Feature Information
Cisco IOS USB Token PKI Enhancements—Phase 2	12.4(11)T	<p>This feature enhances USB token functionality by using the USB token as a cryptographic device. USB tokens may be used for RSA operations such as key generation, signing, and authentication.</p> <p>The following sections in this document provide information about this feature:</p> <ul style="list-style-type: none"> RSA Key Pair and Certificate of the Certificate Server Trustpoint of the Certificate Server Generating a Certificate Server RSA Key Pair <p>Note This document covers the use of using USB tokens for RSA operations during certificate server configuration.</p>
IOS Certificate Server (CS) Split Database	12.4(4)T	<p>This feature allows the user to set storage locations and publish locations for specific certificate server file types.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Certificate Server Database Configuring Certificate Server Functionality Configuring Specific Storage and Publication Locations: Examples <p>The following command was modified by this feature: database url</p>

Table 4 *Feature Information for the Cisco IOS Certificate Server (continued)*

Feature Name	Releases	Feature Information
Subordinate/RA Mode IOS Certificate Server (CS) Rollover	12.4(4)T	<p>This feature expands on Certificate Authority (CA) Key Rollover introduced in 12.4(2)T to allow CA certificate rollover for subordinate CAs and RA-mode CAs. This functionality allows the rollover expiring CA certificates and keys and to have these changes propagate through the PKI network without manual intervention.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Automatic CA Certificate and Key Rollover • Configuring Certificate Servers • RA Mode Certificate Server: Example <p>The following command was modified by this feature: grant auto rollover</p>
Certificate Authority (CA) Key Rollover	12.4(2)T	<p>This feature introduces the ability for root or subordinate CAs to roll over expiring CA certificates and keys and to have these changes propagate through the PKI network without manual intervention.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Automatic CA Certificate and Key Rollover • Configuring Certificate Servers • Working with Automatic CA Certificate Rollover • Enabling CA Certificate Rollover to Start Immediately: Example <p>The following commands were introduced or modified by this feature: auto-rollover, crypto pki certificate chain, crypto pki export pem, crypto pki server info request, crypto pki server, show crypto pki certificates, show crypto pki server, and show crypto pki trustpoint</p>
Cisco IOS Certificate Server	12.3(8)T	<p>This feature introduces support for the Cisco IOS certificate server, which offers users a CA that is directly integrated with Cisco IOS software to more easily deploy basic PKI networks.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About Cisco IOS Certificate Servers • How to Set Up and Deploy a Cisco IOS Certificate Server

Table 4 *Feature Information for the Cisco IOS Certificate Server (continued)*

Feature Name	Releases	Feature Information
The Certificate Server Auto Archive Enhancement ¹	12.3(11)T	<p>This enhancement enables the CA certificate and CA key to be backed up automatically just once after they are generated by the certificate server. As a result, it is not necessary to generate an exportable CA key if CA backup is desirable.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Certificate Enrollment Using a Certificate Server Configuring Certificate Server Functionality <p>The following commands were introduced by this feature: crypto pki server remote, database archive</p>
The Certificate Server Registration Authority (RA) Mode enhancement	12.3(7)T	<p>A certificate server can be configured to run in RA mode.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> Configuring a Certificate Server to Run in RA Mode <p>The following commands were introduced by this feature: grant ra-auto, lifetime enrollment-requests</p>
PKI Status ¹	12.3(11)T	<p>This enhancement provides a quick snapshot of current trustpoint status.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none"> Maintaining, Verifying, and Troubleshooting the Certificate Server, Certificates, and the CA <p>The following command was modified by this enhancement: show crypto pki trustpoints</p>
Subordinate Certificate Server ¹	12.3(14)T	<p>This enhancement allows you to configure a subordinate certificate server to grant all or certain SCEP or manual certificate requests.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none"> Configuring a Subordinate Certificate Server <p>The following command was introduced by this enhancement: mode sub-cs</p>
Cisco IOS Certificate Server	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Trustpoint CLI	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

1. This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005–2009 Cisco Systems, Inc. All rights reserved.



Storing PKI Credentials

First Published: May 2, 2005

Last Updated: August 21, 2007

This module explains how to store public key infrastructure (PKI) credentials, such as Rivest, Shamir, and Adelman (RSA) keys and certificates in a specific location.

An example of a certificate storage location includes NVRAM, which is the default location, and other local storage locations, such as flash, as supported by your platform.

An example of an RSA key and certificate storage location includes a USB token. Selected Cisco platforms support smart card technology in a USB key form factor (such as an Aladdin USB eToken key). USB tokens provide secure configuration distribution, provide RSA operations such as on-token key generation, signing, and authentication, and allow users to store Virtual Private Network (VPN) credentials for deployment.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Storing PKI Credentials](#)” section on [page 25](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Storing PKI Credentials, page 2](#)
- [Restrictions for Storing PKI Credentials, page 2](#)
- [Information About Storing PKI Credentials, page 3](#)
- [How to Configure PKI Storage, page 5](#)
- [Configuration Examples for PKI Storage, page 21](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 23](#)
- [Feature Information for Storing PKI Credentials, page 25](#)

Prerequisites for Storing PKI Credentials

Prerequisites for Specifying a Local Certificate Storage Location

Before you can specify the local certificate storage location, your system should meet the following requirements:

- A Cisco IOS Release 12.4(2)T PKI-enabled image or a later image
- A platform that supports storing PKI credentials as separate files
- A configuration that contains at least one certificate
- An accessible local file system

Prerequisites for Specifying USB Token Storage for PKI Credentials

Before you can use a USB token, your system should meet the following requirements:

- A Cisco 871 router, Cisco 1800 series, Cisco 2800 series, a Cisco 3800 series router, or a Cisco 7200VXR NPE-G2 platform
- At least a Cisco IOS Release 12.3(14)T image running on any of the supported platforms
- A Cisco supported USB token
- A k9 image

Restrictions for Storing PKI Credentials

Restrictions for Specifying a Local Certificate Storage Location

When storing certificates to a local storage location, the following restrictions are applicable:

- Only local file systems may be used. An error message will be displayed if a remote file system is selected, and the command will not take effect.
- A subdirectory may be specified if supported by the local file system. NVRAM does not support subdirectories.

Restrictions for Specifying USB Token Storage

When using a USB token to store PKI data, the following restrictions are applicable:

- USB token support requires a 3DES (k9) Cisco IOS software image, which provides secure file storage.
- You cannot boot an image from a USB token. (However, you can boot a configuration from a USB token.)
- USB hubs are currently not supported. Thus, the number of supported devices is limited to the number of available USB ports.

Information About Storing PKI Credentials

To determine where to store PKI credentials, you should understand the following concepts:

- [Storing Certificates to a Local Storage Location, page 3](#)
- [PKI Credentials and USB Tokens, page 3](#)

Storing Certificates to a Local Storage Location

Certificates are stored to NVRAM by default, however some routers do not have the required amount of NVRAM to successfully store certificates. Introduced in Cisco IOS Release 12.4(2)T is the ability to specify where certificates are stored on a local file system.

All Cisco platforms support NVRAM and flash local storage. Depending on your platform, you may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token.

During run time, you can specify what active local storage device you would like to use to store certificates.

PKI Credentials and USB Tokens

To use a secure USB token on your router, you should understand the following concepts:

- [How a USB Token Works, page 3](#)
- [Benefits of USB Tokens, page 4](#)

How a USB Token Works

A smart card is a small plastic card, containing a microprocessor and memory that allows you to store and process data. A USB token is a smart card with a USB interface. The token can securely store any type of file within its available storage space (32 KB). Configuration files that are stored on the USB token can be encrypted and accessed only via a user PIN. The router will not load the configuration file unless the proper PIN has been configured for secure deployment of router configuration files.

After you plug the USB token into the router, you must log into the USB token; thereafter, you can change default settings, such as the user PIN (default: 1234567890) and the allowed number of failed login attempts (default: 15 attempts) before future logins are refused. For more information on accessing and configuring the USB token, see the section “[Logging Into and Setting Up the USB Token.](#)”

After you have successfully logged into the USB token, you can copy files from the router on to the USB token via the **copy** command. USB token RSA keys and associated IPsec tunnels remain available until the router is reloaded. To specify the length of time before the keys are removed and the IPsec tunnels are torn down, issue the **crypto pki token removal timeout** command.

[Table 1](#) highlights the capabilities of the USB token.

Table 1 **Functionality Highlights for USB Tokens**

Function	USB Token
Accessibility	Used to securely store and transfer digital certificates, preshared keys, and router configurations from the USB token to the router.
Storage Size	32 KB

Table 1 **Functionality Highlights for USB Tokens (continued)**

Function	USB Token
File Types	<ul style="list-style-type: none"> Typically used to store digital certificates, preshared keys, and router configurations for IPsec VPNs. USB tokens cannot store Cisco IOS images.
Security	<ul style="list-style-type: none"> Files can be encrypted and accessed only with a user PIN. Files can also be stored in a nonsecure format.
Boot Configurations	<ul style="list-style-type: none"> The router can use the configuration stored in the USB token during boot time. The router can use the secondary configuration stored in the USB token during boot time. (A secondary configuration allows users to load their IPsec configuration.)

Benefits of USB Tokens

USB token support on a Cisco router provides the following application benefits:

Removable Credentials: Provide or Store VPN Credentials on an External Device for Deployment

A USB token can use smart card technology to store a digital certificate and configuration for IPsec VPN deployment. This ability enhances the capability of the router to generate RSA public keys to authenticate at least one IPsec tunnel. (Because a router can initiate multiple IPsec tunnels, the USB token can contain several certificates, as appropriate.)

Storing VPN credentials on an external device reduces the threat of compromising secure data.

PIN Configuration for Secure File Deployment

A USB token can store a configuration file that can be used for enabling encryption on the router via a user-configured PIN. (That is, no digital certificates, preshared keys, or VPNs are used.)

Touchless or Low Touch Configuration

The USB token can provide remote software configuration and provisioning with little or no human interaction. Configuration is set up as an automated process. That is, the USB token can store a bootstrap configuration that the router can use to boot from after the USB token has been inserted into the router. The bootstrap configuration connects the router to a TFTP server, which contains a configuration that completely configures the router.

RSA Operations

As of Cisco IOS Release 12.4(11)T and later releases, a USB token may be used as a cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication to be performed on the token.

General-purpose, special-usage, encryption, or signature RSA key pairs with a modulus of 2048 bits or less may be generated from credentials located on your token storage device. Private keys are not distributed and remain on the token by default, however you may configure the private key storage location.

Keys that reside on a USB token are saved to persistent token storage when they are generated. Key deletion will remove the keys stored on the token from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the **write memory** or a similar command is issued.)

Remote Device Configuration and Provisioning in a Secure Device Provisioning (SDP) Environment

As of Cisco IOS Release 12.4(15)T and later releases, SDP may be used to configure a USB token. The configured USB token may be transported to provision a device at a remote location. That is, a USB token may be used to transfer cryptographic information from one network device to another remote network device providing a solution for a staged USB token deployment.

For information about using USB tokens with SDP, see document titles in the “[Related Documents](#)” section.

How to Configure PKI Storage

This section contains the following configuration tasks:

- [Specifying a Local Storage Location for Certificates, page 5](#)
- [Setting Up and Using USB Tokens on Cisco Routers, page 6](#)
- [Troubleshooting USB Tokens, page 16](#)

Specifying a Local Storage Location for Certificates

The following procedure allows you to specify the local storage location for certificates.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. `crypto pki certificate storage location-name`
4. `exit`
5. **copy** *source-url destination-url*
6. `show crypto pki certificates storage`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki certificate storage <i>location-name</i> Example: Router(config)# crypto pki certificate storage flash:/certs	Specifies the local storage location for certificates.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.
Step 5	copy <i>source-url destination-url</i> Example: Router# copy system:running-config nvram:startup-config	(Optional) Saves the running configuration to the startup configuration. Note Settings will only take effect when the running configuration is saved to the startup configuration.
Step 6	show crypto pki certificates storage Example: Router# show crypto pki certificates storage	(Optional) Displays the current setting for the PKI certificate storage location.

Examples

The following is sample output for the **show crypto pki certificates storage** command where the certificates are stored in the certs subdirectory of disk0:

```
Router# show crypto pki certificates storage
```

```
Certificates will be stored in disk0:/certs/
```

Setting Up and Using USB Tokens on Cisco Routers

This section contains the following procedures that allow you to configure a router to support USB tokens:

- [Storing the Configuration on a USB Token, page 7](#)
- [Logging Into and Setting Up the USB Token, page 7](#)
- [Configuring the USB Token, page 10](#)
- [Setting Administrative Functions on the USB Token, page 13](#)

Storing the Configuration on a USB Token

Perform this task to store the configuration file in a USB token.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **boot config usbtoken[0-9]:filename**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	boot config usbtoken[0-9]:filename Example: Router(config)# boot config usbtoken0:file	Specifies that the startup configuration file is stored in a secure USB token.

Logging Into and Setting Up the USB Token

Perform this task to log into and to perform the initial set up of a USB token.

Use of RSA Keys with a USB Token

- RSA keys are loaded after the USB token is successfully logged into the router.
- By default, newly generated RSA keys are stored on the most recently inserted USB token. Regenerated keys should be stored in the same location where the original RSA key was generated.

Automatic Login

Automatic login allows the router to completely come back up without any user or operator intervention. The PIN is stored in the private NVRAM, so it is not visible in the startup or running configuration.



Note

A hand-generated startup configuration can contain the automatic login command for deployment purposes, but the **copy system:running-config nvram: startup-config** command must be issued to put the hand-generated configuration in the private configuration.

Manual Login

Unlike automatic login, manual login requires that the user know the actual USB token PIN.

Manual login can be used when storing a PIN on the router is not desirable. Manual login may also be suitable for some initial deployment or hardware replacement scenarios for which the router is obtained from the local supplier or drop-shipped to the remote site. Manual login can be executed with or without privileges, and it will make files and RSA keys on the USB token available to the Cisco IOS software. If a secondary configuration file is configured, it will be executed only with the privileges of the user who is performing the login. Thus, if you want to use manual login and set up the secondary configuration on the USB token to perform anything useful, you need to enable privileges.

Manual login can also be used in recovery scenarios for which the router configuration has been lost. If the scenario contains a remote site that normally connects to the core network with a VPN, the loss of the configuration and RSA keys requires out-of-band services that the USB token can provide. The USB token can contain a boot configuration, a secondary configuration, or both, and RSA keys to authenticate the connection.

SUMMARY STEPS

1. **enable**
2. **crypto pki token** *token-name* [**admin**] **login** [*pin*]
or
configure terminal
3. **crypto pki token** *token-name* **user-pin** [*pin*]
4. **exit**
5. **show usbtoken**[0-9]:*filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	crypto pki token token-name [admin] login [pin] Example: Router# crypto pki token usbtokens admin login 5678 or configure terminal Example: Router# configure terminal	Manually logs into the USB token. You must specify the admin keyword if later you want to change the user PIN. or Puts the router in global configuration mode, which allows you to configure automatic USB token login.
Step 3	crypto pki token token-name user-pin [pin] Example: Router(config)# crypto pki token usbtokens user-pin 1234	(Optional) Configures the router to log into the token automatically, using the specified PIN at router startup or when the USB token is inserted into a USB slot. The PIN is encrypted and stored in NVRAM. Note You will be asked to enter your passphrase.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.
Step 5	show usbtokens[0-9]:filename Example: Router# show usbtokens:usbfile	(Optional) Verifies whether the USB token has been logged onto the router.

What to Do Next

After you have logged into the USB token, it is available for use.

- To further configure the USB token, see the “[Configuring the USB Token](#)” section.
- To perform USB token administrative tasks, such as changing the user PIN, copying files from the router to the USB token set key storage location, and changing USB tokens, see the “[Setting Administrative Functions on the USB Token](#)” section.
- To utilize the USB token as a cryptographic device to perform RSA operations, see the document titles in the “[Related Documents](#)” section.
- To specify that the USB token be used for RSA operations during initial autoenrollment, see the document titles in the “[Related Documents](#)” section.

Configuring the USB Token

After you have set up automatic login, you may perform this task to further configure the USB token.

PINs and Passphrases

For additional PIN security with automatic login, you may encrypt your PIN stored in NVRAM and set up a passphrase for your USB token. Establishing a passphrase allows you to keep your PIN secure; another user needs only to know the passphrase, not the PIN.

When the USB token is inserted into the router, the passphrase is needed to decrypt the PIN. Once the PIN is decrypted, the router can then use the PIN to login the USB token.

**Note**

The user has only the access they would normally have and needs only privilege level 1 to log in.

Unlocking and Locking the USB Token

The USB token itself can be locked (encrypted) or unlocked (decrypted).

Unlocking the USB token allows it to be used. Once unlocked, Cisco IOS treats the token as if it were automatically logged in. Any keys on the USB token are loaded, and if a secondary configuration file is on the token, it is executed with full user privileges (privilege level 15) independent of the privilege level of the logged-in user.

Locking the token, unlike logging out of the token, deletes any RSA keys loaded from the token and runs the secondary unconfiguration file, if configured.

Secondary Configuration and Unconfiguration Files

Configuration files that exist on a USB token are called secondary configuration files. If you create and configure a secondary configuration file, it is executed after the token is logged in. The existence of a secondary configuration file is determined by the presence of a secondary configuration file option in the Cisco IOS configuration stored in NVRAM. When the token is removed or logged out and the removal timer expires, a separate secondary unconfiguration file is processed to remove all secondary configuration elements from the running configuration. Secondary configuration and secondary unconfiguration files are executed at privilege level 15 and are not dependent on the level of the user logged in.

SUMMARY STEPS

1. **enable**
2. **crypto pki token *token-name* unlock [*pin*]**
3. **configure terminal**
4. **crypto pki token *token-name* encrypted-user-pin [write]**
5. **crypto pki token *token-name* secondary unconfig *file***
6. **exit**
7. **crypto pki token *token-name* lock [*pin*]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	crypto pki token token-name unlock [pin] Example: Router# crypto pki token mytoken unlock mypin	(Optional) Allows the token to be used if the USB token has been locked. Once unlocked, Cisco IOS treats the token as if it has been automatically logged in. Any keys on the token are loaded and if a secondary configuration file exists, it is executed.
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	crypto pki token token-name encrypted-user-pin [write] Example: Router(config)# crypto pki token mytoken encrypted-user-pin write	(Optional) Encrypts the stored PIN in NVRAM.
Step 5	crypto pki token token-name secondary unconfig file Example: Router(config)# crypto pki token mytoken secondary unconfig configs/myunconfigfile.cfg	(Optional) Specifies the secondary configuration file and its location.
Step 6	exit Example: Router(config)# exit	Enters privileged EXEC mode.
Step 7	crypto pki token token-name lock [pin] Example: Router# crypto pki token mytoken lock mypin	(Optional) Deletes any RSA keys loaded from the token and runs the secondary unconfiguration file, if it exists.

Examples

The following example shows both the configuration and encryption of a user PIN and then the router reloading and the user PIN being unlocked:

```
! Configuring the user PIN
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# crypto pki token usbtoken0: user-pin
```

```
Enter password:
```

```
! Encrypt the user PIN
```

```

Router (config)# crypto pki token usbtoken0: encrypted-user-pin
    Enter passphrase:
Router(config)# exit
Router#
Sep 20 21:51:38.076: %SYS-5-CONFIG_I: Configured from console by console
!

Router# show running config
.
.
.
crypto pki token usbtoken0 user-pin *encrypted*
.
.
.

! Reloading the router.
!
Router> enable
Password:
!
! Decrypting the user pin.
!
Router# crypto pki token usbtoken0: unlock
Token eToken is usbtoken0
!
Enter passphrase:
Token login to usbtoken0(eToken) successful
Router#
Sep 20 22:31:13.128: %CRYPTO-6-TOKENLOGIN: Cryptographic Token eToken
Login Successful

```

The following example shows how a secondary unconfiguration file might be used to remove secondary configuration elements from the running configuration. For example, a secondary configuration file might be used to set up a PKI trustpoint. A corresponding unconfiguration file, named `mysecondaryunconfigfile.cfg`, might contain this command line:

```
no crypto pki trustpoint token-tp
```

If the token were removed and the following commands executed, the trustpoint and associated certificates would be removed from the router's running configuration:

```

Router# configure terminal
Router(config)# no crypto pki token mytoken secondary unconfig mysecondaryunconfigfile.cfg

```

What to Do Next

After you have logged into and configured the USB token, it is available for use.

- To perform USB token administrative tasks, such as changing the user PIN, copying files from the router to the USB token set key storage location, and changing USB tokens, see the “[Setting Administrative Functions on the USB Token](#)” section.
- To utilize the USB token as a cryptographic device to perform RSA operations, see the document titles in the “[Related Documents](#)” section.

- To specify that the USB token be used for RSA operations during initial autoenrollment, see the document titles in the “[Related Documents](#)” section.

Setting Administrative Functions on the USB Token

Perform this task to change default settings, such as the user PIN, the maximum number of failed attempts on the USB token, or the credential storage location.

SUMMARY STEPS

1. **enable**
2. **crypto pki token** *token-name* [**admin**] **change-pin** [*pin*]
3. **crypto pki token** *token-name* **device: label** *token-label*
4. **configure terminal**
5. **crypto key storage** *device:*
6. **crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename:*] [**on** *devicename:*]
7. **crypto key move rsa** *keylabel* [**non-exportable**] [**on** | **storage**] *location*
8. **crypto pki token** {*token-name* | **default**} **removal timeout** [*seconds*]
9. **crypto pki token** {*token-name* | **default**} **max-retries** [*number*]
10. **exit**
11. **copy usbflash**[0-9]:*filename* *destination-url*
12. **show usbtok**[0-9]:*filename*
13. **crypto pki token** *token-name* **logout**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	crypto pki token token-name [admin] change-pin [pin] Example: Router# crypto pki token usbtoken0 admin change-pin	(Optional) Changes the user PIN number on the USB token. <ul style="list-style-type: none"> If the PIN is not changed, the default PIN—1234567890—will be used. Note After the PIN has been changed, you must reset the login failure count to zero (via the crypto pki token max-retries command). The maximum number of allowable login failures is set (by default) to 15.
Step 3	crypto pki token token-name device: label token-label Example: Router# crypto pki token my token usb0: label newlabel	(Optional) Sets or changes the name of the USB token. <ul style="list-style-type: none"> The value of the <i>token-label</i> argument may be up to 31 alphanumeric characters in length including dashes and underscores. Tip This command is useful when configuring multiple USB tokens for automatic login, secondary configuration files, or other token specific settings.
Step 4	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 5	crypto key storage device: Example: Router(config)# crypto key storage usbtoken0:	(Optional) Sets the default RSA key storage location for newly created keys. Note Regardless of configuration settings, existing keys are stored on the device from where they were originally loaded.
Step 6	crypto key generate rsa [general-keys usage-keys signature encryption] [label key-label] [exportable] [modulus modulus-size] [storage devicename:] [on devicename:] Example: Router(config)# crypto key generate rsa label tokenkey1 storage usbtoken0:	(Optional) Generates the RSA key pair. <ul style="list-style-type: none"> The storage keyword specifies the key storage location. The on keyword specifies that the keys will be generated on the designated device.

	Command or Action	Purpose
Step 7	<p>crypto key move rsa <i>keylabel</i> [non-exportable] [on storage] <i>location</i></p> <p>Example: Router(config)# crypto key move rsa keypairname non-exportable on token</p>	<p>(Optional) Moves existing Cisco IOS credentials from the current storage location to the specified storage location.</p> <p>By default, the RSA key pair remains stored on the current device.</p> <p>Generating the key on the router and moving it to the token takes less than a minute. Generating a key on the token, using the on keyword could take five to ten minutes, and is dependent on hardware key generation routines available on the USB token.</p> <p>When an existing RSA key pair is generated in Cisco IOS, stored on a USB token, and used for an enrollment, it may be necessary to move those existing RSA key pairs to an alternate location for permanent storage.</p> <p>This command is useful when using SDP with USB tokens to deploy credentials.</p>
Step 8	<p>crypto pki token {<i>token-name</i> default} removal timeout [<i>seconds</i>]</p> <p>Example: Router(config)# crypto pki token usbtokens0 removal timeout 60</p>	<p>(Optional) Sets the time interval, in seconds, that the router will wait before removing the RSA keys that are stored in the USB token after the USB token has been removed from the router.</p> <p>Note If this command is not issued, all RSA keys and IPsec tunnels associated with the USB token are torn down immediately after the USB token is removed from the router.</p>
Step 9	<p>crypto pki token {<i>token-name</i> default} max-retries [<i>number</i>]</p> <p>Example: Router(config)# crypto pki token usbtokens0 max-retries 20</p>	<p>(Optional) Sets the maximum number of consecutive failed login attempts allowed before access to the USB token is denied.</p> <ul style="list-style-type: none"> By default, the value is set at 15.
Step 10	<p>exit</p> <p>Example: Router(config)# exit</p>	Exits global configuration mode.
Step 11	<p>copy usbflash[0-9]:<i>filename</i> <i>destination-url</i></p> <p>Example: Router# copy usbflash0:file1 nvram:</p>	<p>Copies files from USB token to the router.</p> <ul style="list-style-type: none"> <i>destination-url</i>—See the copy command page documentation for a list of supported options.
Step 12	<p>show usbtokens[0-9]:<i>filename</i></p> <p>Example: Router# show usbtokens:usbfile</p>	(Optional) Displays information about the USB token. You can use this command to verify whether the USB token has been logged onto the router.
Step 13	<p>crypto pki token <i>token-name</i> logout</p> <p>Example: Router# crypto pki token usbtokens0 logout</p>	<p>Logs the router out of the USB token.</p> <p>Note If you want to save any data to the USB token, you must log back into the token.</p>

Troubleshooting USB Tokens

This section contains descriptions of the following Cisco IOS commands that can be used to help troubleshoot possible problems that may arise while using a USB token:

- [The show file systems Command, page 16](#)
- [The show usb device Command, page 17](#)
- [The show usb controllers Command, page 17](#)
- [The dir Command, page 19](#)

The show file systems Command

Use the **show file systems** command to determine whether the router recognizes that there is a USB module plugged into a USB port. The USB module should appear on the list of file systems. If the module does not appear on the list, it can indicate any of the following problems:

- A connection problem with the USB module.
- The Cisco IOS image running on the router does not support a USB module.
- A hardware problem with the USB module itself.

SUMMARY STEPS

1. **show file systems**

DETAILED STEPS

- Step 1** Sample output from the **show file systems** command showing a USB token appears below. The USB module listing appears in the last line of the examples.

```
Router# show file systems

File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
      -          -          -      -      -
      -          -          opaque  rw      archive:
      -          -          opaque  rw      system:
      -          -          opaque  rw      null:
      -          -          network  rw      tftp:
* 129880064      69414912      disk    rw      flash:#
      491512      486395      nvram   rw      nvram:
      -          -          opaque  wo      syslog:
      -          -          opaque  rw      xmodem:
      -          -          opaque  rw      ymodem:
      -          -          network  rw      rcp:
      -          -          network  rw      pram:
      -          -          network  rw      ftp:
      -          -          network  rw      http:
      -          -          network  rw      scp:
      -          -          network  rw      https:
      -          -          opaque  ro      cns:
      63158272    33037312    usbflash  rw      usbflash0:
      32768      858      usbtoken  rw      usbtoken1:
```


The show usb device Command

Use the **show usb device** command to determine if a USB token is supported by Cisco.

SUMMARY STEPS

1. **show usb device**

DETAILED STEPS

- Step 1** The following sample output for the **show usb device** command indicates whether or not the module is supported is bold in the sample output below:

```
Router# show usb device

Host Controller:1
Address:0x11
Device Configured:YES
Device Supported:YES
Description:eToken Pro 4254
Manufacturer:AKS
Version:1.0
Serial Number:
Device Handle:0x1010000
USB Version Compliance:1.0
Class Code:0xFF
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x529
Product ID:0x514
Max. Packet Size of Endpoint Zero:8
Number of Configurations:1
Speed:Low
Selected Configuration:1
Selected Interface:0

Configuration:
  Number:1
  Number of Interfaces:1
  Description:
  Attributes:None
  Max Power:60 mA

  Interface:
    Number:0
    Description:
    Class Code:255
    Subclass:0
    Protocol:0
    Number of Endpoints:0
```

The show usb controllers Command

Use the **show usb controllers** command to determine if there is a hardware problem with a USB flash module. If the **show usb controllers** command displays an error, the error indicates a hardware problem in the USB module.

You can also use the **show usb controllers** command to verify that copy operations onto a USB flash module are occurring successfully. Issuing the **show usb controllers** command after performing a file copy should display successful data transfers.

SUMMARY STEPS

1. show usb controllers

DETAILED STEPS

- Step 1** The following sample output for the **show usb controllers** command displays a working USB flash module:

```
Router# show usb controllers
```

```
Name:1362HCD
Controller ID:1
Controller Specific Information:
  Revision:0x11
  Control:0x80
  Command Status:0x0
  Hardware Interrupt Status:0x24
  Hardware Interrupt Enable:0x80000040
  Hardware Interrupt Disable:0x80000040
  Frame Interval:0x27782EDF
  Frame Remaining:0x13C1
  Frame Number:0xDA4C
  LSThreshold:0x628
  RhDescriptorA:0x19000202
  RhDescriptorB:0x0
  RhStatus:0x0
  RhPort1Status:0x100103
  RhPort2Status:0x100303
  Hardware Configuration:0x3029
  DMA Configuration:0x0
  Transfer Counter:0x1
  Interrupt:0x9
  Interrupt Enable:0x196
  Chip ID:0x3630
  Buffer Status:0x0
  Direct Address Length:0x80A00
  ATL Buffer Size:0x600
  ATL Buffer Port:0x0
  ATL Block Size:0x100
  ATL PTD Skip Map:0xFFFFFFFF
  ATL PTD Last:0x20
  ATL Current Active PTD:0x0
  ATL Threshold Count:0x1
  ATL Threshold Timeout:0xFF

Int Level:1
Transfer Completion Codes:
  Success          :920          CRC          :0
  Bit Stuff        :0           Stall          :0
  No Response      :0           Overrun       :0
  Underrun         :0           Other         :0
  Buffer Overrun    :0           Buffer Underrun:0

Transfer Errors:
  Canceled Transfers :2          Control Timeout:0

Transfer Failures:
  Interrupt Transfer  :0          Bulk Transfer   :0
```

```

        Isochronous Transfer :0
Transfer Successes:
        Interrupt Transfer :0
        Isochronous Transfer :0
        Control Transfer:0
        Bulk Transfer :26
        Control Transfer:894

USB Failures:
        Enumeration Failures :0
        Power Budget Exceeded:0
        No Class Driver Found:0

USB MSCD SCSI Class Driver Counters:
        Good Status Failures :3
        Good Status Timed out:0
        Device Never Opened :0
        Illegal App Handle :0
        Invalid Unit Number :0
        Application Overflow :0
        Control Pipe Stall :0
        Device Stalled :0
        Device Detached :0
        Invalid Logic Unit Num:0
        Command Fail :0
        Device not Found:0
        Drive Init Fail :0
        Bad API Command :0
        Invalid Argument:0
        Device in use :0
        Malloc Error :0
        Bad Command Code:0
        Unknown Error :0

USB Aladdin Token Driver Counters:
        Token Inserted :1
        Send Insert Msg Fail :0
        Dev Entry Add Fail :0
        Dev Entry Remove Fail:0
        Response Txn Fail :0
        Txn Invalid Dev Handle:0
        Token Removed :0
        Response Txns :434
        Request Txns :434
        Request Txn Fail:0
        Command Txn Fail:0

USB Flash File System Counters:
        Flash Disconnected :0
        Flash Device Fail :0
        Flash startstop Fail :0
        Flash Connected :1
        Flash Ok :1
        Flash FS Fail :0

USB Secure Token File System Counters:
        Token Inserted :1
        Token FS success :1
        Token Max Inserted :0
        Token Event :0
        Watched Boolean Create Failures:0
        Token Detached :0
        Token FS Fail :0
        Create Talker Failures:0
        Destroy Talker Failures:0

```

The dir Command

Use the **dir** command with the **filesystem** keyword option **usbtoken[0-9]**: to display all files, directories, and their permission strings on the USB token.

SUMMARY STEPS

1. **dir [filesystem:]**

DETAILED STEPS

Step 1 The following sample output displays directory information for the USB token:

```
Router# dir usbtoken1:
```

```
Directory of usbtoken1:/
```

```

 2  d---          64  Dec 22 2032 05:23:40 +00:00 1000
 5  d---        4096  Dec 22 2032 05:23:40 +00:00 1001
 8  d---          0  Dec 22 2032 05:23:40 +00:00 1002
10  d---        512  Dec 22 2032 05:23:42 +00:00 1003
12  d---          0  Dec 22 2032 05:23:42 +00:00 5000
13  d---          0  Dec 22 2032 05:23:42 +00:00 6000
14  d---          0  Dec 22 2032 05:23:42 +00:00 7000
15  ----        940  Jun 27 1992 12:50:42 +00:00 mystartup-config
16  ----       1423  Jun 27 1992 12:51:14 +00:00 myrunning-config
```

```
32768 bytes total (858 bytes free)
```

The following sample output displays directory information for all devices the router is aware of:

```
Router# dir all-filesystems
```

```
Directory of archive:/
```

```
No files in directory
```

```
No space information available
```

```
Directory of system:/
```

```

 2  drwx          0          <no date> its
115 dr-x          0          <no date> lib
144 dr-x          0          <no date> memory
 1  -rw-       1906          <no date> running-config
114 dr-x          0          <no date> vfiles
```

```
No space information available
```

```
Directory of flash:/
```

```
 1  -rw-   30125020  Dec 22 2032 03:06:04 +00:00 c3825-entservicesk9-mz.123-14.T
```

```
129880064 bytes total (99753984 bytes free)
```

```
Directory of nvram:/
```

```

476 -rw-       1947          <no date> startup-config
477 ----        46          <no date> private-config
478 -rw-       1947          <no date> underlying-config
 1  -rw-          0          <no date> ifIndex-table
 2  ----         4          <no date> rf_cold_starts
 3  ----        14          <no date> persistent-data
```

```
491512 bytes total (486395 bytes free)
```

```
Directory of usbflash0:/
```

```
 1  -rw-   30125020  Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T
```

```
63158272 bytes total (33033216 bytes free)
```

```
Directory of usbtoken1:/
```

```

 2  d---          64  Dec 22 2032 05:23:40 +00:00 1000
 5  d---        4096  Dec 22 2032 05:23:40 +00:00 1001
 8  d---          0  Dec 22 2032 05:23:40 +00:00 1002
```

```

10 d---          512 Dec 22 2032 05:23:42 +00:00 1003
12 d---          0 Dec 22 2032 05:23:42 +00:00 5000
13 d---          0 Dec 22 2032 05:23:42 +00:00 6000
14 d---          0 Dec 22 2032 05:23:42 +00:00 7000
15 ----          940 Jun 27 1992 12:50:42 +00:00 mystartup-config
16 ----         1423 Jun 27 1992 12:51:14 +00:00 myrunning-config

```

32768 bytes total (858 bytes free)

Configuration Examples for PKI Storage

This section contains the following configuration examples:

- [Storing Certificates to a Specific Local Storage Location: Example, page 21](#)
- [Logging Into a USB Token and Saving RSA Keys to the USB Token: Example, page 22](#)

Storing Certificates to a Specific Local Storage Location: Example

The following configuration example shows how to store certificates to the certs subdirectory. The certs subdirectory does not exist and is automatically created.

Router# **dir nvram:**

```

114 -rw-          4687 <no date> startup-config
115 ----          5545 <no date> private-config
116 -rw-          4687 <no date> underlying-config
  1 ----           34 <no date> persistent-data
  3 -rw-          707 <no date> ioscaroot#7401CA.cer
  9 -rw-          863 <no date> msca-root#826E.cer
10 -rw-          759 <no date> msca-root#1BA8CA.cer
11 -rw-          863 <no date> msca-root#75B8.cer
24 -rw-         1149 <no date> storagename#6500CA.cer
26 -rw-          863 <no date> msca-root#83EE.cer

```

129016 bytes total (92108 bytes free)

Router# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# **crypto pki certificate storage disk0:/certs**

Requested directory does not exist -- created

Certificates will be stored in disk0:/certs/

Router(config)# **end**

Router# **write**

*May 27 02:09:00:%SYS-5-CONFIG_I:Configured from console by consolemem

Building configuration...

[OK]

Router# **directory disk0:/certs**

Directory of disk0:/certs/

```

14 -rw-          707 May 27 2005 02:09:02 +00:00 ioscaroot#7401CA.cer
15 -rw-          863 May 27 2005 02:09:02 +00:00 msca-root#826E.cer
16 -rw-          759 May 27 2005 02:09:02 +00:00 msca-root#1BA8CA.cer
17 -rw-          863 May 27 2005 02:09:02 +00:00 msca-root#75B8.cer
18 -rw-         1149 May 27 2005 02:09:02 +00:00 storagename#6500CA.cer

```

```

19  -rw-          863  May 27 2005 02:09:02 +00:00  msca-root#83EE.cer

47894528 bytes total (20934656 bytes free)

! The certificate files are now on disk0/certs:

```

Logging Into a USB Token and Saving RSA Keys to the USB Token: Example

The following configuration example shows to how log into the USB token, generate RSA keys, and store the RSA keys onto the USB token:

```

! Configure the router to automatically log into the eToken
configure terminal
  crypto pki token default user-pin 0 1234567890
! Generate RSA keys and enroll certificates with the CA.
crypto pki trustpoint IOSCA
  enrollment url http://10.23.2.2
exit
crypto ca authenticate IOSCA
Certificate has the following attributes:
    Fingerprint MD5:23272BD4 37E3D9A4 236F7E1A F534444E
    Fingerprint SHA1:D1B4D9F8 D603249A 793B3CAF 8342E1FE 3934EB7A

% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
crypto pki enroll
crypto pki enroll IOSCA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include:c2851-27.cisco.com
% Include the router serial number in the subject name? [yes/no]:no
% Include an IP address in the subject name? [no]:no
Request certificate from CA? [yes/no]:yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate IOSCA verbose' command will show the fingerprint.

*Jan 13 06:47:19.413:CRYPTO_PKI: Certificate Request Fingerprint MD5:E6DDAB1B
  0E30EFE6 54529D8A DA787DBA
*Jan 13 06:47:19.413:CRYPTO_PKI: Certificate Request Fingerprint SHA1:3B0F33B
  7 57C02A10 3935042B C4B6CD3D 61039251
*Jan 13 06:47:21.021:%PKI-6-CERTRET:Certificate received from Certificate Authority
! Issue the write memory command, which will automatically save the RSA keys to the eToken
! instead of private NVRAM.
Router# write memory
Building configuration...
[OK]

*Jan 13 06:47:29.481:%CRYPTO-6-TOKENSTOREKEY:Key c2851-27.cisco.com stored on
Cryptographic Token eToken Successfully

```

The following sample output from the **show crypto key mypubkey rsa** command displays stored credentials after they are successfully loaded from the USB token. Credentials that are stored on the USB token are in the protected area. When storing the credentials on the USB token, the files are stored in a directory called /keystore. However, the key files are hidden from the command-line interface (CLI).

```
Router# show crypto key mypubkey rsa

% Key pair was generated at:06:37:26 UTC Jan 13 2005
Key name:c2851-27.cisco.com
Usage:General Purpose Key
Key is not exportable.
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E3C644 43AA7DDD
 732E0F4E 3CA0CDAB 387ABF05 EB8F22F2 2431F1AE 5D51FEE3 FCDEA934 7FBD3603
 7C977854 B8E999BF 7FC93021 7F46ABF8 A4BA2ED6 172D3D09 B5020301 0001
% Key pair was generated at:06:37:27 UTC Jan 13 2005
Key name:c2851-27.cisco.com.server
Usage:Encryption Key
Key is not exportable.
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00DD96AE 4BF912EB
 2C261922 4784EF98 2E70E837 774B3778 7F7AEB2D 87F5669B BF5DDFBC F0D521A5
 56AB8FDC 9911968E DE347FB0 A514A856 B30EAF4 D1F453E1 003CFE65 0CCC6DC7
 21FBE3AC 2F8DEA16 126754BC 1433DEF9 53266D33 E7338C95 BB020301 0001
```

Additional References

The following sections provide references related to PKI storage support.

Related Documents

Related Topic	Document Title
Connecting the USB modules to the router	Cisco Access Router USB Flash Module and USB eToken Hardware Installation Guide
eToken and USB flash data sheet	USB eToken and USB Flash Features Support
RSA keys	Deploying RSA Keys Within a PKI
File management (loading, copying, and rebooting files)	Cisco IOS Configuration Fundamentals Configuration Guide on Cisco.com
USB Token RSA Operations: Certificate server configuration	<p>“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” chapter in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i></p> <p>See the “Generating a Certificate Server RSA Key Pair” section, the “Configuring a Certificate Server Trustpoint” section, and related examples.</p>

Related Topic	Document Title
USB Token RSA Operations: Using USB tokens for RSA operations upon initial autoenrollment	<p>“Configuring Certificate Enrollment for a PKI” chapter in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>.</p> <p>See the “Configuring Certificate Enrollment or Autoenrollment” section.</p>
SDP setup, configuration and use with USB tokens	<p>“Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI” chapter in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>.</p> <p>See the feature information section for the feature names on using SDP and USB tokens to deploy PKI credentials.</p>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Storing PKI Credentials

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Implementing and Managing PKI Features Roadmap](#).”

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for Storing PKI Credentials

Feature Name	Releases	Feature Information
USB Token and Secure Device Provisioning (SDP) Integration	12.4(15)T	<p>This feature provides the ability to provision remote devices with USB tokens using SDP.</p> <p>The following sections in this document provide information about this feature:</p> <ul style="list-style-type: none">• Benefits of USB Tokens• Setting Administrative Functions on the USB Token <p>The following commands were introduced by this feature: binary file, crypto key move rsa, template file.</p> <p>Note This document introduces the benefits of using USB tokens and SDP for a deployment solution. For other documentation on this topic, see the “Related Documents” section.</p>

Table 2 *Feature Information for Storing PKI Credentials (continued)*

Feature Name	Releases	Feature Information
Cisco IOS USB Token PKI Enhancements — Phase 2	12.4(11)T	<p>This feature enhances USB token functionality by using the USB token as a cryptographic device. USB tokens may be used for RSA operations such as key generation, signing, and authentication.</p> <p>The following sections in this document provide information about this feature:</p> <ul style="list-style-type: none"> • Benefits of USB Tokens • Logging Into and Setting Up the USB Token • Setting Administrative Functions on the USB Token <p>Note This document introduces the benefits of using USB tokens and the keys on the token for RSA operations. For other documentation on this topic, see the “Related Documents” section.</p>
USB Storage PKI Enhancements	12.4(4)T 12.4(11)T	<p>This feature enhances the USB token PIN security for automatic login and increases the flexibility of USB token configuration and the RSA key storage.</p> <p>Cisco IOS Release 12.4(11)T introduced support for USB Storage on NPE-G2.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Configuring the USB Token • Setting Administrative Functions on the USB Token <p>The following commands were introduced or modified by this feature: crypto key storage, crypto pki generate rsa, crypto pki token encrypted-user-pin, crypto pki token label, crypto pki token lock, crypto pki token secondary unconfig, crypto pki token unlock</p>
Certificate — Storage Location Specification	12.2(33)SXH 12.2(33)SRA 12.4(2)T	<p>This feature allows you to specify the storage location of local certificates for platforms that support storing certificates as separate files. All Cisco platforms support NVRAM, which is the default location, and flash local storage. Depending on your platform, you may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Storing Certificates to a Local Storage Location • Specifying a Local Storage Location for Certificates • Storing Certificates to a Specific Local Storage Location: Example <p>The following commands were introduced by this feature: crypto pki certificate storage, show crypto pki certificates storage</p>

Table 2 *Feature Information for Storing PKI Credentials (continued)*

Feature Name	Releases	Feature Information
USB Storage	12.3(14)T 12.4(11)T	<p>This feature enables certain models of Cisco routers to support USB tokens. USB tokens provide secure configuration distribution and allow users to VPN credentials for deployment.</p> <p>Cisco IOS Release 12.4(11)T introduced support for USB Storage on NPE-G2.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • PKI Credentials and USB Tokens • Setting Up and Using USB Tokens on Cisco Routers • Troubleshooting USB Tokens • Logging Into a USB Token and Saving RSA Keys to the USB Token: Example <p>The following commands were introduced or modified by this feature: copy, crypto pki token change-pin, crypto pki token login, crypto pki token logout, crypto pki token max-retries, crypto pki token removal timeout, crypto pki token secondary config, crypto pki token user-pin, debug usb driver, dir, show usb controllers, show usb device, show usb driver, show usbtokn</p>
Certificate - Storage Location Specification	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2009 Cisco Systems, Inc. All rights reserved.



Source Interface Selection for Outgoing Traffic with Certificate Authority

The Source Interface Selection for Outgoing Traffic with Certificate Authority feature allows you to specify that the address of an interface be used as the source address for all outgoing TCP connections associated with that trustpoint when a designated trustpoint has been configured.

Feature Specifications for Source Interface Selection for Outgoing Traffic with Certificate Authority

Feature History

Release	Modification
12.2(15)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Supported Platforms

Cisco 1600, Cisco 1600R, Cisco 1710, Cisco 1720, Cisco 1750, Cisco 1751, Cisco 1760, Cisco 2400, Cisco 2610–2613, Cisco 2610XM–2611XM, Cisco 2620–2621, Cisco 2620XM–2621XM, Cisco 2650–2651, Cisco 2650XM–2651XM, Cisco 2691, Cisco 3620, Cisco 3631, Cisco 3640, Cisco 3660, Cisco 3725, Cisco 3745, Cisco 7100, Cisco 7200, Cisco 7400, Cisco 7500, Cisco 801–Cisco 806, Cisco 811, Cisco 813, Cisco 828, Cisco 8850-RPM, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco MC3810, Cisco ubr7200, Cisco ubr905, Cisco ubr925

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Information About Source Interface Selection for Outgoing Traffic with Certificate Authority, page 2](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [How to Configure Source Interface Selection for Outgoing Traffic with Certificate Authority, page 3](#)
- [Configuration Examples for Source Interface Selection for Outgoing Traffic with Certificate Authority, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)
- [Glossary, page 8](#)

Information About Source Interface Selection for Outgoing Traffic with Certificate Authority

To configure the Source Interface Selection for Outgoing Traffic with Certificate Authority feature, you must understand the following concepts:

- [Certificates That Identify an Entity, page 2](#)
- [Source Interface for Outgoing TCP Connections Associated with a Trustpoint, page 2](#)

Certificates That Identify an Entity

Certificates can be used to identify an entity. A trusted server, known as the certification authority (CA), issues the certificate to the entity after determining the identity of the entity. A router that is running Cisco IOS software obtains its certificate by making a network connection to the CA. Using the Simple Certificate Enrollment Protocol (SCEP), the router transmits its certificate request to the CA and receives the granted certificate. The router obtains the certificate of the CA in the same manner using SCEP. When validating a certificate from a remote device, the router may again contact the CA or a Lightweight Directory Access Protocol (LDAP) or HTTP server to determine whether the certificate of the remote device has been revoked. (This process is known as checking the certificate revocation list [CRL].)

In some configurations, the router may make the outgoing TCP connection using an interface that does not have a valid or routable IP address. The user must specify that the address of a different interface be used as the source IP address for the outgoing connection. Cable modems are a specific example of this requirement because the outgoing cable interface (the RF interface) usually does not have a routable address. However, the user interface (usually Ethernet) does have a valid IP address.

Source Interface for Outgoing TCP Connections Associated with a Trustpoint

The **crypto ca trustpoint** command is used to specify a trustpoint. The **source interface** command is used along with the **crypto ca trustpoint** command to specify the address of the interface that is to be used as the source address for all outgoing TCP connections associated with that trustpoint.



Note

If the interface address is not specified using the **source interface** command, the address of the outgoing interface is used.

How to Configure Source Interface Selection for Outgoing Traffic with Certificate Authority

This section includes the following procedure:

- [Configuring the Interface for All Outgoing TCP Connections Associated with a Trustpoint, page 3](#)

Configuring the Interface for All Outgoing TCP Connections Associated with a Trustpoint

Perform this task to configure the interface that you want to use as the source address for all outgoing TCP connections associated with a trustpoint.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ca trustpoint** *name*
4. **enrollment url** *url*
5. **source interface** *interface-address*
6. **interface** *type slot/port*
7. **description** *string*
8. **ip address** *ip-address mask*
9. **interface** *type slot/port*
10. **description** *string*
11. **ip address** *ip-address mask*
12. **crypto map** *map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	crypto ca trustpoint <i>name</i> Example: Router (config)# crypto ca trustpoint ms-ca	Declares the Certificate Authority (CA) that your router should use and enters ca-trustpoint configuration mode.
Step 4	enrollment url <i>url</i> Example: Router (ca-trustpoint)# enrollment url http://yourname:80/certsrv/mscep/mscep.dll	Specifies the enrollment parameters of your CA.
Step 5	source interface <i>interface-address</i> Example: Router (ca-trustpoint)# interface ethernet 0	Interface to be used as the source address for all outgoing TCP connections associated with that trustpoint.
Step 6	interface <i>type slot/port</i> Example: Router (ca-trustpoint)# interface ethernet 1	Configures an interface type and enters interface configuration mode.
Step 7	description <i>string</i> Example: Router (config-if)# description inside interface	Adds a description to an interface configuration.
Step 8	ip address <i>ip-address mask</i> Example: Router (config-if)# ip address 10.1.1.1 255.255.255.0	Sets a primary or secondary IP address for an interface.
Step 9	interface <i>type slot/port</i> Example: Router (config-if)# interface ethernet1/0	Configures an interface type.
Step 10	description <i>string</i> Example: Router (config-if)# description outside interface 10.1.1.205 255.255.255.0	Adds a description to an interface configuration.
Step 11	ip address <i>ip-address mask</i> Example: Router (config-if)# ip address 10.2.2.205 255.255.255.0	Sets a primary or secondary IP address for an interface.
Step 12	crypto map <i>map-name</i> Example: Router (config-if)# crypto map mymap	Applies a previously defined crypto map set to an interface.

Troubleshooting Tips

Ensure that the interface specified in the command has a valid address. Attempt to ping the router using the address of the specified interface from another device (possibly the HTTP or LDAP server that is serving the CRL). You can do the same thing by using a traceroute to the router from the external device.

You can also test connectivity between the router and the CA or LDAP server by using Cisco IOS command-line interface (CLI). Enter the **ping ip** command and respond to the prompts. If you answer “yes” to the “Extended commands [n]:” prompt, you will be able to specify the source address or interface.

In addition, you can use Cisco IOS CLI to input a traceroute command. If you enter the **traceroute ip** command (in EXEC mode), you will be prompted for the destination and source address. You should specify the CA or LDAP server as the destination and the address of the interface that you specified in the “source interface” as the source address.

Configuration Examples for Source Interface Selection for Outgoing Traffic with Certificate Authority

This section includes the following example:

- [Source Interface Selection for Outgoing Traffic with Certificate Authority Example, page 5](#)

Source Interface Selection for Outgoing Traffic with Certificate Authority Example

In the following example, the router is located in a branch office. The router uses IP Security (IPSec) to communicate with the main office. Ethernet 1 is the “outside” interface that connects to the Internet Service Provider (ISP). Ethernet 0 is the interface connected to the LAN of the branch office. To access the CA server located in the main office, the router must send its IP datagrams out interface Ethernet 1 (address 10.2.2.205) using the IPSec tunnel. Address 10.2.2.205 is assigned by the ISP. Address 10.2.2.205 is not a part of the branch office or main office.

The CA cannot access any address outside the company because of a firewall. The CA sees a message coming from 10.2.2.205 and cannot respond (that is, the CA does not know that the router is located in a branch office at address 10.1.1.1, which it is able to reach).

Adding the **source interface** command tells the router to use address 10.1.1.1 as the source address of the IP datagram that it sends to the CA. The CA is able to respond to 10.1.1.1.

This scenario is configured using the **source interface** command and the interface addresses as described above.

```
crypto ca trustpoint ms-ca
  enrollment url http://ms-ca:80/certsrv/mscep/mscep.dll
  source interface ethernet0
!
interface ethernet 0
  description inside interface
  ip address 10.1.1.1 255.255.255.0
!
interface ethernet 1
  description outside interface
  ip address 10.2.2.205 255.255.255.0
  crypto map main-office
```

Additional References

For additional information related to Source Interface Selection for Outgoing Traffic with Certificate Authority, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring IPSec and certification authority	Security for VPNs with IPsec
IPSec and certification authority commands	Cisco IOS Security Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features

- **source interface**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Glossary

authenticate—To prove the identity of an entity using the certificate of an identity and a secret that the identity poses (usually the private key corresponding to the public key in the certificate).

CA—Certificate Authority. A CA is an entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

CA authentication—The user manually approves a certificate from a root CA. Usually a fingerprint of the certificate is presented to the user, and the user is asked to accept the certificate based on the fingerprint. The certificate of a root CA is signed by itself (self-signed) so that it cannot be automatically authenticated using the normal certificate verification process.

CRL—certificate revocation list. A CRL is a data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire.

enrollment—A router receives its certificate via the enrollment process. The router generates a request for a certificate in a specific format (known as PKCS #10). The request is transmitted to a CA, which grants the request and generates a certificate encoded in the same format as the request. The router receives the granted certificate and stores it in an internal database for use during normal operations.

certificate—A data structure defined in International Organization for Standardization (ISO) standard X.509 to associate an entity (machine or human) with the public key of that entity. The certificate contains specific fields, including the name of the entity. The certificate is normally issued by a CA on behalf of the entity. In this case the router will act as its own CA. Common fields within a certificate include the distinguished name (DN) of the entity, the DN of the authority issuing the certificate, and the public key of the entity.

LDAP—Lightweight Directory Access Protocol. A LDAP is a protocol that provides access for management and browser applications that provide read-and-write interactive access to the X.509 directory.

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2009 Cisco Systems, Inc. All rights reserved.



Dynamic Multipoint VPN (DMVPN)



Dynamic Multipoint VPN (DMVPN)

First Published: November 25, 2002

Last Updated: February 3, 2009

The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IP Security (IPsec) Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Dynamic Multipoint VPN \(DMVPN\)” section on page 53](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Catalyst OS, and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Dynamic Multipoint VPN \(DMVPN\), page 2](#)
- [Restrictions for Dynamic Multipoint VPN \(DMVPN\), page 2](#)
- [Information About Dynamic Multipoint VPN \(DMVPN\), page 4](#)
- [How to Configure Dynamic Multipoint VPN \(DMVPN\), page 11](#)
- [Configuration Examples for Dynamic Multipoint VPN \(DMVPN\) Feature, page 31](#)
- [Additional References, page 50](#)
- [Command Reference, page 52](#)
- [Feature Information for Dynamic Multipoint VPN \(DMVPN\), page 53](#)
- [Glossary, page 54](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Dynamic Multipoint VPN (DMVPN)

- Before a multipoint GRE (mGRE) and IPsec tunnel can be established, you must define an Internet Key Exchange (IKE) policy by using the **crypto isakmp policy** command.
- For the NAT-Transparency Aware enhancement to work, you must use IPsec transport mode on the transform set. Also, even though NAT-Transparency can support two peers (IKE and IPsec) being translated to the same IP address (using the User Datagram Protocol [UDP] ports to differentiate them [that is, Peer Address Translation (PAT)]), this functionality is not supported for DMVPN. All DMVPN spokes must have a unique IP address after they have been NAT translated. They can have the same IP address before they are NAT translated.
- To enable 2547oDMPVN—Traffic Segmentation Within DMVPN you must configure multiprotocol label switching (MPLS) by using the **mpls ip** command.

Restrictions for Dynamic Multipoint VPN (DMVPN)

- If you use the [Dynamic Creation for Spoke-to-Spoke Tunnels](#) benefit of this feature, you must use IKE certificates or wildcard preshared keys for Internet Security Association Key Management Protocol (ISAKMP) authentication.



Note

It is highly recommended that you *do not use* wildcard preshared keys because the attacker will have access to the VPN if one spoke router is compromised.

- GRE tunnel keepalives (that is, the **keepalive** command under a GRE interface) are not supported on point-to-point or multipoint GRE tunnels in a DMVPN Network.
- For best DMVPN functionality, it is recommended that you run the latest Cisco IOS software Release 12.4 mainline, 12.4T, or 12.2(18)SXF.
- If one spoke is behind one NAT device and another different spoke is behind another NAT device, and Peer Address Translation (PAT) is the type of NAT used on both NAT devices, then a session initiated between the two spokes cannot be established.

One example of a PAT configuration on a NAT interface is:

```
ip nat inside source list nat_acl interface FastEthernet0/1 overload
```

DMVPN Support on the Cisco 6500 and Cisco 7600

Blade-to-Blade Switchover on the Cisco 6500 and Cisco 7600

- DMVPN does not support blade-to-blade switchover on the Cisco 6500 and Cisco 7600.

Cisco 6500 or Cisco 7600 As a DMVPN Hub

- A Cisco 6500 or Cisco 7600 that is functioning as a DMVPN hub cannot be located behind a NAT router.
- If a Cisco 6500 or Cisco 7600 is functioning as a DMVPN hub, the spoke behind NAT must be a Cisco 6500 or Cisco 7600, respectively, or the router must be upgraded to Cisco IOS software Release 12.3(11)T02 or a later release.

Cisco 6500 or Cisco 7600 As a DMVPN Spoke

- If a Cisco 6500 or Cisco 7600 is functioning as a spoke, the hub cannot be behind NAT.
- If a Cisco 6500 or Cisco 7600 is functioning as a DMVPN spoke behind NAT, the hub must be a Cisco 6500 or Cisco 7600, respectively, or the router must be upgraded to Cisco IOS Release 12.3(11)T02 or a later release.

DMVPN Hub or Spoke Supervisor Engine

- Only a Supervisor Engine 720 can be used as a DMVPN hub or spoke. A Supervisor Engine 2 cannot be used.

Encrypted Multicast with GRE

- Encrypted Multicast with GRE is not supported on the Cisco 6500 nor on the Cisco 7600.

mGRE Interfaces

- If there are two mGRE interfaces on the same DMVPN node and they both do not have a tunnel key, the two mGRE interfaces must each have a unique tunnel source address (or interface) configured.
- On the Cisco 6500 and Cisco 7600, each GRE interface (multipoint or point-to-point) must have a unique tunnel source address (or interface).
- The following commands are not supported under mGRE with DMVPN: **ip tcp adjust-mss**, **qos pre-classify tunnel vrf**, **tunnel path-mtu-discovery**, and **tunnel vrf**.

Quality of Service (QoS)

- You cannot use QoS for DMVPN packets on a Cisco 6500 or Cisco 7600.

Tunnel Key

- The use of a tunnel key on a GRE (multipoint or point-to-point) interface is not supported in the hardware switching ASICs on the Cisco 6500 and Cisco 7600 platforms. If a tunnel key is configured, throughput performance is greatly reduced.
- In Cisco IOS Release 12.3(11)T3 and Release 12.3(14)T, the requirement that a mGRE interface must have a tunnel key was removed. Therefore, in a DMVPN network that includes a Cisco 6500 or Cisco 7600 as a DMVPN node, you should remove the tunnel key from all DMVPN nodes in the DMVPN network, thus preserving the throughput performance on the Cisco 6500 and Cisco 7600 platforms.
- If the tunnel key is not configured on any DMVPN node within a DMVPN network, it must not be configured on all DMVPN nodes with the DMVPN network.

VRF-Aware DMVPN Scenarios

- The **mls mpls tunnel-recir** command must be configured on the provider equipment (PE) DMVPN hub if customer equipment (CE) DMVPN spokes need to “talk” to other CEs across the MPLS cloud.
- The mGRE interface should be configured with a large enough IP maximum transmission unit (1400 packets) to avoid having the route processor doing fragmentation.
- Enhanced Interior Gateway Routing Protocol (EIGRP) should be avoided.

Information About Dynamic Multipoint VPN (DMVPN)

To configure the Dynamic Multipoint VPN (DMVPN) feature, you must understand the following concepts:

- [Benefits of Dynamic Multipoint VPN \(DMVPN\), page 4](#)
- [Feature Design of Dynamic Multipoint VPN \(DMVPN\), page 5](#)
- [IPsec Profiles, page 6](#)
- [VRF Integrated DMVPN, page 6](#)
- [DMVPN—Enabling Traffic Segmentation Within DMVPN, page 7](#)
- [NAT-Transparency Aware DMVPN, page 9](#)
- [Call Admission Control with DMVPN, page 10](#)
- [NHRP Rate-Limiting Mechanism, page 10](#)

Benefits of Dynamic Multipoint VPN (DMVPN)

Hub Router Configuration Reduction

- Currently, for each spoke router, there is a separate block of configuration lines on the hub router that define the crypto map characteristics, the crypto access list, and the GRE tunnel interface. This feature allows users to configure a single mGRE tunnel interface, a single IPsec profile, and no crypto access lists on the hub router to handle all spoke routers. Thus, the size of the configuration on the hub router remains constant even if spoke routers are added to the network.
- DMVPN architecture can group many spokes into a single multipoint GRE interface, removing the need for a distinct physical or logical interface for each spoke in a native IPsec installation.

Automatic IPsec Encryption Initiation

- GRE has the peer source and destination address configured or resolved with NHRP. Thus, this feature allows IPsec to be immediately triggered for the point-to-point GRE tunneling or when the GRE peer address is resolved via NHRP for the multipoint GRE tunnel.

Support for Dynamically Addressed Spoke Routers

- When using point-to-point GRE and IPsec hub-and-spoke VPN networks, the physical interface IP address of the spoke routers must be known when configuring the hub router because IP address must be configured as the GRE tunnel destination address. This feature allows spoke routers to have dynamic physical interface IP addresses (common for cable and DSL connections). When the spoke router comes online, it will send registration packets to the hub router: within these registration packets, is the current physical interface IP address of this spoke.

Dynamic Creation for Spoke-to-Spoke Tunnels

- This feature eliminates the need for spoke-to-spoke configuration for direct tunnels. When a spoke router wants to transmit a packet to another spoke router, it can now use NHRP to dynamically determine the required destination address of the target spoke router. (The hub router acts as the NHRP server, handling the request for the source spoke router.) The two spoke routers dynamically create an IPsec tunnel between them so data can be directly transferred.

VRF Integrated DMVPN

- DMVPNs can be used to extend the Multiprotocol Label Switching (MPLS) networks that are deployed by service providers to take advantage of the ease of configuration of hub and spokes, to provide support for dynamically addressed customer premises equipment (CPEs), and to provide zero-touch provisioning for adding new spokes into a DMVPN.

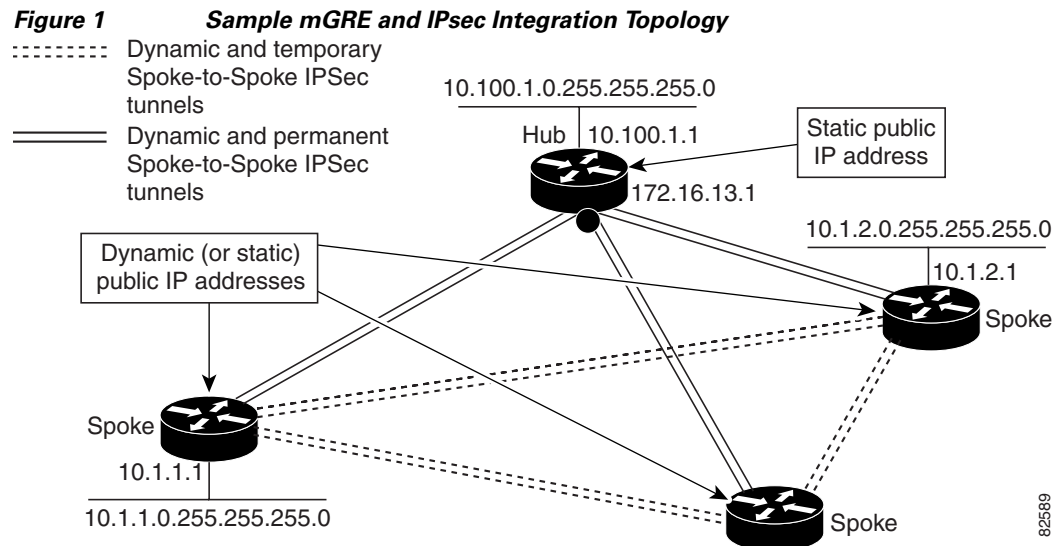
Feature Design of Dynamic Multipoint VPN (DMVPN)

The Dynamic Multipoint VPN (DMVPN) feature combines GRE tunnels, IPsec encryption, and NHRP routing to provide users an ease of configuration via crypto profiles—which override the requirement for defining static crypto maps—and dynamic discovery of tunnel endpoints.

This feature relies on the following two Cisco enhanced standard technologies:

- NHRP—A client and server protocol where the hub is the server and the spokes are the clients. The hub maintains an NHRP database of the public interface addresses of the each spoke. Each spoke registers its real address when it boots and queries the NHRP database for real addresses of the destination spokes to build direct tunnels.
- mGRE Tunnel Interface —Allows a single GRE interface to support multiple IPsec tunnels and simplifies the size and complexity of the configuration.

The topology shown in [Figure 1](#) and the corresponding bullets explain how this feature works.



- Each spoke has a permanent IPsec tunnel to the hub, not to the other spokes within the network. Each spoke registers as clients of the NHRP server.
- When a spoke needs to send a packet to a destination (private) subnet on another spoke, it queries the NHRP server for the real (outside) address of the destination (target) spoke.
- After the originating spoke “learns” the peer address of the target spoke, it can initiate a dynamic IPsec tunnel to the target spoke.
- The spoke-to-spoke tunnel is built over the multipoint GRE interface.

- The spoke-to-spoke links are established on demand whenever there is traffic between the spokes. Thereafter, packets can bypass the hub and use the spoke-to-spoke tunnel.

**Note**

After a preconfigured amount of inactivity on the spoke-to-spoke tunnels, the router will tear down those tunnels to save resources (IPsec security associations [SAs]).

IPsec Profiles

IPsec profiles abstract IPsec policy information into a single configuration entity, which can be referenced by name from other parts of the configuration. Therefore, users can configure functionality such as GRE tunnel protection with a single line of configuration. By referencing an IPsec profile, the user does not have to configure an entire crypto map configuration. An IPsec profile contains only IPsec information; that is, it does not contain any access list information or peering information.

VRF Integrated DMVPN

VPN Routing and Forwarding (VRF) Integrated DMVPN enables users to map DMVPN multipoint interfaces into MPLS VPNs. This mapping allows Internet service providers (ISPs) to extend their existing MPLS VPN services by mapping off-network sites (typically a branch office) to their respective MPLS VPNs. Customer equipment (CE) routers are terminated on the DMVPN PE router, and traffic is placed in the VRF instance of an MPLS VPN.

DMVPN can interact with MPLS VPNs in two ways:

1. The **ip vrf forwarding** command is used to inject the data IP packets (those packets inside the mGRE+IPsec tunnel) into the MPLS VPN. The **ip vrf forwarding** command is supported for DMVPN in Cisco IOS Release 12.3(6) and Release 12.3(7)T.
2. The **tunnel vrf** command is used to transport (route) the mGRE+IPsec tunnel packet itself within an MPLS VPN. The **tunnel vrf** command is supported in Cisco IOS Release 12.3(11)T but not in Cisco IOS Release 12.2(18)SXE.

**Note**

Clear-text data IP packets are forwarded in a VRF using the **ip vrf forwarding** command, and encrypted tunnel IP packets are forwarded in a VRF using the **tunnel vrf** command.

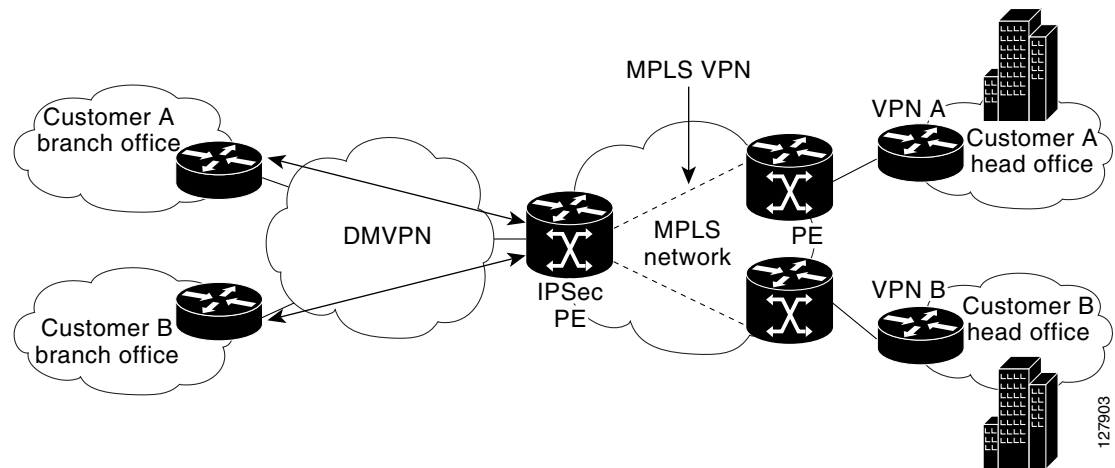
The **ip vrf forwarding** and **tunnel vrf** commands may be used at the same time. If they are used at the same time, the VRF name of each command may be the same or different.

For information about configuring the forwarding of clear-text data IP packets into a VRF, see the section “[Configuring the Forwarding of Clear-Text Data IP Packets into a VRF](#).” For information about configuring the forwarding of encrypted tunnel packets into a VRF, see the section “[Configuring the Forwarding of Encrypted Tunnel Packets into a VRF](#).”

For more information about configuring VRF, see reference in the “[Related Documents](#)” section.

[Figure 2](#) illustrates a typical VRF Integrated DMVPN scenario.

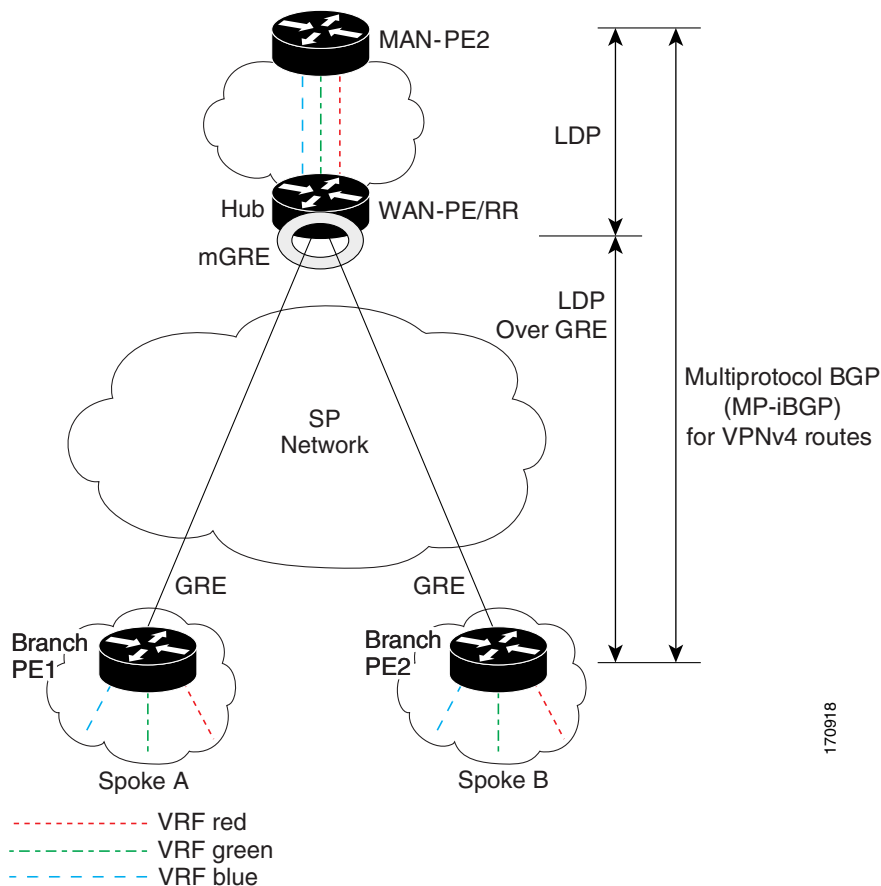
Figure 2 VRF Integrated DMVPN



DMVPN—Enabling Traffic Segmentation Within DMVPN

Cisco IOS Release 12.4(11)T provides an enhancement that allows you to segment VPN traffic within a DMVPN tunnel. VRF instances are labeled, using MPLS, to indicate their source and destination.

The diagram in [Figure 3](#) and the corresponding bullets explain how traffic segmentation within DMVPN works.

Figure 3 Traffic Segmentation with DMVPN

- The hub shown in the diagram is a WAN-PE and a route reflector, and the spokes (PE routers) are clients.
- There are three VRFs, designated “red,” “green,” and “blue.”
- Each spoke has both a neighbor relationship with the hub (multiprotocol Border Gateway Protocol [MP-iBGP] peering) and a GRE tunnel to the hub.
- Each spoke advertises its routes and VPNv4 prefixes to the hub.
- The hub sets its own IP address as the next-hop route for all the VPNv4 addresses it learns from the spokes and assigns a local MPLS label for each VPN when it advertises routes back to the spokes. As a result, traffic from Spoke A to Spoke B is routed via the hub.

An example illustrates the process:

1. Spoke A advertises a VPNv4 route to the hub, and applies the label *X* to the VPN.
2. The hub changes the label to *Y* when the hub advertises the route to Spoke B.
3. When Spoke B has traffic to send to Spoke A, it applies the *Y* label, and the traffic goes to the hub.
4. The hub swaps the VPN label, by removing the *Y* label and applying an *X* label, and sends the traffic to Spoke A.

NAT-Transparency Aware DMVPN

DMVPN spokes are often situated behind a NAT router (which is often controlled by the ISP for the spoke site) with the outside interface address of the spoke router being dynamically assigned by the ISP using a private IP address (per Internet Engineering Task Force [IETF] RFC 1918).

Prior to Cisco IOS Release 12.3(6) and 12.3(7)T, these spoke routers had to use IPsec tunnel mode to participate in a DMVPN network. In addition, their assigned outside interface private IP address had to be unique across the DMVPN network. Even though ISAKMP and IPsec would negotiate NAT-T and “learn” the correct NAT public address for the private IP address of this spoke, NHRP could only “see” and use the private IP address of the spoke for its mapping entries. Effective with the NAT-Transparency Aware DMVPN enhancement, NHRP can now learn and use the NAT public address for its mappings as long as IPsec transport mode is used (which is the recommended IPsec mode for DMVPN networks). The restriction that the private interface IP address of the spoke must be unique across the DMVPN network has been removed. It is recommended that all DMVPN routers be upgraded to the new code before you try to use the new functionality even though spoke routers that are not behind NAT do not need to be upgraded. In addition, you cannot convert upgraded spoke routers that are behind NAT to the new configuration (IPsec transport mode) until the hub routers have been upgraded.

Also added in Cisco IOS Releases 12.3(9a) and 12.3(11)T is the capability to have the hub DMVPN router behind static NAT. This was a change in the ISAKMP NAT-T support. For this functionality to be used, all the DMVPN spoke routers and hub routers must be upgraded, and IPsec must use transport mode.

For these NAT-Transparency Aware enhancements to work, you must use IPsec transport mode on the transform set. Also, even though NAT-Transparency (IKE and IPsec) can support two peers (IKE and IPsec) being translated to the same IP address (using the UDP ports to differentiate them), this functionality is not supported for DMVPN. All DMVPN spokes must have a unique IP address after they have been NAT translated. They can have the same IP address before they are NAT translated.

Figure 4 illustrates a NAT-Transparency Aware DMVPN scenario.



Note

In Cisco IOS Release 12.4(6)T or earlier, DMVPN spokes behind NAT *will not* participate in dynamic direct spoke-to-spoke tunnels. Any traffic to or from a spoke that is behind NAT will be forwarded using the DMVPN hub routers. DMVPN spokes that are not behind NAT in the same DMVPN network may create dynamic direct spoke-to-spoke tunnels between each other.

In Cisco IOS Release 12.4(6)T or later releases, DMVPN spokes behind NAT *will* participate in dynamic direct spoke-to-spoke tunnels. The spokes must be behind NAT boxes that are performing NAT, not PAT. The NAT box must translate the spoke to the same outside NAT IP address for the spoke-spoke connections as the NAT box does for the spoke-hub connection. If there is more than one DMVPN spoke behind the same NAT box, then the NAT box *must* translate the DMVPN spokes to different outside NAT IP addresses. It is also likely that you may not be able to build a direct spoke-spoke tunnel between these spokes. If a spoke-spoke tunnel fails to form, then the spoke-spoke packets will continue to be forwarded via the spoke-hub-spoke path.

Diagram illustrating a network topology for NAT (Network Address Translation) using a hub-and-spoke configuration.

The central hub router (192.168.0.1/24) is connected to two spoke routers, Spoke A (192.168.1.1/24) and Spoke B (192.168.2.1/24).

Spoke A is connected to a cloud representing the Internet (171.16.0.0/16). Spoke B is connected to a cloud representing the DMZ (172.16.0.0/16).

The hub router has a physical interface 172.17.0.1 and a tunnel interface 10.0.0.1. Spoke A has a physical interface 172.16.1.1 and a tunnel interface 10.0.0.11. Spoke B has a physical interface 172.16.2.1 and a tunnel interface 10.0.0.12.

NAT rules are shown:

- NAT: 171.16.1.1 → 172.18.101.1 (Spoke A)
- NAT: 171.16.2.1 → 172.18.102.2 (Spoke B)

How to Configure Dynamic Multipoint VPN (DMVPN)

To enable mGRE and IPsec tunneling for hub and spoke routers, you must configure an IPsec profile that uses a global IPsec policy template and configure your mGRE tunnel for IPsec encryption. This section contains the following procedures:

- [Configuring an IPsec Profile, page 11](#) (required)
- [Configuring the Hub for DMVPN, page 13](#) (required)
- [Configuring the Spoke for DMVPN, page 17](#) (required)
- [Configuring the Forwarding of Clear-Text Data IP Packets into a VRF, page 20](#) (optional)
- [Configuring the Forwarding of Encrypted Tunnel Packets into a VRF, page 21](#) (optional)
- [Configuring DMVPN—Traffic Segmentation Within DMVPN, page 22](#)
- [Troubleshooting Dynamic Multipoint VPN \(DMVPN\), page 27](#) (optional)

Configuring an IPsec Profile

The IPsec profile shares most of the same commands with the crypto map configuration, but only a subset of the commands are valid in an IPsec profile. Only commands that pertain to an IPsec policy can be issued under an IPsec profile; you cannot specify the IPsec peer address or the access control list (ACL) to match the packets that are to be encrypted.

Prerequisites

Before configuring an IPsec profile, you must define a transform set by using the **crypto ipsec transform-set** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **set transform-set** *transform-set-name*
5. **set identity**
6. **set security association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}
7. **set pfs** [**group1** | **group2**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec profile <i>name</i> Example: Router(config)# crypto ipsec profile vpnprof	Defines the IPsec parameters that are to be used for IPsec encryption between “spoke and hub” and “spoke and spoke” routers. This command enters crypto map configuration mode. <ul style="list-style-type: none"> The <i>name</i> argument specifies the name of the IPsec profile.
Step 4	set transform-set <i>transform-set-name</i> Example: Router(config-crypto-map)# set transform-set trans2	Specifies which transform sets can be used with the IPsec profile. <ul style="list-style-type: none"> The <i>transform-set-name</i> argument specifies the name of the transform set.
Step 5	set identity Example: Router(config-crypto-map)# set identity	(Optional) Specifies identity restrictions to be used with the IPsec profile.
Step 6	set security association lifetime {seconds <i>seconds</i> kilobytes <i>kilobytes</i>} Example: Router(config-crypto-map)# set security association lifetime seconds 1800	(Optional) Overrides the global lifetime value for the IPsec profile. <ul style="list-style-type: none"> The seconds <i>seconds</i> option specifies the number of seconds a security association will live before expiring; the kilobytes <i>kilobytes</i> option specifies the volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before that security association expires. The default for the <i>seconds</i> argument is 3600 seconds.
Step 7	set pfs [<i>group1</i> <i>group2</i>] Example: Router(config-crypto-map)# set pfs group2	(Optional) Specifies that IPsec should ask for perfect forward secrecy (PFS) when requesting new security associations for this IPsec profile. If this command is not specified, the default (group1) will be enabled. <ul style="list-style-type: none"> The group1 keyword specifies that IPsec should use the 768-bit Diffie-Hellman (DH) prime modulus group when performing the new DH exchange; the group2 keyword specifies the 1024-bit DH prime modulus group.

What to Do Next

Proceed to the following sections “[Configuring the Hub for DMVPN](#)” and “[Configuring the Spoke for DMVPN](#).”

Configuring the Hub for DMVPN

To configure the hub router for mGRE and IPsec integration (that is, associate the tunnel with the IPsec profile configured in the previous procedure), use the following commands:

**Note**

NHRP network IDs are locally significant and can be different. It makes sense from a deployment and maintenance perspective to use unique network ID numbers (using the **ip nhrp network-id** command) across all routers in a DMVPN network, but it is not necessary that they be the same.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** *ip-address mask [secondary]*
5. **ip mtu** *bytes*
6. **ip nhrp authentication** *string*
7. **ip nhrp map multicast dynamic**
8. **ip nhrp network-id** *number*
9. **tunnel source** {*ip-address* | *type number*}
10. **tunnel key** *key-number*
11. **tunnel mode gre multipoint**
12. **tunnel protection ipsec profile** *name*
13. **bandwidth** *kbps*
14. **ip tcp adjust-mss** *max-segment-size*
15. **ip nhrp holdtime** *seconds*
16. **delay** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel number Example: Router(config)# interface tunnel 5	Configures a tunnel interface and enters interface configuration mode <ul style="list-style-type: none"> The <i>number</i> argument specifies the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.
Step 4	ip address ip-address mask [secondary] Example: Router(config-if)# ip address 10.0.0.1 255.255.255.0	Sets a primary or secondary IP address for the tunnel interface. Note All hubs and spokes that are in the same DMVPN network must be addressed in the same IP subnet.
Step 5	ip mtu bytes Example: Router(config-if)# ip mtu 1400	Sets the maximum transmission unit (MTU) size, in bytes, of IP packets sent on an interface.
Step 6	ip nhrp authentication string Example: Router(config-if)# ip nhrp authentication donttell	Configures the authentication string for an interface using NHRP. Note The NHRP authentication string must be set to the same value on all hubs and spokes that are in the same DMVPN network.
Step 7	ip nhrp map multicast dynamic Example: Router(config-if)# ip nhrp map multicast dynamic	Allows NHRP to automatically add spoke routers to the multicast NHRP mappings.
Step 8	ip nhrp network-id number Example: Router(config-if)# ip nhrp network-id 99	Enables NHRP on an interface. <ul style="list-style-type: none"> The <i>number</i> argument specifies a globally unique 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.
Step 9	tunnel source {ip-address type number} Example: Router (config-if)# tunnel source Ethernet0	Sets source address for a tunnel interface.

	Command or Action	Purpose
Step 10	tunnel key <i>key-number</i> Example: Router (config-if)# tunnel key 100000	(Optional) Enables an ID key for a tunnel interface. <ul style="list-style-type: none"> The <i>key-number</i> argument specifies a number from 0 to 4,294,967,295 that identifies the tunnel key. Note The key number must be set to the same value on all hubs and spokes that are in the same DMVPN network. Note This command should not be configured if you are using a Cisco 6500 or Cisco 7600 platform.
Step 11	tunnel mode gre multipoint Example: Router(config-if)# tunnel mode gre multipoint	Sets the encapsulation mode to mGRE for the tunnel interface.
Step 12	tunnel protection ipsec profile <i>name</i> Example: Router(config-if)# tunnel protection ipsec profile vpnprof	Associates a tunnel interface with an IPsec profile. <ul style="list-style-type: none"> The <i>name</i> argument specifies the name of the IPsec profile; this value must match the <i>name</i> specified in the crypto ipsec profile name command.
Step 13	bandwidth <i>kbps</i> Example: Router(config-if)# bandwidth 1000	Sets the current bandwidth value for an interface to higher-level protocols. <ul style="list-style-type: none"> The <i>kbps</i> argument specifies the bandwidth in kilobits per second. The default value is 9. The recommend bandwidth value is 1000 or greater. Setting the bandwidth value to at least 1000 is critical if EIGRP is used over the tunnel interface. Higher bandwidth values may be necessary depending on the number of spokes supported by a hub.
Step 14	ip tcp adjust-mss <i>max-segment-size</i> Example: Router(config-if)# ip tcp adjust-mss 1360	Adjusts the maximum segment size (MSS) value of TCP packets going through a router. <ul style="list-style-type: none"> The <i>max-segment-size</i> argument specifies the maximum segment size, in bytes. The range is from 500 to 1460. The recommended value is 1360 when the number of IP MTU bytes is set to 1400. With these recommended settings, TCP sessions quickly scale back to 1400-byte IP packets so the packets will “fit” in the tunnel.

	Command or Action	Purpose
Step 15	ip nhrp holdtime <i>seconds</i> Example: Router(config-if)# ip nhrp holdtime 450	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses. <ul style="list-style-type: none">The <i>seconds</i> argument specifies the time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses. The recommended value ranges from 300 seconds to 600 seconds.
Step 16	delay <i>number</i> Example: Router(config-if)# delay 1000	(Optional) Used to change the EIGRP routing metric for routes learned over the tunnel interface. <ul style="list-style-type: none">The <i>number</i> argument specifies the delay time in seconds. The recommend value is 1000.

Configuring the Spoke for DMVPN

To configure spoke routers for mGRE and IPsec integration, use the following commands.

**Note**

NHRP network IDs are locally significant and can be different. It makes sense from a deployment and maintenance perspective to use unique network ID numbers (using the **ip nhrp network-id** command) across all routers in a DMVPN network, but it is not necessary that they be the same.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** *ip-address mask [secondary]*
5. **ip mtu** *bytes*
6. **ip nhrp authentication** *string*
7. **ip nhrp map** *hub-tunnel-ip-address hub-physical-ip-address*
8. **ip nhrp map multicast** *hub-physical-ip-address*
9. **ip nhrp nhs** *hub-tunnel-ip-address*
10. **ip nhrp network-id** *number*
11. **tunnel source** {*ip-address* | *type number*}
12. **tunnel key** *key-number*
13. **tunnel mode gre multipoint**
or
tunnel destination *hub-physical-ip-address*
14. **tunnel protection ipsec profile** *name*
15. **bandwidth** *kbps*
16. **ip tcp adjust-mss** *max-segment-size*
17. **ip nhrp holdtime** *seconds*
18. **delay** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel number Example: Router(config)# interface tunnel 5	Configures a tunnel interface and enters interface configuration mode. <ul style="list-style-type: none"> The <i>number</i> argument specifies the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.
Step 4	ip address ip-address mask [secondary] Example: Router(config-if)# ip address 10.0.0.2 255.255.255.0	Sets a primary or secondary IP address for the tunnel interface. Note All hubs and spokes that are in the same DMVPN network must be addressed in the same IP subnet.
Step 5	ip mtu bytes Example: Router(config-if)# ip mtu 1400	Sets the MTU size, in bytes, of IP packets sent on an interface.
Step 6	ip nhrp authentication string Example: Router(config-if)# ip nhrp authentication donttell	Configures the authentication string for an interface using NHRP. Note The NHRP authentication string be set to the same value on all hubs and spokes that are in the same DMVPN network.
Step 7	ip nhrp map hub-tunnel-ip-address hub-physical-ip-address Example: Router(config-if)# ip nhrp map 10.0.0.1 172.17.0.1	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an MBMA network. <ul style="list-style-type: none"> <i>hub-tunnel-ip-address</i>—Defines the NHRP server at the hub, which is permanently mapped to the static public IP address of the hub. <i>hub-physical-ip-address</i>—Defines the static public IP address of the hub.
Step 8	ip nhrp map multicast hub-physical-ip-address Example: Router(config-if)# ip nhrp map multicast 172.17.0.1	Enables the use of a dynamic routing protocol between the spoke and hub, and sends multicast packets to the hub router.

	Command or Action	Purpose
Step 9	ip nhrp nhs <i>hub-tunnel-ip-address</i> Example: Router(config-if)# ip nhrp nhs 10.0.0.1	Configures the hub router as the NHRP next-hop server.
Step 10	ip nhrp network-id <i>number</i> Example: Router(config-if)# ip nhrp network-id 99	Enables NHRP on an interface. <ul style="list-style-type: none"> The <i>number</i> argument specifies a globally unique 32-bit network identifier from a NBMA network. The range is from 1 to 4294967295.
Step 11	tunnel source { <i>ip-address</i> <i>type number</i> } Example: Router (config-if)# tunnel source Ethernet0	Sets the source address for a tunnel interface.
Step 12	tunnel key <i>key-number</i> Example: Router (config-if)# tunnel key 100000	(Optional) Enables an ID key for a tunnel interface. <ul style="list-style-type: none"> The <i>key-number</i> argument specifies a number from 0 to 4,294,967,295 that identifies the tunnel key. The key number must be set to the same value on all hubs and spokes that are in the same DMVPN network. Note This command should not be configured if you are using a Cisco 6500 or Cisco 7600 platform.
Step 13	tunnel mode gre multipoint or tunnel destination <i>hub-physical-ip-address</i> Example: Router(config-if)# tunnel mode gre multipoint or Router(config-if)# tunnel destination 172.17.0.1	Sets the encapsulation mode to mGRE for the tunnel interface. Use this command if data traffic can use dynamic spoke-to-spoke traffic. Specifies the destination for a tunnel interface. Use this command if data traffic can use hub-and-spoke tunnels.
Step 14	tunnel protection ipsec profile <i>name</i> Example: Router(config-if)# tunnel protection ipsec profile vpnprof	Associates a tunnel interface with an IPsec profile. <ul style="list-style-type: none"> The <i>name</i> argument specifies the name of the IPsec profile; this value must match the <i>name</i> specified in the crypto ipsec profile name command.
Step 15	bandwidth <i>kbps</i> Example: Router(config-if)# bandwidth 1000	Sets the current bandwidth value for an interface to higher-level protocols. <ul style="list-style-type: none"> The <i>kbps</i> argument specifies the bandwidth in kilobits per second. The default value is 9. The recommend bandwidth value is 1000 or greater. The bandwidth setting for the spoke does not need to equal the bandwidth setting for the DMVPN hub. It is usually easier if all of the spokes use the same or similar value.

	Command or Action	Purpose
Step 16	ip tcp adjust-mss <i>max-segment-size</i> Example: Router(config-if)# ip tcp adjust-mss 1360	Adjusts the maximum segment size (MSS) value of TCP packets going through a router. <ul style="list-style-type: none"> The <i>max-segment-size</i> argument specifies the maximum segment size, in bytes. The range is from 500 to 1460. The recommended number value is 1360 when the number of IP MTU bytes is set to 1400. With these recommended settings, TCP sessions quickly scale back to 1400-byte IP packets so the packets will “fit” in the tunnel.
Step 17	ip nhrp holdtime <i>seconds</i> Example: Router(config-if)# ip nhrp holdtime 450	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses. <ul style="list-style-type: none"> The <i>seconds</i> argument specifies the time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses. The recommended value ranges from 300 seconds to 600 seconds.
Step 18	delay <i>number</i> Example: Router(config-if)# delay 1000	(Optional) Used to change the EIGRP routing metric for routes learned over the tunnel interface. <ul style="list-style-type: none"> The <i>number</i> argument specifies the delay time in seconds. The recommend value is 1000.

Configuring the Forwarding of Clear-Text Data IP Packets into a VRF

To configure the forwarding of clear-text data IP packets into a VRF, perform the following steps. This configuration assumes that the VRF BLUE has already been configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: Router> enable	Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	interface <i>type number</i>	Configures an interface type and enters interface configuration mode.
	Example: Router (config)# interface tunnel0	
Step 4	ip vrf forwarding <i>vrf-name</i>	Associates a VPN VRF with an interface or subinterface.
	Example: Router (config-if)# ip vrf forwarding BLUE	

Configuring the Forwarding of Encrypted Tunnel Packets into a VRF

To configure the forwarding of encrypted tunnel packets into a VRF, perform the following steps. This configuration assumes that the VRF RED has already been configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. interface *type number*
4. **tunnel vrf** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: Router> enable	Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	<code>interface type number</code> Example: Router (config)# interface tunnel0	Configures an interface type and enters interface configuration mode.
Step 4	<code>tunnel vrf vrf-name</code> Example: Router (config-if)# tunnel vrf RED	Associates a VPN VRF instance with a specific tunnel destination, interface, or subinterface.

Configuring DMVPN—Traffic Segmentation Within DMVPN

There are no new commands to use for configuring traffic segmentation, but there are tasks you must complete in order to segment traffic within a DMVPN tunnel:

- [Enabling MPLS on the VPN Tunnel, page 22](#)
- [Configuring Multiprotocol BGP on the Hub Router, page 23](#)
- [Configuring Multiprotocol BGP on the Spoke Routers, page 25](#)

Prerequisites

The tasks that follow assume that the DMVPN tunnel and the VRFs “red” and “blue” have already been configured.

For information on configuring a DMVPN tunnel, see the “[Configuring the Hub for DMVPN](#)” section on [page 13](#) and the “[Configuring the Spoke for DMVPN](#)” section on [page 17](#). For details about VRF configuration, see the “[Configuring the Forwarding of Clear-Text Data IP Packets into a VRF](#)” section on [page 20](#) and the “[Configuring the Forwarding of Encrypted Tunnel Packets into a VRF](#)” section on [page 21](#).

Enabling MPLS on the VPN Tunnel

Because traffic segmentation within a DMVPN tunnel depends upon MPLS, you must configure MPLS for each VRF instance in which traffic will be segmented. For detailed information about configuring MPLS, see [Cisco IOS Multiprotocol Label Switching Configuration Guide](#), Release 12.4.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. `interface type number`
4. **mpls ip**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: Router> enable	Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	interface type number	Configures an interface type and enters interface configuration mode.
	Example: Router (config)# interface tunnel0	
Step 4	mpls ip	Enables MPLS tagging of packets on the specified tunnel interface.
	Example: Router (config-if)# mpls ip	

Configuring Multiprotocol BGP on the Hub Router

You must configure multiprotocol iBGP (MP-iBGP) to enable advertisement of VPNv4 prefixes and labels to be applied to the VPN traffic. Use BGP to configure the hub as a route reflector. To force all traffic to be routed via the hub, configure the BGP route reflector to change the next hop to itself when it advertises VPNv4 prefixes to the route reflector clients (spokes).

For more information about the BGP routing protocol, see the “BGP” chapter in the *Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp**
4. **neighbor ipaddress remote-as as-number**
5. **neighbor ipaddress update-source interface**
6. **address-family vpnv4**
7. **neighbor ipaddress activate**
8. **neighbor ipaddress send-community extended**
9. **neighbor ipaddress route-reflector-client**
10. **neighbor ipaddress route-map nexthop out**
11. **exit-address family**
12. **address-family ipv4 vrf-name**

13. redistribute connected
14. route-map
15. set ip next-hop *ipaddress*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router bgp Example: Router (config)# router bgp	Enters BGP configuration mode.
Step 4	neighbor ipaddress remote-as as-number Example: Router (config)# neighbor 10.0.0.11 remote-as 1	Adds an entry to the BGP or multiprotocol BGP neighbor table.
Step 5	neighbor ipaddress update-source interface Example: Router (config)# neighbor 10.10.10.11 update-source Tunnell	Configures the Cisco IOS software to allow BGP sessions to use any operational interface for TCP connections.
Step 6	address-family vpnv4 Example: Router (config)# address-family vpnv4	Enters address family configuration mode to configure a routing session using Virtual Private Network (VPN) Version 4 address prefixes.
Step 7	neighbor ipaddress activate Example: Router (config)# neighbor 10.0.0.11 activate	Enables the exchange of information with a BGP neighbor.
Step 8	neighbor ipaddress send-community extended Example: Router (config)# neighbor 10.0.0.11 send-community extended	Specifies that extended community attributes should be sent to a BGP neighbor.

	Command or Action	Purpose
Step 9	neighbor <i>ipaddress</i> route-reflector-client Example: Router (config)# neighbor 10.0.0.11 route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
Step 10	neighbor <i>ipaddress</i> route-map <i>nexthop</i> out Example: Router (config)# neighbor 10.0.0.11 route-map nexthop out	Forces all traffic to be routed via the hub.
Step 11	exit-address-family Example: Router (config)# exit-address-family	Exits the address family configuration mode for VPNv4.
Step 12	address-family <i>ipv4</i> <i>vrf-name</i> Example: Router (config)# address-family ipv4 vrf red	Enters address family configuration mode to configure a routing session using standard IP Version 4 address prefixes.
Step 13	redistribute connected Example: Router (config)# redistribute connected	Redistributes routes that are established automatically by virtue of having enabled IP on an interface from one routing domain into another routing domain.
Step 14	route-map Example: Router (config)# route-map nexthop permit 10	Enters route map configuration mode to configure the next-hop that will be advertised to the spokes.
Step 15	set ip next-hop <i>ipaddress</i> Example: Router (config)# set ip next-hop 10.0.0.1	Sets the next hop to be the hub.

Configuring Multiprotocol BGP on the Spoke Routers

Multiprotocol-iBGP (MP-iBGP) must be configured on the spoke routers and the hub. Follow the steps below for each spoke router in the DMVPN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp**
4. **neighbor *ipaddress* remote-as *as-number***
5. **neighbor *ipaddress* update-source *interface***
6. **address-family vpnv4**

7. **neighbor ipaddress activate**
8. **neighbor ipaddress send-community extended**
9. **exit-address-family**
10. **address-family ipv4 vrf-name**
11. **redistribute connected**
12. **exit-address-family**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router bgp Example: Router (config)# router bgp 1	Enters BGP configuration mode.
Step 4	neighbor ipaddress remote-as as-number Example: Router (config)# neighbor 10.0.0.1 remote-as 1	Adds an entry to the BGP or multiprotocol BGP neighbor table.
Step 5	neighbor ipaddress update-source interface Example: Router (config)# neighbor 10.10.10.1 update-source Tunnell	Configures the Cisco IOS software to allow BGP sessions to use any operational interface for TCP connections.
Step 6	address-family vpngv4 Example: Router (config)# address-family vpngv4	Enters address family configuration mode to configure a routing session using Virtual Private Network (VPN) Version 4 address prefixes.
Step 7	neighbor ipaddress activate Example: Router (config)# neighbor 10.0.0.1 activate	Enables the exchange of information with a BGP neighbor.
Step 8	neighbor ipaddress send-community extended Example: Router (config)# neighbor 10.0.0.1 send-community extended	Specifies that extended community attributes should be sent to a BGP neighbor.

	Command or Action	Purpose
Step 9	exit-address-family Example: Router (config)# exit-address-family	Exits the address family configuration mode.
Step 10	address-family ipv4 vrf-name Example: Router (config)# address-family ipv4 vrf red	Enters address family configuration mode to configure a routing session using standard IP Version 4 address prefixes.
Step 11	redistribute connected Example: Router (config)# redistribute connected	Redistributes routes that are established automatically by virtue of having enabled IP on an interface from one routing domain into another routing domain.
Step 12	exit-address-family Example: Router (config)# exit-address-family	Exits the address family configuration mode. Note Repeat Steps 10–12 for each VRF.

Troubleshooting Dynamic Multipoint VPN (DMVPN)

After configuring DMVPN, to verify that DMVPN is operating correctly, to clear DMVPN statistics or sessions, or to debug DMVPN, you may perform the following optional steps:

SUMMARY STEPS

1. **clear dmvpn session** [peer {nbma | tunnel} ip-address] [interface {tunnel number}] [vrf vrf-name] [static]
2. **clear dmvpn statistics** [peer {nbma | tunnel} ip-address] [interface {tunnel number}] [vrf vrf-name]
3. **debug dmvpn** {[condition [unmatched] | [peer [nbma | tunnel {ip-address}]] | [vrf {vrf-name}]] | [interface {tunnel number}]} | [{error | detail | packet | all} {nhrp | crypto | tunnel | socket | all}]}
4. **debug nhrp condition**
5. **debug nhrp error**
6. **logging dmvpn** [rate-limit seconds]
7. **show crypto ipsec sa** [active | standby]
8. **show crypto isakmp sa**
9. **show crypto map**
10. **show dmvpn** [peer [nbma | tunnel {ip-address}] | [network {ip-address} {mask}]] [vrf {vrf-name}] [interface {tunnel number}] [detail] [static] [debug-condition]
11. **show ip nhrp traffic** [interface {tunnel number}]

DETAILED STEPS

-
- Step 1** The **clear dmvpn session** command is used to clear DMVPN sessions.
- The following example clears only dynamic DMVPN sessions:
- ```
Router# clear dmvpn session peer nbma
```
- The following example clears all DMVPN sessions, both static and dynamic, for the specified tunnel:
- ```
Router# clear dmvpn session interface tunnel 100 static
```
- Step 2** The **clear dmvpn statistics** command is used to clear DMVPN related counters. The following example shows how to clear DMVPN related session counters for the specified tunnel interface:
- ```
Router# clear dmvpn statistics peer tunnel 192.0.2.3
```
- Step 3** The **debug dmvpn** command is used to debug DMVPN sessions. You can enable or disable DMVPN debugging based on a specific condition. There are three levels of DMVPN debugging, listed in the order of details from lowest to highest:
- Error level
  - Detail level
  - Packet level
- The following example shows how to enable conditional DMVPN debugging that displays all error debugs for next hop routing protocol (NHRP), sockets, tunnel protection and crypto information:
- ```
Router# debug dmvpn error all
```
- Step 4** The **debug nhrp condition** command enables or disables debugging based on a specific condition. The following example shows how to enable conditional NHRP debugging:
- ```
Router# debug nhrp condition
```
- Step 5** The **debug nhrp error** command displays information about NHRP error activity. The following example shows how to enable debugging for NHRP error messages:
- ```
Router# debug nhrp error
```
- Step 6** The **logging dmvpn** command is used to enable DMVPN system logging. The following command shows how to enable DMVPN system logging at the rate of 1 message every 20 seconds:
- ```
Router(config)# logging dmvpn rate-limit 20
```
- The following example shows a sample system log with DMVPN messages:
- ```
%DMVPN-7-CRYPTO_SS: Tunnel101-192.0.2.1 socket is UP
%DMVPN-5-NHRP_NHS: Tunnel101 192.0.2.251 is UP
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel1 Registered.
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel101 came UP.
%DMVPN-3-NHRP_ERROR: Registration Request failed for 192.0.2.251 on Tunnel101
```
- Step 7** The **show crypto ipsec sa** command displays the settings used by the current SAs. The following example output shows the IPsec SA status of only the active device:
- ```
Router# show crypto ipsec sa active

interface: Ethernet0/0
 Crypto map tag: to-peer-outside, local addr 209.165.201.3
 protected vrf: (none)
 local ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
 remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
 current_peer 209.165.200.225 port 500
 PERMIT, flags={origin_is_acl,}
 #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
```

```
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 209.165.201.3, remote crypto endpt.: 209.165.200.225
path mtu 1500, media mtu 1500
current outbound spi: 0xD42904F0(3559458032)
inbound esp sas:
spi: 0xD3E9ABD0(3555306448)
transform: esp-3des ,
in use settings ={Tunnel, }
conn id: 2006, flow_id: 6, crypto map: to-peer-outside
sa timing: remaining key lifetime (k/sec): (4586265/3542)
HA last key lifetime sent(k): (4586267)
ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

**Step 8** The **show crypto isakmp sa** command displays all current IKE SAs at a peer. For example, the following sample output is displayed after IKE negotiations have successfully completed between two peers.

Router# **show crypto isakmp sa**

| dst           | src           | state   | conn-id | slot |
|---------------|---------------|---------|---------|------|
| 172.17.63.19  | 172.16.175.76 | QM_IDLE | 2       | 0    |
| 172.17.63.19  | 172.17.63.20  | QM_IDLE | 1       | 0    |
| 172.16.175.75 | 172.17.63.19  | QM_IDLE | 3       | 0    |

**Step 9** The **show crypto map** command displays the crypto map configuration.

The following sample output is displayed after a crypto map has been configured:

Router# **show crypto map**

```
Crypto Map "Tunnel5-head-0" 10 ipsec-isakmp
 Profile name: vpnprof
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={trans2, }

Crypto Map "Tunnel5-head-0" 20 ipsec-isakmp
 Map is a PROFILE INSTANCE.
 Peer = 172.16.175.75
 Extended IP access list
 access-list permit gre host 172.17.63.19 host 172.16.175.75
 Current peer: 172.16.175.75
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={trans2, }

Crypto Map "Tunnel5-head-0" 30 ipsec-isakmp
 Map is a PROFILE INSTANCE.
 Peer = 172.17.63.20
 Extended IP access list
 access-list permit gre host 172.17.63.19 host 172.17.63.20
 Current peer: 172.17.63.20
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={trans2, }

Crypto Map "Tunnel5-head-0" 40 ipsec-isakmp
 Map is a PROFILE INSTANCE.
 Peer = 172.16.175.76
```

```

Extended IP access list
 access-list permit gre host 172.17.63.19 host 172.16.175.76
Current peer: 172.16.175.76
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={trans2, }
Interfaces using crypto map Tunnel5-head-0:
Tunnel5

```

**Step 10** The **show dmvpn** command displays DMVPN specific session information. The following example shows example summary output:

```

Router# show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
 N - NATed, L - Local, X - No Socket
 # Ent --> Number of NHRP entries with same NBMA peer

! The line below indicates that the sessions are being displayed for Tunnel1.
! Tunnel1 is acting as a spoke and is a peer with three other NBMA peers.

Tunnel1, Type: Spoke, NBMA Peers: 3,
Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb

 2 192.0.2.21 192.0.2.116 IKE 3w0d D
 1 192.0.2.102 192.0.2.11 NHRP 02:40:51 S
 1 192.0.2.225 192.0.2.10 UP 3w0d S

Tunnel2, Type: Spoke, NBMA Peers: 1,
Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb

 1 192.0.2.25 192.0.2.171 IKE never S

```

**Step 11** The **show ip nhrp traffic** command displays NHRP statistics. The following example shows output for a specific tunnel, tunnel7:

```

Router# show ip nhrp traffic interface tunnel7

Tunnel7: Max-send limit:100Pkts/10Sec, Usage:0%
Sent: Total 79
 18 Resolution Request 10 Resolution Reply 42 Registration Request
 0 Registration Reply 3 Purge Request 6 Purge Reply
 0 Error Indication 0 Traffic Indication
Rcvd: Total 69
 10 Resolution Request 15 Resolution Reply 0 Registration Request
 36 Registration Reply 6 Purge Request 2 Purge Reply
 0 Error Indication 0 Traffic Indication

```

## What to Do Next

If you have troubleshooted your DMVPN configuration and proceed to contact technical support, the **show tech-support** command includes information for DMVPN sessions. For more information, see the **show tech-support** command in the Cisco IOS Configuration Fundamentals Command Reference.

# Configuration Examples for Dynamic Multipoint VPN (DMVPN) Feature

This section provides the following comprehensive configuration examples:

- [Hub Configuration for DMVPN: Example, page 31](#)
- [Spoke Configuration for DMVPN: Example, page 32](#)
- [VRF Aware DMVPN: Example, page 33](#)

## Hub Configuration for DMVPN: Example

In the following example, which configures the hub router for multipoint GRE and IPsec integration, no explicit configuration lines are needed for each spoke; that is, the hub is configured with a global IPsec policy template that all spoke routers can talk to. In this example, EIGRP is configured to run over the private physical interface and the tunnel interface.

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
! Ensures longer packets are fragmented before they are encrypted; otherwise, the
receiving router would have to do the reassembly.
 ip mtu 1400
! The following line must match on all nodes that "want to use" this mGRE tunnel:
 ip nhrp authentication donttell
! Note that the next line is required only on the hub.
 ip nhrp map multicast dynamic
! The following line must match on all nodes that want to use this mGRE tunnel:
 ip nhrp network-id 99
 ip nhrp holdtime 300
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
advertise routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
! Enables dynamic, direct spoke-to-spoke tunnels when using EIGRP.
 no ip next-hop-self eigrp 1
 ip tcp adjust-mss 1360
 delay 1000
! Sets IPsec peer address to Ethernet interface's public address.
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
```

```

!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
!

```

For information about defining and configuring ISAKMP profiles, see the references in the ["Related Documents"](#) section.

## Spoke Configuration for DMVPN: Example

In the following example, all spokes are configured the same except for tunnel and local interface address, thereby, reducing necessary configurations for the user:

```

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
! The following line must match on all nodes that want to use this mGRE tunnel:
 ip nhrp authentication donttell
! Definition of NHRP server at the hub (10.0.0.1), which is permanently mapped to the
static public address of the hub (172.17.0.1).
 ip nhrp map 10.0.0.1 172.17.0.1
! Sends multicast packets to the hub router, and enables the use of a dynamic routing
protocol between the spoke and the hub.
 ip nhrp map multicast 172.17.0.1
! The following line must match on all nodes that want to use this mGRE tunnel:
 ip nhrp network-id 99
 ip nhrp holdtime 300
! Configures the hub router as the NHRP next-hop server.
 ip nhrp nhs 10.0.0.1
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel:
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
! This is a spoke, so the public address might be dynamically assigned via DHCP.
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
! EIGRP is configured to run over the inside physical interface and the tunnel.
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255

```



## VRF Aware DMVPN: Example

When configuring VRF Aware DMVPN, you must create a separate DMVPN network for each VRF instance. In the following example, there are two DMVPN networks: BLUE and RED. In addition, a separate source interface has been used on the hub for each DMVPN tunnel—a must for Cisco IOS Release 12.2(18)SXE. For other Cisco IOS releases, you can configure the same tunnel source for both of the tunnel interfaces, but you must configure the **tunnel key** and **tunnel protection (tunnel protection ipsec profile {name} shared)** commands.



### Note

If you use the **shared** keyword, then you should be running Cisco IOS Release 12.4(5) or Release 12.4(6)T, or a later release. Otherwise the IPsec/GRE tunnels under the two mGRE tunnel interfaces may not function correctly.

### Hub Configuration

```
interface Tunnel0
! Note the next line.
 ip vrf forwarding BLUE
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1436
 ! Note the next line.
 ip nhrp authentication BLUE!KEY
 ip nhrp map multicast dynamic
 ! Note the next line
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 ip tcp adjust-mss 1360
 delay 1000
 ! Note the next line.
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel protection ipsec profile vpnprof!
interface Tunnel1
! Note the next line.
 ip vrf forwarding RED
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1436
 ! Note the next line.
 ip nhrp authentication RED!KEY
 ip nhrp map multicast dynamic
 ! Note the next line.
 ip nhrp network-id 20000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 ip tcp adjust-mss 1360
 delay 1000
 ! Note the next line.
 tunnel source Ethernet1
 tunnel mode gre multipoint
 tunnel protection ipsec profile vpnprof!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
```

```
ip address 192.0.2.171 255.255.255.0
```

**Note**

For the hub configuration shown above, a separate DMVPN network is configured for each VPN. The NHRP network ID and authentication keys must be unique on the two mGRE interfaces.

**EIGRP Configuration on the Hub**

```
router eigrp 1
auto-summary
!
address-family ipv4 vrf BLUE
network 10.0.0.0 0.0.0.255
no auto-summary
autonomous-system 1
exit-address-family
!
address-family ipv4 vrf RED
network 10.0.0.0 0.0.0.255
no auto-summary
autonomous-system 1
exit-address-family
```

**Spoke Configurations****Spoke 1:**

```
interface Tunnel0
bandwidth 1000
ip address 10.0.0.2 255.255.255.0
ip mtu 1436
! Note the next line.
ip nhrp authentication BLUE!KEY
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
ip tcp adjust-mss 1360
delay 1000
tunnel mode gre multipoint
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel protection ipsec profile vpnprof
```

**Spoke 2:**

```
interface Tunnel0
bandwidth 1000
ip address 10.0.0.2 255.255.255.0
ip mtu 1436
ip nhrp authentication RED!KEY
ip nhrp map 10.0.0.1 192.0.2.171
ip nhrp network-id 200000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
ip tcp adjust-mss 1360
delay 1000
tunnel source Ethernet0
tunnel destination 192.0.2.171
tunnel protection ipsec profile vpnprof!
```

## 2547oDMVPN with Traffic Segmentation (with BGP only): Example

The following example show a traffic segmentation configuration in which traffic is segmented between two spokes that serve as provider edge (PE) devices.

### Hub Configuration

```
hostname hub-pe1

boot-start-marker
boot-end-marker

no aaa new-model

resource policy

clock timezone EST 0
ip cef
no ip domain lookup

!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t1 esp-des
 mode transport

crypto ipsec profile prof
 set transform-set t1

interface Tunnel1
 ip address 10.9.9.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 1

!The command below enables MPLS on the DMVPN network:
mpls ip
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile prof

interface Loopback0
 ip address 10.0.0.1 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.1 255.255.255.0
```

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop information to set itself as the next-hop and assigns a new VPN label for the prefixes learned from the spokes and advertises the VPN prefix:

```
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.11 remote-as 1
 neighbor 10.0.0.11 update-source Tunnel1
 neighbor 10.0.0.12 remote-as 1
 neighbor 10.0.0.12 update-source Tunnel1
 no auto-summary

 address-family vpnv4
 neighbor 10.0.0.11 activate
 neighbor 10.0.0.11 send-community extended
 neighbor 10.0.0.11 route-reflector-client
 neighbor 10.0.0.11 route-map NEXTHOP out
 neighbor 10.0.0.12 activate
 neighbor 10.0.0.12 send-community extended
 neighbor 10.0.0.12 route-reflector-client
 neighbor 10.0.0.12 route-map NEXTHOP out
 exit-address-family

 address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit-address-family

 address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit-address-family
```

```
no ip http server
no ip http secure-server
```

!In this route map information, the hub sets the next hop to itself, and the VPN prefixes are advertised:

```
route-map NEXTHOP permit 10
 set ip next-hop 10.0.0.1
```

```
control-plane
```

```
line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login
```

```
end
```

## Spoke Configurations

### Spoke 2

```
hostname spoke-pe2

boot-start-marker
boot-end-marker

no aaa new-model
```

```
resource policy

clock timezone EST 0
ip cef
no ip domain lookup

!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t1 esp-des
 mode transport

crypto ipsec profile prof
 set transform-set t1

interface Tunnel1
 ip address 10.0.0.11 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map 10.0.0.1 172.0.0.1
 ip nhrp map multicast 172.0.0.1
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1

!The command below enables MPLS on the DMVPN network:
mpls ip
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile prof

interface Loopback0
 ip address 10.9.9.11 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.11 255.255.255.0
!
```

```

!
interface Ethernet1/0
 ip vrf forwarding red
 ip address 192.168.11.2 255.255.255.0

interface Ethernet2/0
 ip vrf forwarding blue
 ip address 192.168.11.2 255.255.255.0

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 1
 neighbor 10.0.0.1 update-source Tunnel1
 no auto-summary

 address-family vpnv4
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.1 send-community extended
 exit-address-family

!
 address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit-address-family

!
 address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit-address-family

no ip http server
no ip http secure-server

control-plane

line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login

end

```

### Spoke 3

```

hostname spoke-PE3

boot-start-marker
boot-end-marker

no aaa new-model

resource policy

clock timezone EST 0
ip cef
no ip domain lookup

```

```
!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t1 esp-des
 mode transport

crypto ipsec profile prof
 set transform-set t1

interface Tunnel1
 ip address 10.0.0.12 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map 10.0.0.1 172.0.0.1
 ip nhrp map multicast 172.0.0.1
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1

!The command below enables MPLS on the DMVPN network:
mpls ip
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile prof
!
interface Loopback0
 ip address 10.9.9.12 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.12 255.255.255.0

interface Ethernet1/0
 ip vrf forwarding red
 ip address 192.168.12.2 255.255.255.0

interface Ethernet2/0
 ip vrf forwarding blue
 ip address 192.168.12.2 255.255.255.0

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 1
 neighbor 10.0.0.1 update-source Tunnel1
 no auto-summary
```

```

address-family vpnv4
neighbor 10.0.0.1 activate
neighbor 10.0.0.1 send-community extended
exit-address-family

address-family ipv4 vrf red
redistribute connected
no synchronization
exit-address-family

address-family ipv4 vrf blue
redistribute connected
no synchronization
exit-address-family

no ip http server
no ip http secure-server

control-plane

line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login

end

```

## 2547oDMVPN with Traffic Segmentation (Enterprise Branch): Example

The following example shows a configuration for segmenting traffic between two spokes located at branch offices of an enterprise. In this example, EIGRP is configured to learn routes to reach BGP neighbors within the DMVPN.

### Hub Configuration

```

hostname HUB

boot-start-marker
boot-end-marker

no aaa new-model

resource policy

clock timezone EST 0
ip cef
no ip domain lookup

!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

```



```
!This refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t1 esp-des
 mode transport

crypto ipsec profile prof
 set transform-set t1

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 1

!EIGRP is enabled on the DMVPN network to learn the IGP prefixes:
no ip split-horizon eigrp 1

!The command below enables MPLS on the DMVPN network:
mpls ip
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile prof

!This address is advertised by EIGRP and used as the BGP endpoint:
interface Loopback0
 ip address 10.9.9.1 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.1 255.255.255.0

!EIGRP is configured to learn the BGP peer addresses (10.9.9.x networks)
router eigrp 1
 network 10.9.9.1 0.0.0.0
 network 10.0.0.0 0.0.0.255
 no auto-summary

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp router-id 10.9.9.1
 bgp log-neighbor-changes
 neighbor 10.9.9.11 remote-as 1
 neighbor 10.9.9.11 update-source Loopback0
 neighbor 10.9.9.12 remote-as 1
 neighbor 10.9.9.12 update-source Loopback0
 no auto-summary

address-family vpnv4
 neighbor 10.9.9.11 activate
 neighbor 10.9.9.11 send-community extended
 neighbor 10.9.9.11 route-reflector-client
```

```

neighbor 10.9.9.12 activate
neighbor 10.9.9.12 send-community extended
neighbor 10.9.9.12 route-reflector-client
exit-address-family

address-family ipv4 vrf red
redistribute connected
no synchronization
exit-address-family

address-family ipv4 vrf blue
redistribute connected
no synchronization
exit-address-family

no ip http server
no ip http secure-server

control-plane

line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login

end

```

## Spoke Configurations

### Spoke 2

```

hostname Spoke2

boot-start-marker
boot-end-marker

no aaa new-model

resource policy

clock timezone EST 0
ip cef
no ip domain lookup

!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

```

```
crypto ipsec transform-set t1 esp-des
mode transport

crypto ipsec profile prof
set transform-set t1

interface Tunnel1
 ip address 10.0.0.11 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map 10.0.0.1 172.0.0.1
 ip nhrp map multicast 172.0.0.1
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1

!The command below enables MPLS on the DMVPN network:
mpls ip
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile prof

!This address is advertised by EIGRP and used as the BGP endpoint:
interface Loopback0
 ip address 10.9.9.11 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.11 255.255.255.0

interface Ethernet1/0
 ip vrf forwarding red
 ip address 192.168.11.2 255.255.255.0

interface Ethernet2/0
 ip vrf forwarding blue
 ip address 192.168.11.2 255.255.255.0

!EIGRP is enabled on the DMVPN network to learn the IGP prefixes:
router eigrp 1
 network 10.9.9.11 0.0.0.0
 network 10.0.0.0 0.0.0.255
 no auto-summary

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp router-id 10.9.9.11
 bgp log-neighbor-changes
 neighbor 10.9.9.1 remote-as 1
 neighbor 10.9.9.1 update-source Loopback0
 no auto-summary

address-family vpnv4
 neighbor 10.9.9.1 activate
 neighbor 10.9.9.1 send-community extended
 exit-address-family

address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit-address-family
```

```

 address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit-address-family

no ip http server
no ip http secure-server

control-plane

line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login

end

```

### Spoke 3

```

hostname Spoke3

boot-start-marker
boot-end-marker

no aaa new-model

resource policy

clock timezone EST 0
ip cef
no ip domain lookup

!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t1 esp-des
 mode transport

crypto ipsec profile prof
 set transform-set t1

interface Tunnell
 ip address 10.0.0.12 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic

```

```
ip nhrp map 10.0.0.1 172.0.0.1
ip nhrp map multicast 172.0.0.1
ip nhrp network-id 1
ip nhrp nhs 10.0.0.1

!The command below enables MPLS on the DMVPN network:
mpls ip
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile prof

!This address is advertised by EIGRP and used as the BGP endpoint:
interface Loopback0
 ip address 10.9.9.12 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.12 255.255.255.0

interface Ethernet1/0
 ip vrf forwarding red
 ip address 192.168.12.2 255.255.255.0

interface Ethernet2/0
 ip vrf forwarding blue
 ip address 192.168.12.2 255.255.255.0

!EIGRP is enabled on the DMVPN network to learn the IGP prefixes:
router eigrp 1
 network 10.9.9.12 0.0.0.0
 network 10.0.0.0 0.0.0.255
 no auto-summary

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp router-id 10.9.9.12
 bgp log-neighbor-changes
 neighbor 10.9.9.1 remote-as 1
 neighbor 10.9.9.1 update-source Loopback0
 no auto-summary

address-family vpnv4
 neighbor 10.9.9.1 activate
 neighbor 10.9.9.1 send-community extended
 exit-address-family

address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit-address-family

address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit-address-family

no ip http server
no ip http secure-server

control-plane
```

```

line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login

end

```

### Sample Command Output: show mpls ldp bindings

```

Spoke2# show mpls ldp bindings

tib entry: 10.9.9.1/32, rev 8
 local binding: tag: 16
 remote binding: tsr: 10.9.9.1:0, tag: imp-null
tib entry: 10.9.9.11/32, rev 4
 local binding: tag: imp-null
 remote binding: tsr: 10.9.9.1:0, tag: 16
tib entry: 10.9.9.12/32, rev 10
 local binding: tag: 17
 remote binding: tsr: 10.9.9.1:0, tag: 17
tib entry: 10.0.0.0/24, rev 6
 local binding: tag: imp-null
 remote binding: tsr: 10.9.9.1:0, tag: imp-null
tib entry: 172.0.0.0/24, rev 3
 local binding: tag: imp-null
 remote binding: tsr: 10.9.9.1:0, tag: imp-null
Spoke2#

```

### Sample Command Output: show mpls forwarding-table

```

Spoke2# show mpls forwarding-table

Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
16 Pop tag 10.9.9.1/32 0 Tu1 10.0.0.1
17 17 10.9.9.12/32 0 Tu1 10.0.0.1
18 Aggregate 192.168.11.0/24[V] \
 0
19 Aggregate 192.168.11.0/24[V] \
 0
Spoke2#

```

### Sample Command Output: show ip route vrf red

```

Spoke2# show ip route vrf red

Routing Table: red
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B 192.168.12.0/24 [200/0] via 10.9.9.12, 00:00:02
C 192.168.11.0/24 is directly connected, Ethernet1/0
Spoke2#

```

**Sample Command Output: show ip route vrf blue**

Spoke2# **show ip route vrf blue**

Routing Table: blue

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B 192.168.12.0/24 [200/0] via 10.9.9.12, 00:00:08

C 192.168.11.0/24 is directly connected, Ethernet2/0

Spoke2#

Spoke2# **show ip cef vrf red 192.168.12.0**

192.168.12.0/24, version 5, epoch 0

0 packets, 0 bytes

tag information set

local tag: VPN-route-head

fast tag rewrite with Tu1, 10.0.0.1, tags imposed: {17 18}

via 10.9.9.12, 0 dependencies, recursive

next hop 10.0.0.1, Tunnel1 via 10.9.9.12/32

valid adjacency

tag rewrite with Tu1, 10.0.0.1, tags imposed: {17 18}

Spoke2#

**Sample Command Output: show ip bgp neighbors**

Spoke2# **show ip bgp neighbors**

BGP neighbor is 10.9.9.1, remote AS 1, internal link

BGP version 4, remote router ID 10.9.9.1

BGP state = Established, up for 00:02:09

Last read 00:00:08, last write 00:00:08, hold time is 180, keepalive interval is 60 seconds

Neighbor capabilities:

Route refresh: advertised and received(old & new)

Address family IPv4 Unicast: advertised and received

Address family VPNv4 Unicast: advertised and received

Message statistics:

InQ depth is 0

OutQ depth is 0

|                | Sent | Rcvd |
|----------------|------|------|
| Opens:         | 1    | 1    |
| Notifications: | 0    | 0    |
| Updates:       | 4    | 4    |
| Keepalives:    | 4    | 4    |
| Route Refresh: | 0    | 0    |
| Total:         | 9    | 9    |

Default minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast

BGP table version 1, neighbor version 1/0

Output queue size : 0

Index 1, Offset 0, Mask 0x2

1 update-group member

|                    | Sent | Rcvd |
|--------------------|------|------|
| Prefix activity:   | ---- | ---- |
| Prefixes Current:  | 0    | 0    |
| Prefixes Total:    | 0    | 0    |
| Implicit Withdraw: | 0    | 0    |
| Explicit Withdraw: | 0    | 0    |
| Used as bestpath:  | n/a  | 0    |
| Used as multipath: | n/a  | 0    |

|                               | Outbound | Inbound |
|-------------------------------|----------|---------|
| Local Policy Denied Prefixes: | -----    | -----   |
| Total:                        | 0        | 0       |

Number of NLRIs in the update sent: max 0, min 0

For address family: VPNv4 Unicast  
 BGP table version 9, neighbor version 9/0  
 Output queue size : 0  
 Index 1, Offset 0, Mask 0x2  
 1 update-group member

|                    | Sent | Rcvd                   |
|--------------------|------|------------------------|
| Prefix activity:   | ---- | ----                   |
| Prefixes Current:  | 2    | 2 (Consumes 136 bytes) |
| Prefixes Total:    | 4    | 2                      |
| Implicit Withdraw: | 2    | 0                      |
| Explicit Withdraw: | 0    | 0                      |
| Used as bestpath:  | n/a  | 2                      |
| Used as multipath: | n/a  | 0                      |

|                               | Outbound | Inbound |
|-------------------------------|----------|---------|
| Local Policy Denied Prefixes: | -----    | -----   |
| ORIGINATOR loop:              | n/a      | 2       |
| Bestpath from this peer:      | 4        | n/a     |
| Total:                        | 4        | 2       |

Number of NLRIs in the update sent: max 1, min 1

Connections established 1; dropped 0  
 Last reset never  
 Connection state is ESTAB, I/O status: 1, unread input bytes: 0  
 Connection is ECN Disabled  
 Local host: 10.9.9.11, Local port: 179  
 Foreign host: 10.9.9.1, Foreign port: 12365

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x2D0F0):

| Timer     | Starts | Wakeups | Next |
|-----------|--------|---------|------|
| Retrans   | 6      | 0       | 0x0  |
| TimeWait  | 0      | 0       | 0x0  |
| AckHold   | 7      | 3       | 0x0  |
| SendWnd   | 0      | 0       | 0x0  |
| KeepAlive | 0      | 0       | 0x0  |
| GiveUp    | 0      | 0       | 0x0  |
| PmtuAger  | 0      | 0       | 0x0  |
| DeadWait  | 0      | 0       | 0x0  |

iss: 3328307266 snduna: 3328307756 sndnxt: 3328307756 sndwnd: 15895  
 irs: 4023050141 rcvnxt: 4023050687 rcvwnd: 16384 delrcvwnd: 0

SRTT: 165 ms, RTT0: 1457 ms, RTV: 1292 ms, KRTT: 0 ms  
 minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms  
 Flags: passive open, nagle, gen tcbs  
 IP Precedence value : 6



```
Datagrams (max data segment is 536 bytes):
Rcvd: 13 (out of order: 0), with data: 7, total data bytes: 545
Sent: 11 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with
data: 6, total data bytes: 489
Spoke2#
```

# Additional References

The following sections provide references related to Dynamic Multipoint VPN (DMVPN):

## Related Documents

| Related Topic                                          | Document Title                                                                                                                                             |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Call Admission Control                                 | <a href="#">Call Admission Control for IKE</a>                                                                                                             |
| GRE tunnel keepalive information                       | <a href="#">Generic Routing Encapsulation (GRE) Tunnel Keepalive</a> , Cisco IOS Release 12.2(8)T                                                          |
| IKE configuration tasks such as defining an IKE policy | The chapter “ <a href="#">Configuring Internet Key Exchange for IPSec VPNs</a> ” in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i> |
| IPsec configuration tasks                              | The chapter “ <a href="#">Configuring Security for VPNs with IPsec</a> ” in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>         |
| Configuring VRF-Aware IPsec                            | The chapter “ <a href="#">VRF-Aware IPsec</a> ” in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>                                  |
| Configuring MPLS                                       | The chapter “ <a href="#">Configuring Multiprotocol Label Switching</a> ” in the <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i>        |
| Configuring BGP                                        | The chapter “ <a href="#">Cisco BGP Overview</a> ” in the <i>Cisco IOS IP Routing Protocols Configuration Guide</i>                                        |
| System messages                                        | System Message Guide                                                                                                                                       |
| Defining and configuring ISAKMP profiles               | “ <a href="#">Certificate to ISAKMP Profile Mapping</a> ” chapter in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>                |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs     | Title         |
|----------|---------------|
| RFC 2547 | BGP/MPLS VPNs |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

The following commands are introduced or modified in the feature or features

- **clear dmvpn session**
- **clear dmvpn statistics**
- **debug dmvpn**
- **debug nhrp condition**
- **debug nhrp error**
- **logging dmvpn**
- **show dmvpn**
- **show ip nhrp traffic**

# Feature Information for Dynamic Multipoint VPN (DMVPN)

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Dynamic Multipoint VPN (DMVPN)

| Feature Name                                     | Releases                             | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DMVPN—Enabling Traffic Segmentation Within DMVPN | 12.4(11)T                            | The 2547oDMVPN feature allows users to segment VPN traffic within a DMVPN tunnel by applying MPLS labels to VRF instances to indicate the source and destination of each VRF.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Mangeability Enhancements for DMVPN              | 12.4(9)T                             | DMVPN session manageabilty was expanded with DMVPN specific commands for debugging, show output, session and counter control, and system log information.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li><a href="#">Troubleshooting Dynamic Multipoint VPN (DMVPN)</a></li> </ul> The following commands were introduced or modified by this feature: <b>clear dmvpn session</b> , <b>clear dmvpn statistics</b> , <b>debug dmvpn</b> , <b>debug nhrp condition</b> , <b>debug nhrp error</b> , <b>logging dmvpn</b> , <b>show dmvpn</b> , <b>show ip nhrp traffic</b> |
| DMVPN Phase 2                                    | 12.2(18)SXE<br>12.3(9)a<br>12.3(8)T1 | DMVPN Spoke-to-Spoke functionality was made more production ready. If you are using this functionality in a production network, the minimum release is Release 12.3(9a) or Release 12.3(8)T1.<br><br>In Release 12.2(18)SXE, support was added for the Cisco Catalyst 6500 series switch and the Cisco 7600 series router.                                                                                                                                                                                                                                                                                                            |

**Table 1**      **Feature Information for Dynamic Multipoint VPN (DMVPN)**

| Feature Name                           | Releases                 | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| —                                      | 12.3(6)<br>12.3(7)T      | Virtual Route Forwarding Integrated DMVPN and Network Address Translation-Transparency (NAT-T) Aware DMVPN enhancements were added. In addition, DMVPN Hub-to-Spoke functionality was made more production ready. If you are using this functionality in a production network, the minimum release requirement is Cisco IOS Release 12.3(6) or 12.3(7)T.<br><br>The enhancements added in Cisco IOS Release 12.3(6) were integrated into Cisco IOS Release 12.3(7)T. |
| Dynamic Multipoint VPN (DMVPN) Phase 1 | 12.2(13)T                | The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IPsec Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IP security (IPsec) encryption, and Next Hop Resolution Protocol (NHRP).                                                                                                                                                                                                     |
| DMVPN - Phase 2                        | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                        |
| Dynamic Multipoint VPN (DMVPN) Phase 1 | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                        |

## Glossary

**AM**—aggressive mode. A mode during IKE negotiation. Compared to MM, AM eliminates several steps, making it faster but less secure than MM. Cisco IOS software will respond in aggressive mode to an IKE peer that initiates aggressive mode.

**GRE**—generic routing encapsulation. Tunnels that provide a specific pathway across the shared WAN and encapsulate traffic with new packet headers to ensure delivery to specific destinations. The network is private because traffic can enter a tunnel only at an endpoint. Tunnels do not provide true confidentiality (encryption does) but can carry encrypted traffic.

GRE tunneling can also be used to encapsulate non-IP traffic into IP and send it over the Internet or IP network. The Internet Package Exchange (IPX) and AppleTalk protocols are examples of non-IP traffic.

**IKE**—Internet Key Exchange. A hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. Although IKE can be used with other protocols, its initial implementation is with IPsec. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations.

**IPsec**—IP security. A framework of open standards developed by the Internet Engineering Task Force (IETF). IPsec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (“peers”), such as Cisco routers.

**ISAKMP**—Internet Security Association Key Management Protocol. A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.

**MM**—main mode. Mode that is slower than aggressive mode but more secure and more flexible than aggressive mode because it can offer an IKE peer more security proposals. The default action for IKE authentication (rsa-sig, rsa-encr, or preshared) is to initiate main mode.

**NHRP**—Next Hop Resolution Protocol. Routers, access servers, and hosts can use NHRP to discover the addresses of other routers and hosts connected to a NBMA network.

The Cisco implementation of NHRP supports the IETF draft version 11 of *NBMA Next Hop Resolution Protocol (NHRP)*.

The Cisco implementation of NHRP supports IP Version 4, Internet Packet Exchange (IPX) network layers, and, at the link layer, ATM, Ethernet, SMDS, and multipoint tunnel networks. Although NHRP is available on Ethernet, NHRP need not be implemented over Ethernet media because Ethernet is capable of broadcasting. Ethernet support is unnecessary (and not provided) for IPX.

**PFS**—Perfect Forward Secrecy. A cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.

**SA**—security association. Describes how two or more entities will utilize security services to communicate securely. For example, an IPsec SA defines the encryption algorithm (if used), the authentication algorithm, and the shared session key to be used during the IPsec connection.

Both IPsec and IKE require and use SAs to identify the parameters of their connections. IKE can negotiate and establish its own SA. The IPsec SA is established either by IKE or by manual user configuration.

**transform**—The list of operations done on a dataflow to provide data authentication, data confidentiality, and data compression. For example, one transform is the ESP protocol with the HMAC-MD5 authentication algorithm; another transform is the AH protocol with the 56-bit DES encryption algorithm and the ESP protocol with the HMAC-SHA authentication algorithm.

**VPN**—Virtual Private Network. A framework that consists of multiple peers transmitting private data securely to one another over an otherwise public infrastructure. In this framework, inbound and outbound network traffic is protected using protocols that tunnel and encrypt all data. This framework permits networks to extend beyond their local topology, while remote users are provided with the appearance and functionality of a direct network connection.

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.







Easy VPN





# Cisco Easy VPN Remote

---

**First Published: November 25, 2002**

**Last Updated: November 4, 2008**

This document provides information on configuring and monitoring the Cisco Easy VPN Remote feature to create IPsec Virtual Private Network (VPN) tunnels between a supported router and an Easy VPN server (Cisco IOS router, VPN 3000 concentrator, or Cisco PIX Firewall) that supports this form of IPsec encryption and decryption.

For the benefits of this feature, see the section “[Benefits of the Cisco Easy VPN Remote Feature.](#)”

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Easy VPN Remote](#)” section on page 107.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Cisco Easy VPN Remote, page 2](#)
- [Restrictions for Cisco Easy VPN Remote, page 2](#)
- [Information About Cisco Easy VPN Remote, page 4](#)
- [How to Configure Cisco Easy VPN Remote, page 35](#)
- [Configuration Examples for Cisco Easy VPN Remote, page 67](#)
- [Additional References, page 102](#)
- [Command Reference, page 106](#)
- [Feature Information for Easy VPN Remote, page 107](#)
- [Glossary, page 111](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2008 Cisco Systems, Inc. All rights reserved.

# Prerequisites for Cisco Easy VPN Remote

## Cisco Easy VPN Remote Feature

- A Cisco 800 series router running Cisco IOS Release 12.2(15)T, 12.3(2)T, 12.3(4)T, 12.3(7)T, or 12.3(7)XR2 configured as a Cisco Easy VPN remote.
- A Cisco 1700 series router running Cisco IOS Release 12.2(15)T, 12.3(2)T, 12.3(4)T, 12.3(7)T, or 12.3(7)XR, configured as a Cisco Easy VPN remote.
- A Cisco 1800 series fixed configuration router running Cisco IOS Release 12.3(8)YI.
- A Cisco uBR905 or Cisco uBR925 cable access router running Cisco IOS Release 12.2(15)T, configured as a Cisco Easy VPN remote.
- Another Cisco router or VPN concentrator that supports the Cisco Easy VPN Server feature and that is configured as a Cisco IOS Easy VPN server. See the “[Required Easy VPN Servers](#)” section for a detailed list.

## Reactivate Primary Peer Feature

- An existing Easy VPN remote configuration can be enhanced to accommodate the Reactivate Primary Peer feature using the **peer** command (and **default** keyword) and the **idle-time** command. After the tunnel between the Easy VPN remote and a nondefault peer is working, the Reactivate Primary Peer features takes effect, that is, the Easy VPN remote periodically tries to check the connectivity with the primary peer. Any time the Easy VPN remote detects that the link is working, the Easy VPN remote tears down the existing connection and brings up the tunnel with the primary peer.

# Restrictions for Cisco Easy VPN Remote

## Required Easy VPN Servers

The Cisco Easy VPN Remote feature requires that the destination peer be a Cisco IOS Easy VPN server or VPN concentrator that supports the Cisco Easy VPN Server feature. At the time of publication, servers or concentrators that support this feature include the following platforms when running the indicated software releases:

- Cisco 806, Cisco 826, Cisco 827, Cisco 828, Cisco 831, Cisco 836, and Cisco 837 routers—Cisco IOS Release 12.2(8)T or later release. Cisco 800 series routers are not supported in Cisco IOS Release 12.3(7)XR, but they are supported in Cisco IOS Release 12.3(7)XR2.
- Cisco 870 series—Cisco IOS Release 12.3(8)YI1.
- Cisco 1700 series—Cisco IOS Release 12.2(8)T or later release.
- Cisco 1800 series fixed configuration router—Cisco IOS Release 12.3(8)YI.
- Cisco 1812 router—Cisco IOS Release 12.3(8)YH.
- Cisco 2600 series—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3620—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3640—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3660—Cisco IOS Release 12.2(8)T or later release.
- Cisco 7100 series VPN routers—Cisco IOS Release 12.2(8)T or later release.
- Cisco 7200 series routers—Cisco IOS Release 12.2(8)T or later release.

- Cisco 7500 series routers—Cisco IOS Release 12.2(8)T or later release.
- Cisco PIX 500 series—Software Release 6.2 or later release.
- Cisco VPN 3000 series—Software Release 3.11 or later release.

### Only ISAKMP Policy Group 2 Supported on Easy VPN Servers

The Unity Protocol supports only Internet Security Association Key Management Protocol (ISAKMP) policies that use group 2 (1024-bit Diffie-Hellman) Internet Key Exchange (IKE) negotiation, so the Easy VPN server being used with the Cisco Easy VPN Remote feature must be configured for a group 2 ISAKMP policy. The Easy VPN server cannot be configured for ISAKMP group 1 or group 5 when being used with a Cisco Easy VPN client.

### Transform Sets Supported

To ensure a secure tunnel connection, the Cisco Easy VPN Remote feature does not support transform sets that provide encryption without authentication (ESP-DES and ESP-3DES) or transform sets that provide authentication without encryption (ESP-NUL ESP-SHA-HMAC and ESP-NUL ESP-MD5-HMAC).



#### Note

The Cisco Unity Client Protocol does not support Authentication Header (AH) authentication, but Encapsulation Security Protocol (ESP) is supported.

### Dial Backup for Easy VPN Remotes

Line-status-based backup is not supported in this feature.

### Network Address Translation Interoperability Support

Network Address Translation (NAT) interoperability is not supported in client mode with split tunneling.

### Multicast and Static NAT

Multicast and static NAT are supported only for Easy VPN remotes using dynamic virtual tunnel interfaces (DVTIs).

### Virtual IPsec Interface Restrictions

- For the Virtual IPsec Interface Support feature to work, virtual templates support is needed.
- If you are using a virtual tunnel interface on the Easy VPN remote device, it is recommended that you configure the server for a virtual tunnel interface.

### Dual Tunnel Support

The following restrictions apply if you are using dual tunnels that share common inside and outside interfaces:

- If dual tunnels are configured, one of the tunnels should have a split tunnel configured on the server.
- Web Intercept can be configured for only one of the tunnels. Web Intercept should not be used for the voice tunnel.
- Web Intercept cannot be used for IP phones until authorization proxy becomes aware of how to bypass the IP phone.
- Some features, such as Pushing a Configuration URL Through a Mode-Configuration Exchange, can be used only through a single tunnel.

**cTCP Support on Easy VPN Clients**

- cTCP listens on only up to 10 ports.
- If there are other applications registered for the port on which cTCP is enabled, those applications will not work.

## Information About Cisco Easy VPN Remote

To configure the Cisco Easy VPN Remote features, you should understand the following concepts:

- [Benefits of the Cisco Easy VPN Remote Feature, page 4](#)
- [Cisco Easy VPN Remote Overview, page 4](#)
- [Modes of Operation, page 5](#)
- [Authentication, page 8](#)
- [Tunnel Activation Options, page 17](#)
- [Dead Peer Detection Stateless Failover Support, page 18](#)
- [Cisco Easy VPN Remote Features, page 19](#)

## Benefits of the Cisco Easy VPN Remote Feature

- Allows dynamic configuration of end-user policy, requiring less manual configuration by end users and field technicians, thus reducing errors and further service calls.
- Allows the provider to change equipment and network configurations as needed, with little or no reconfiguration of the end-user equipment.
- Provides for centralized security policy management.
- Enables large-scale deployments with rapid user provisioning.
- Eliminates the need for end users to purchase and configure external VPN devices.
- Eliminates the need for end users to install and configure Easy VPN Client software on their PCs.
- Offloads the creation and maintenance of the VPN connections from the PC to the router.
- Reduces interoperability problems between the different PC-based software VPN clients, external hardware-based VPN solutions, and other VPN applications.
- Sets up a single IPsec tunnel regardless of the number of multiple subnets that are supported and the size of the split-include list.

## Cisco Easy VPN Remote Overview

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client Protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN server. This server can be a dedicated VPN device, such as a Cisco VPN 3000 concentrator or a Cisco PIX Firewall or a Cisco IOS router that supports the Cisco Unity Client Protocol.

After the Cisco Easy VPN server has been configured, a VPN connection can be created with minimal configuration on an Easy VPN remote, such as a Cisco 800 series router or a Cisco 1700 series router. When the Easy VPN remote initiates the VPN tunnel connection, the Cisco Easy VPN server pushes the IPsec policies to the Easy VPN remote and creates the corresponding VPN tunnel connection.

The Cisco Easy VPN Remote feature provides for automatic management of the following details:

- Negotiating tunnel parameters, such as addresses, algorithms, and lifetime.
- Establishing tunnels according to the parameters that were set.
- Automatically creating the NAT or Port Address Translation (PAT) and associated access lists that are needed, if any.
- Authenticating users, that is, ensuring that users are who they say they are by way of usernames, group names, and passwords.
- Managing security keys for encryption and decryption.
- Authenticating, encrypting, and decrypting data through the tunnel.

## Modes of Operation

The Cisco Easy VPN Remote feature supports three modes of operation: client, network extension, and network extension plus:

- **Client**—Specifies that NAT or PAT be done so that the PCs and other hosts at the remote end of the VPN tunnel form a private network that does not use any IP addresses in the IP address space of the destination server.

An enhancement has been made so that the IP address that is received via mode configuration is automatically assigned to an available loopback interface. The IPsec Security Associations (SAs) for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell).

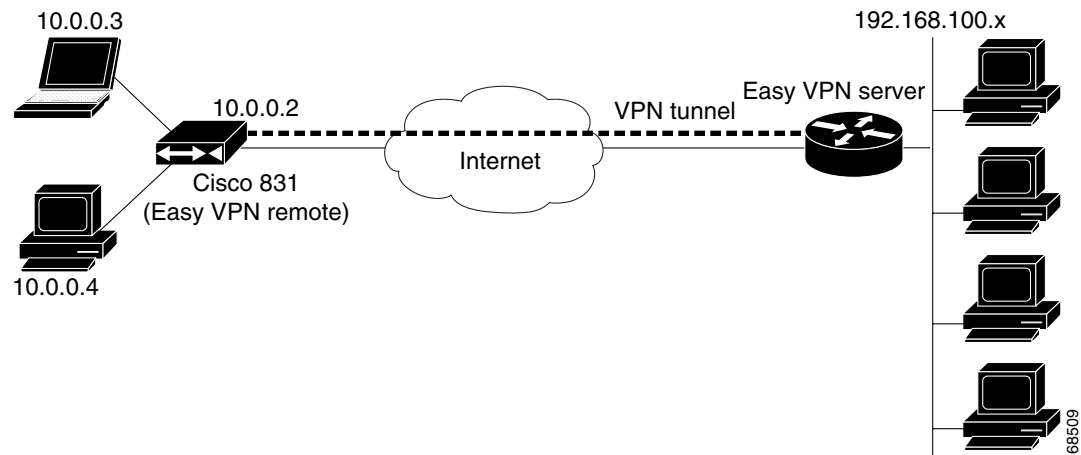
- **Network extension**—Specifies that the PCs and other hosts at the client end of the VPN tunnel should be given IP addresses that are fully routable and reachable by the destination network over the tunneled network so that they form one logical network. PAT is not used, which allows the client PCs and hosts to have direct access to the PCs and hosts at the destination network.
- **Network extension plus (mode network-plus)**—Identical to network extension mode with the additional capability of being able to request an IP address via mode configuration and automatically assign it to an available loopback interface. The IPsec SAs for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell).

All modes of operation also optionally support split tunneling, which allows secure access to corporate resources through the VPN tunnel while also allowing Internet access through a connection to an Internet service provider (ISP) or other service—thereby eliminating the corporate network from the path for web access.

## Client Mode and Network Extension Mode Scenarios

Figure 1 illustrates the client mode of operation. In this example, the Cisco 831 router provides access to two PCs, which have IP addresses in the 10.0.0.0 private network space. These PCs connect to the Ethernet interface on the Cisco 831 router, which also has an IP address in the 10.0.0.0 private network space. The Cisco 831 router performs NAT or PAT translation over the VPN tunnel so that the PCs can access the destination network.

**Figure 1** Cisco Easy VPN Remote Connection



### Note

The diagram in Figure 1 could also represent a split tunneling connection, in which the client PCs can access public resources in the global Internet without including the corporate network in the path for the public resources.

Figure 2 also illustrates the client mode of operation, in which a VPN concentrator provides destination endpoints to multiple xDSL clients. In this example, Cisco 800 series routers provide access to multiple small business clients, each of which uses IP addresses in the 10.0.0.0 private network space. The Cisco 800 series routers perform NAT or PAT translation over the VPN tunnel so that the PCs can access the destination network.



**Figure 2** Cisco Easy VPN Remote Connection (using a VPN concentrator)

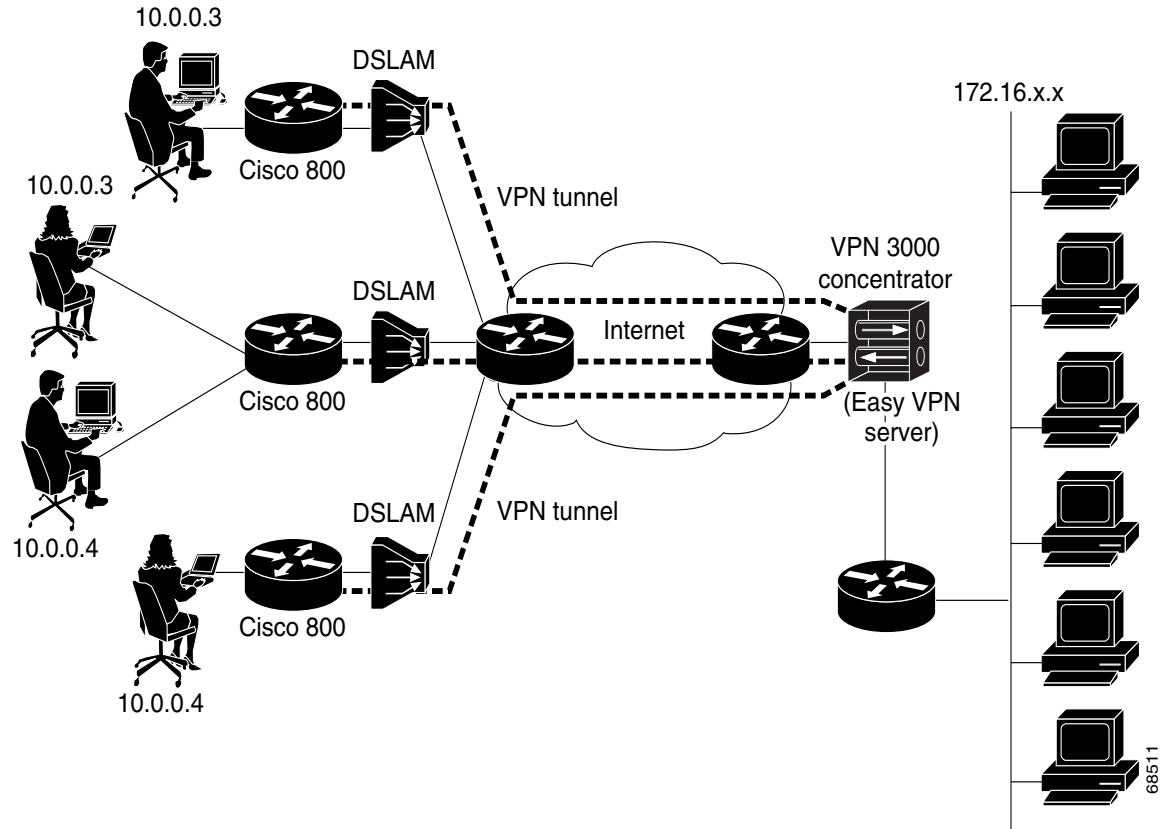
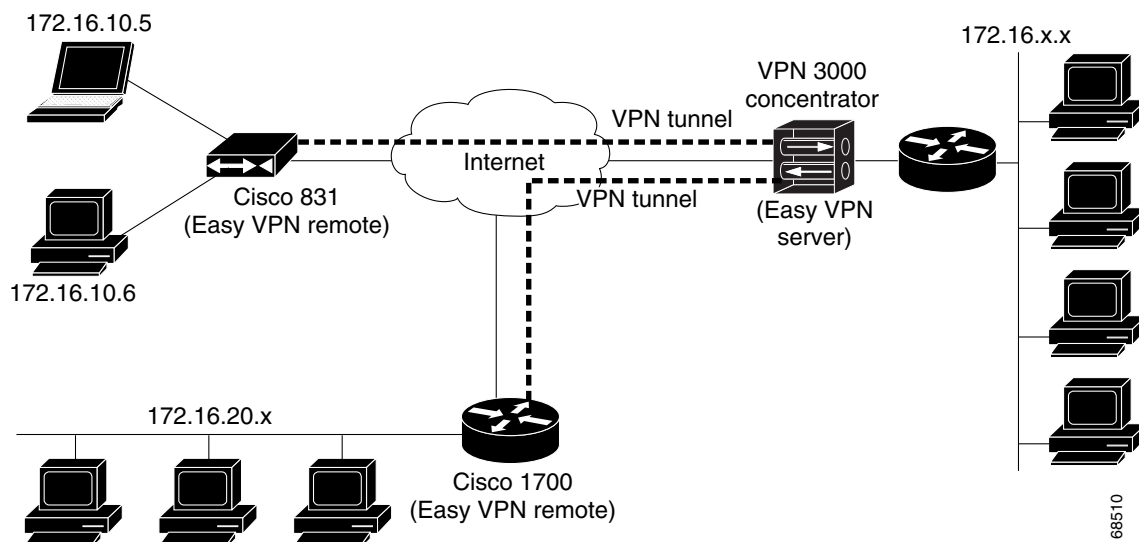


Figure 3 illustrates the network extension mode of operation. In this example, the Cisco 831 router and Cisco 1700 series router both act as Cisco Easy VPN remote devices, connecting to a Cisco VPN 3000 concentrator.

The client hosts are given IP addresses that are fully routable by the destination network over the tunnel. These IP addresses could be either in the same subnet space as the destination network or in separate subnets, assuming that the destination routers are configured to properly route those IP addresses over the tunnel.

In this example, the PCs and hosts attached to the two routers have IP addresses that are in the same address space as the destination enterprise network. The PCs connect to the Ethernet interface of the Cisco 831 router, which also has an IP address in the enterprise address space. This scenario provides a seamless extension of the remote network.

**Figure 3** Cisco Easy VPN Network Extension Connection



## Authentication

The Cisco Easy VPN Remote feature supports a two-stage process for authenticating the remote router to the central concentrator. The first step is Group Level Authentication and is part of the control channel creation. In this first stage, two types of authentication credentials can be used: either preshared keys or digital certificates. The following paragraphs provide details about these options.

The second authentication step is called Extended Authentication or Xauth. In this step, the remote side (in this case the Easy VPN router) submits a username and password to the central site router. This step is the same process as that which occurs when a user of the Cisco VPN software client on a PC enters his or her username and password to activate his or her VPN tunnel. When using the router, the difference is that the router itself is being authenticated to the network, not a PC with Cisco VPN Client software. Xauth is an optional step (it can be disabled) but is normally enabled to improve security. After Xauth is successful and the tunnel comes up, all PCs behind the Easy VPN remote router have access to the tunnel.

If Xauth is enabled, it is key to decide how to input the username and password. There are two options. The first option is to store the Xauth username and password in the configuration file of the router. This option is typically used if the router is shared between several PCs and the goal is to keep the VPN tunnel up all the time (see the section "[Automatic Activation](#)") or to have the router automatically bring up the tunnel whenever there is data to be sent (see the section "[Traffic-Triggered Activation](#)"). An example of this application is a branch office situation, in which the users in the branch office want the VPN tunnel to be available whenever they have data to send and do not want to have to do anything special to activate the VPN tunnel. If the PCs in the branch office must be individually authenticated on the basis of the ID of each user, the correct configuration is to put the Easy VPN router in Automatic Activation mode to keep the tunnel "up" all the time and to use Cisco IOS Authentication Proxy or 802.1x to authenticate the individual PCs. Because the tunnel is always up, Authentication Proxy or 802.1x can access a central site user database such as AAA/RADIUS to authenticate the individual user requests as they are submitted by PC users. (See the "[Related Documents](#)" sections "General information on IPsec and VPN" for a reference to configuring Authentication Proxy and "802.1x authentication" for a reference to configuring 802.1x authentication.)

The second option for entry of the Xauth username and password is not to store it on the router. Instead, a PC user who is connected to the router is presented with a special web page that allows the user to manually enter the username and password (see the section “[Manual Activation](#)”). The router sends the username and password to the central site concentrator, and if the username and password are correct, the tunnel comes up. The typical application for this configuration is a teleworker network. The teleworker wants to control when the tunnel is up and has to enter his or her personal user credentials (which could include one-time passwords) to activate the tunnel. Also, the network administrator may want teleworker tunnels up only when someone is using them to conserve resources on the central concentrators. (See the section “[Web-Based Activation](#)” for details about this configuration.)

The Xauth username and password can also be manually entered from the command-line interface (CLI) of the router. This method is not recommended for most situations because the user must first log in to the router (and needs a user ID on the router to do so). However, it can be useful for network administrators during troubleshooting.

## Using Preshared Keys

Using preshared keys, each peer is aware of the key of the other peer. Preshared keys are displayed in running configurations, so they can be seen by anyone (referred to as clear format). When a more secure type of authentication is required, Cisco software also supports another type of preshared key: the encrypted preshared key.

Using an encrypted preshared key for authentication allows you to securely store plain-text passwords in type 6 (encrypted) format in NVRAM. A group preshared key can be preconfigured on both VPN-tunnel peers. The encrypted form of the keyword can be seen in the running configuration, but the actual keyword is not visible. (For more information about encrypted preshared keys, see [Encrypted Preshared Key](#).)

## Using Digital Certificates

Digital certificates provide for the support of Rivest, Shamir, and Adelman (RSA) signatures on Easy VPN remote devices. The support is provided through a RSA certificate that can be stored on or off the remote device.



### Note

The recommended timeout for Easy VPN using digital certificates is 40 seconds.

For more information about digital certificates, see the [Easy VPN Remote RSA Signature Support](#) feature guide, Release 12.3(7)T1.

## Using Xauth

Xauth is an additional level of authentication that can be used. Xauth is applicable when either group preshared keys or digital certificates are used. Xauth credentials can be entered using a web interface manager, such as Security Device Manager (SDM), or using the CLI. (See the section “[Cisco Easy VPN Remote Web Managers](#).”)

The Save Password feature allows the Xauth username and password to be saved in the Easy VPN Remote configuration so that you are not required to enter the username and password manually. One-Time Passwords (OTPs) are not supported by the Save Password feature and must be entered manually when Xauth is requested. The Easy VPN server must be configured to “Allow Saved Passwords.” (For more information about how to configure the Save Password feature, see the section “[Dead Peer Detection Periodic Message Option](#).”)

Xauth is controlled by the Easy VPN server. When the Cisco IOS Easy VPN server requests Xauth authentication, the following messages are displayed on the console of the router:

```
EZVPN: Pending XAuth Request, Please enter the following command:
crypto ipsec client ezvpn xauth
```

When you see this message, you can provide the necessary user ID, password, and other information by entering the **crypto ipsec client ezvpn connect** command and responding to the prompts that follow.

The recommended Xauth timeout is 50 seconds or fewer.



#### Note

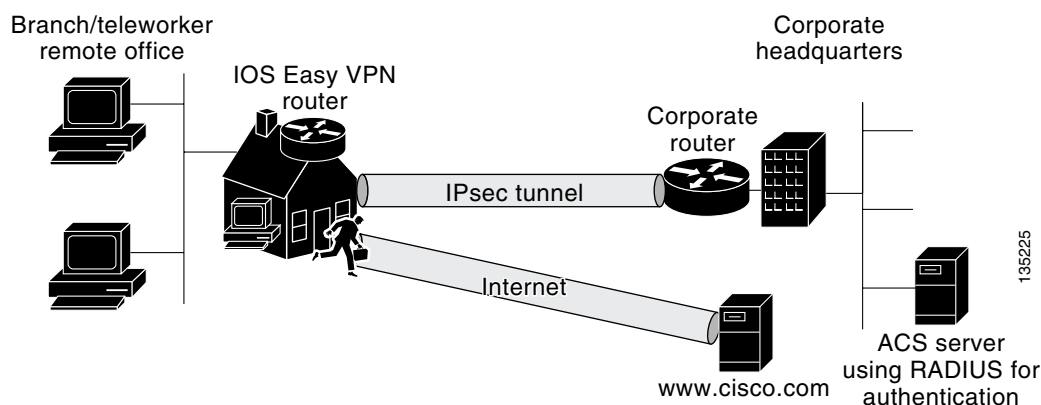
The timeout for entering the username and password is determined by the configuration of the Cisco IOS Easy VPN server. For servers running Cisco IOS software, this timeout value is specified by the **crypto isakmp xauth timeout** command.

## Web-Based Activation

Web-Based Activation provides a user-friendly method for a remote teleworker to authenticate the VPN tunnel between his or her remote Easy VPN router and the central site router. This feature allows administrators to set up their remote LANs so that the initial HTTP request that is coming from any of the remote PCs is intercepted by the remote Easy VPN router. A login page is returned to the user, whereby the user may enter credentials to authenticate the VPN tunnel. After the VPN tunnel comes up, all users behind this remote site can access the corporate LAN without being reprompted for the username and password. Alternatively, the user may choose to bypass the VPN tunnel and connect only to the Internet, in which case a password is not required.

A typical application for web-based activation is a home teleworker who brings up the Easy VPN tunnel only when he or she needs to connect to the corporate LAN. If the remote teleworker is not present, other members of the household (such as a spouse or children) can use the Internet Only option to browse the Internet without activating the VPN tunnel. [Figure 4](#) shows a typical scenario for web-based activation.

**Figure 4** Typical Web-Based Activation Scenario



#### Note

Entering the Xauth credentials brings up the tunnel for all users who are behind this remote site. After the tunnel is up, any additional PCs that are behind the remote site do not get prompted for Xauth credentials. Web-Based Activation is an authentication to bring up the VPN tunnel for all remote PCs and cannot be considered individual user authentication. Individual user authentication for VPN tunnel access is available using the Cisco IOS Authentication Proxy or 802.1x features, which can be

configured on the remote Easy VPN router. (See the “[Related Documents](#)” sections “General information on IPsec and VPN” for a reference to configuring Authentication Proxy and “802.1x authentication” for a reference to configuring 802.1x authentication.)

To configure web-based activation, see the section “[Configuring Web-Based Activation](#).”

The following sections show the various screen shots that a remote teleworker sees when the Web-Based Activation feature is turned on:

- [Web-Based Activation Portal Page, page 11](#)
- [VPN Authentication Bypass, page 12](#)
- [VPN Tunnel Authentication, page 13](#)
- [Successful Authentication, page 14](#)
- [Deactivation, page 15](#)

## Web-Based Activation Portal Page

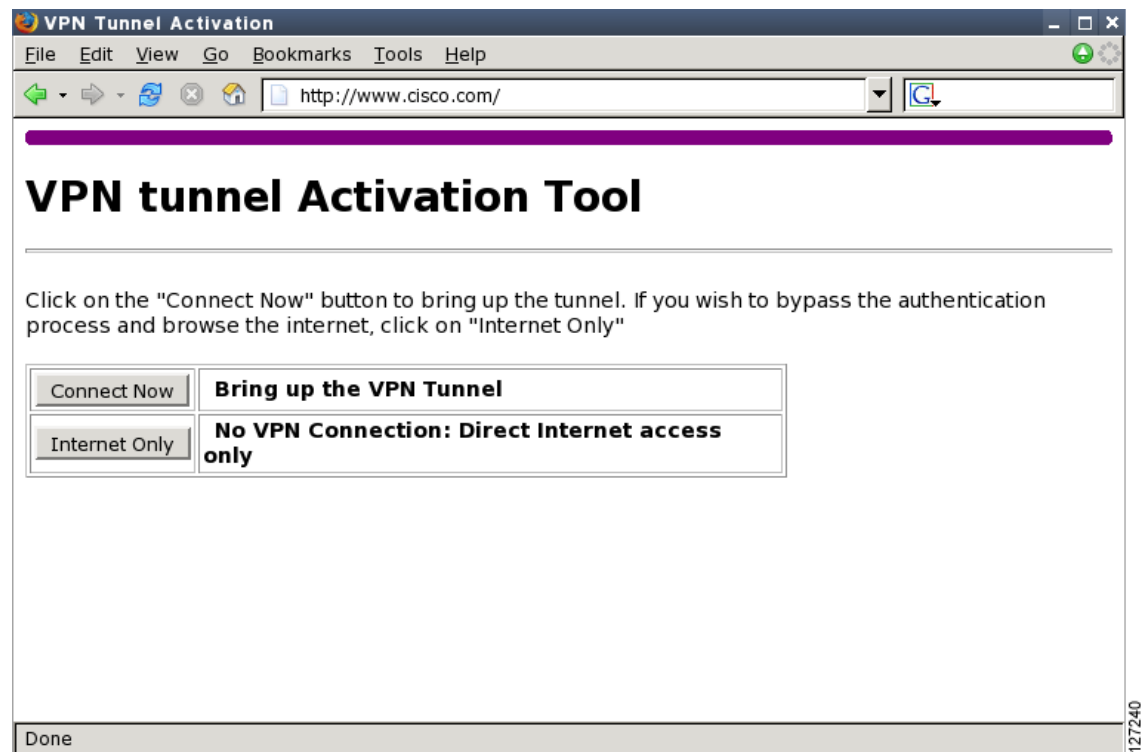
[Figure 5](#) is an example of a web-based activation portal page. The user may choose to connect to the corporate LAN by clicking Connect Now or he or she may choose to connect only to the Internet by clicking Internet Only.



**Note**

If the user chooses to connect only to the Internet, a password is not required.

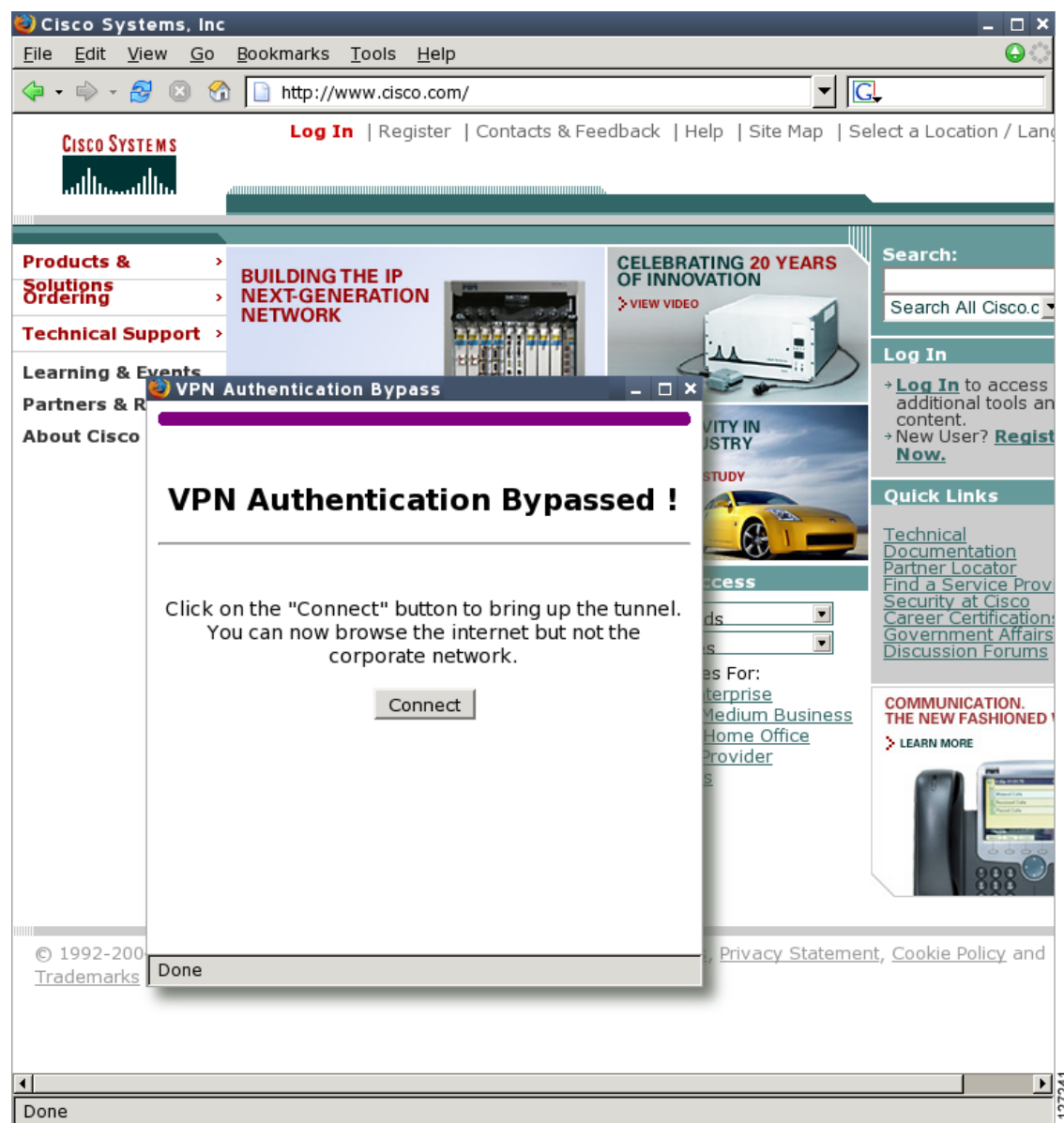
**Figure 5**      **Portal Page**



## VPN Authentication Bypass

Figure 6 is an example of a web-based activation in which the user chose to connect only to the Internet by clicking the Internet Only option. This option is most useful for household members who need to browse the Internet while the remote teleworker is not available to authenticate the VPN tunnel for corporate use.

**Figure 6** VPN Authentication Bypass Page



127241

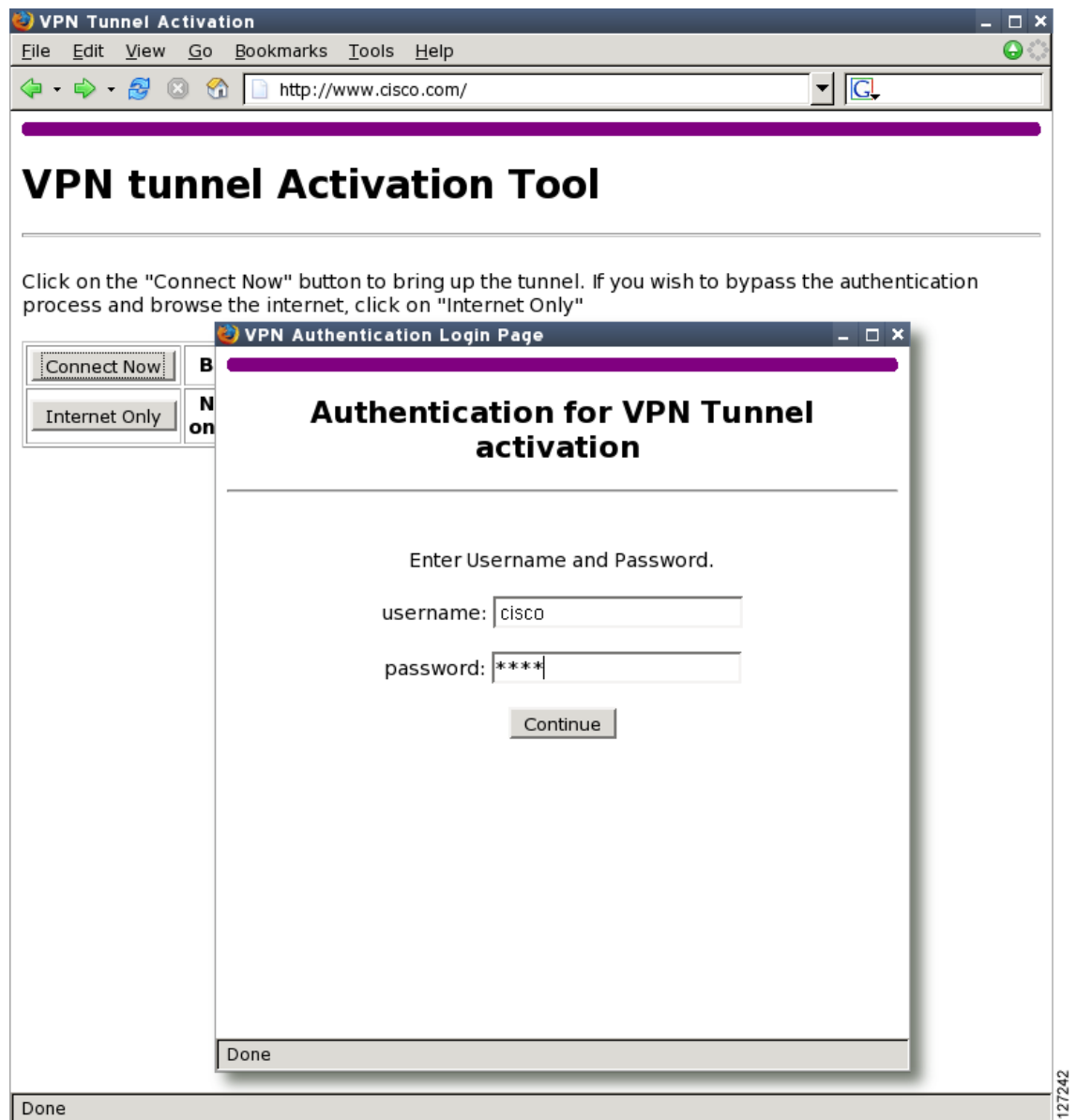
**Note**

If the Web-Based Activation window is mistakenly closed, to connect again, a user should follow this two-step process:

1. In a browser, type “http://routeripaddress/ezvpn/bypass” and try to connect to the URL. Entering this URL clears the bypass state that was created for your IP address (when the “Internet only” button was pressed). If you get a message saying that no such page is found, it does not matter because the only purpose of accessing the URL is to clear the bypass state.
2. After clearing the bypass state, you can browse to any external site. The Connect and Bypass page appears again. You can connect to VPN by pressing the Connect button.

**VPN Tunnel Authentication**

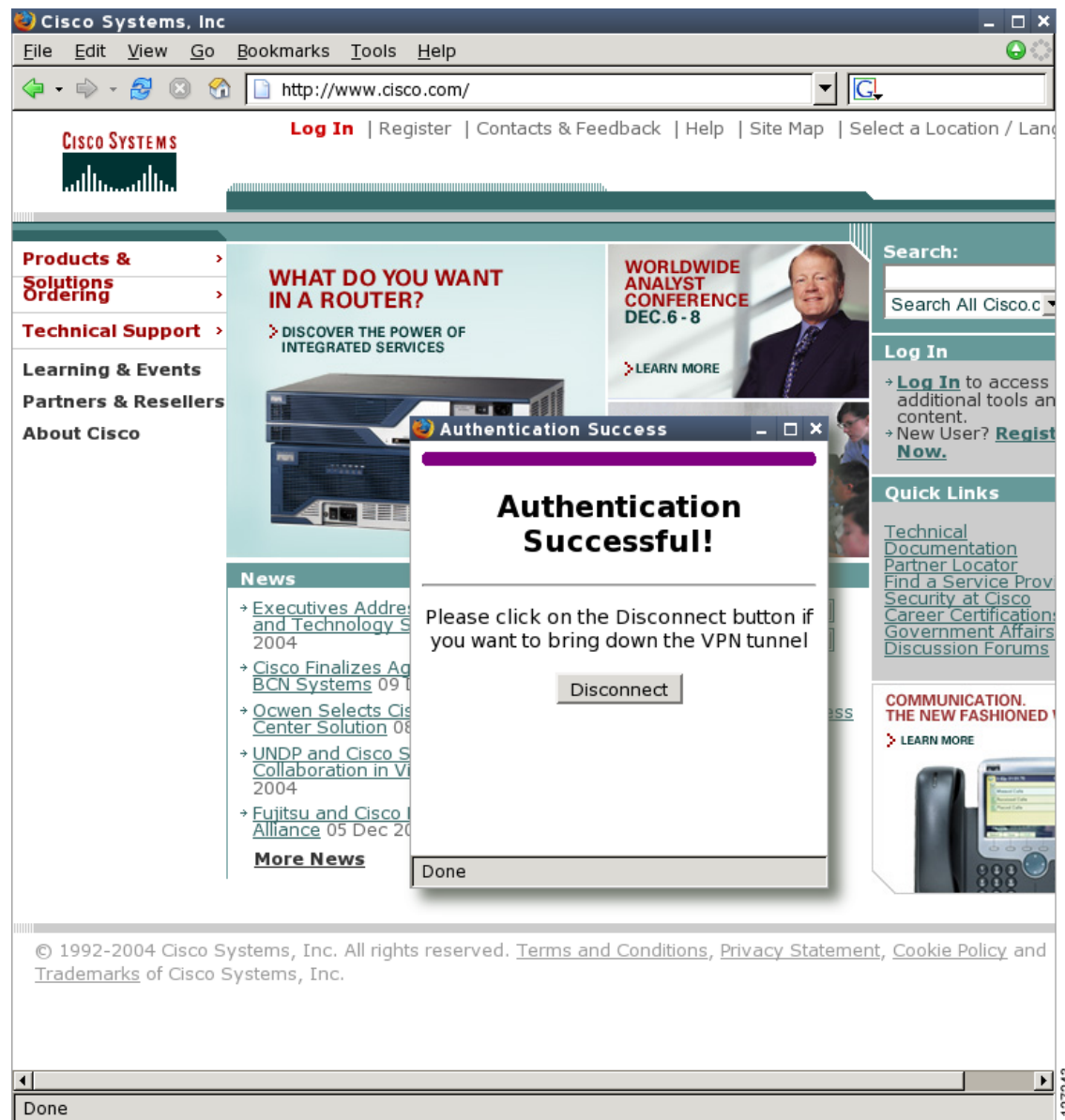
[Figure 7](#) is an example of a web-based activation in which the user chose to connect to the corporate LAN by entering a username and password. After the user is successfully authenticated, the Easy VPN tunnel is brought up for this remote site. If there are multiple PCs behind this remote site, none of the additional users who are connecting to the corporate LAN will be requested for the Xauth credentials because the tunnel is already up.

**Figure 7** VPN Tunnel Authentication

### Successful Authentication

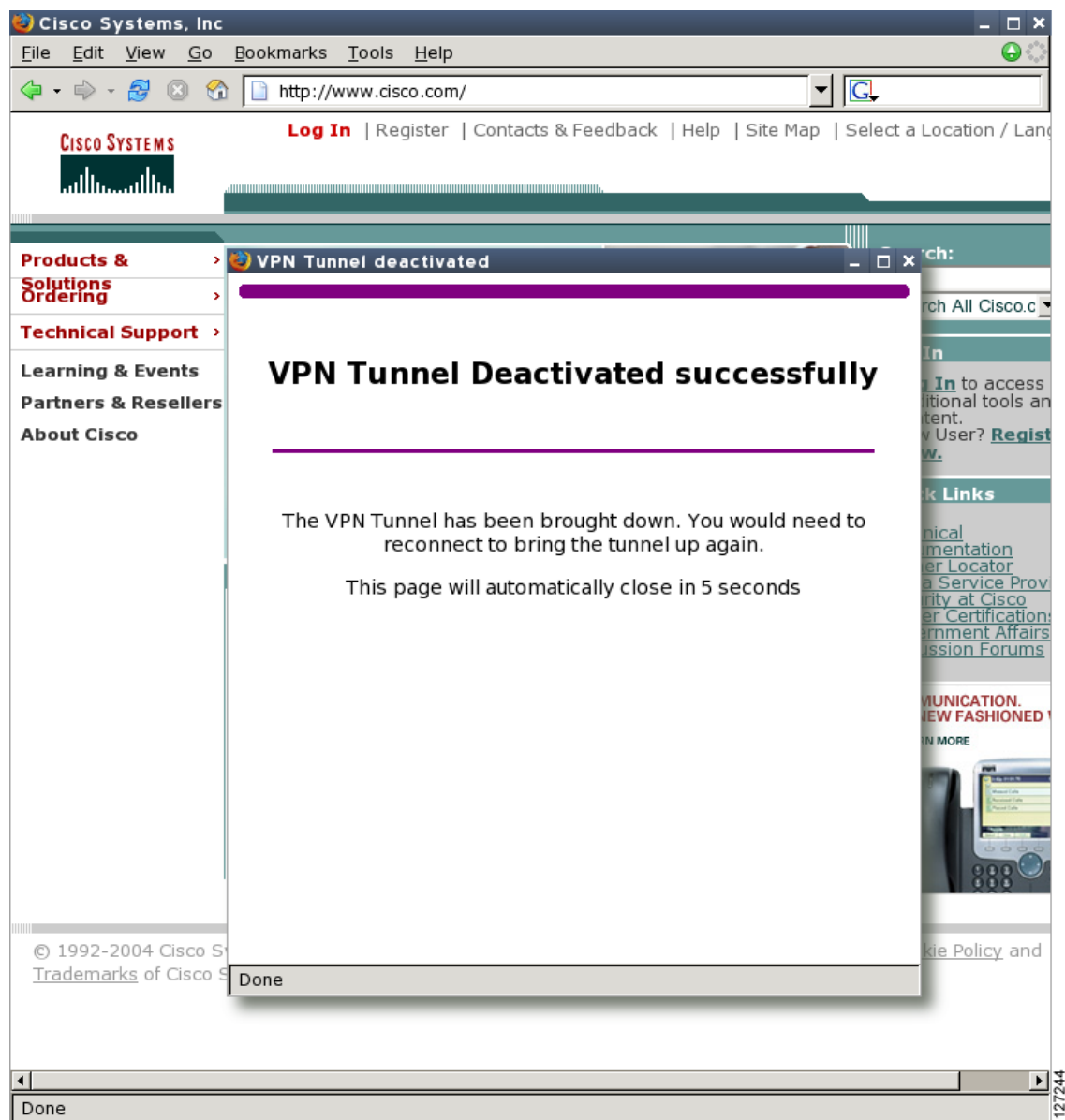
Figure 8 is an example of a successful activation. If the user chooses to deactivate the VPN tunnel, he or she should click the Disconnect button. After the IKE security association (SA) times out (the default value is 24 hours), the remote teleworker has to enter the Xauth credentials to bring up the tunnel.



**Figure 8 Successful Activation**

## Deactivation

Figure 9 is an example of a VPN tunnel that has been deactivated successfully. The page automatically closes in 5 seconds.

**Figure 9** *VPN Tunnel Deactivated Successfully*

## 802.1x Authentication

The 802.1x Authentication feature allows you to combine Easy VPN client mode operation with 802.1x authentication on Cisco IOS routers. For more information about this feature, see “802.1x Authentication” in the section “[Additional References](#).”

## Tunnel Activation Options

There are three tunnel activation options:

- Automatic activation
- Manual activation
- Traffic-triggered activation (not available in Cisco IOS Release 12.3(11)T)

Tunnel connect and disconnect options are available with SDM.

### Automatic Activation

The Cisco Easy VPN tunnel is automatically connected when the Cisco Easy VPN Remote feature is configured on an interface. If the tunnel times out or fails, the tunnel automatically reconnects and retries indefinitely.

To specify automatic tunnel control on a Cisco Easy VPN remote device, you need to configure the **crypto ipsec client ezvpn** command and then the **connect auto** subcommand. However, you do not need to use these two commands when you are creating a new Easy VPN remote configuration because the default is “automatic.”

To disconnect or reset a particular tunnel, you should use the **clear crypto ipsec client ezvpn** command, or you can use SDM.

### Manual Activation

The Cisco Easy VPN Remote software implements manual control of the Cisco Easy VPN tunnels so that you can establish and terminate the tunnel on demand.

To specify manual tunnel control on a Cisco Easy VPN remote device, you need to input the **crypto ipsec client ezvpn** command and then the **connect manual** command.

The manual setting means that the Cisco Easy VPN remote will wait for a command before attempting to establish the Cisco Easy VPN Remote connection. When the tunnel times out or fails, subsequent connections will also have to wait for the command.

If the configuration is manual, the tunnel is connected only after you issue the command **crypto ipsec client ezvpn connect**.

To disconnect or reset a particular tunnel, you should use the **clear crypto ipsec client ezvpn** command, or you can use SDM.

See the “[Configuring Manual Tunnel Control](#)” section for specific information on how to configure manual control of a tunnel.

### Traffic-Triggered Activation



#### Note

This feature is not available in Cisco IOS Release 12.3(11)T.

The Traffic-Triggered Activation feature is recommended for transactional-based VPN applications. It is also recommended for use with the Easy VPN dial backup feature for the backup Easy VPN configuration so that backup is activated only when there is traffic to send across the tunnel.

To use Access Control List (ACL) tunnel control, you must first describe the traffic that is considered “interesting.” For more information about ACLs, see the chapter “[Access Control Lists: Overview and Guidelines](#)” in the “Traffic Filtering and Firewalls” section of the *Cisco IOS Security Configuration Guide, Release 12.3*. To actually configure an ACL-triggered tunnel, use the **crypto ipsec client ezvpn** command with the **connect acl** subcommand.

## Dead Peer Detection Stateless Failover Support

Two options are available for configuring Dead Peer Detection Stateless Failover Support:

- Backup Server List Local Configuration
- Backup Server List Auto Configuration

### Backup Server List Local Configuration

Backup Server List Local Configuration allows users to enter multiple peer statements. With this feature configured, if the client is connecting to a peer and the negotiation fails, Easy VPN fails over to the next peer. This failover continues through the list of peers. When the last peer is reached, Easy VPN rolls over to the first peer. The IKE and IPsec SAs to the previous peer are deleted. Multiple peer statements work for both IP addresses as well as for hostnames. Setting or unsetting the peer statements will not affect the order of the peer statements.

To use this feature, use the **peer** subcommand of the **crypto ipsec client ezvpn** command.

### Backup Server List Auto Configuration

Easy VPN remote that is based on Cisco IOS software can have up to 10 backup servers configured for redundancy. The Backup Server feature allows the Easy VPN server to “push” the backup server list to the Easy VPN remote.

The backup list allows the administrator to control the backup servers to which a specific Easy VPN remote will connect in case of failure, retransmissions, or dead peer detection (DPD) messages.

**Note**

Before the backup server feature can work, the backup server list has to be configured on the server.

#### How a Backup Server Works

If remote A goes to server A and the connection fails, remote A goes to server B. If server B has a backup list configured, that list will override the backup server list of server A. If the connection to server B fails, remote A will continue through the backup servers that have been configured.

**Note**

If you are in auto mode and you have a failure, you will transition automatically from server A to server B. However, if you are in manual mode, you have to configure the transition manually. To configure the transition manually, use the **crypto ipsec client ezvpn** command with the **connect** keyword.

No new configuration is required at the Easy VPN remote to enable this feature. If you want to display the current server, you can use the **show crypto ipsec client ezvpn** command. If you want to find out which peers were pushed by the Easy VPN server, you can use the same command.

To troubleshoot this feature, use the **debug crypto ipsec client ezvpn** command. If more information is needed for troubleshooting purposes, use the **debug crypto isakmp** command. The **show crypto ipsec client ezvpn** command may also be used for troubleshooting.

## Cisco Easy VPN Remote Features

The Cisco Easy VPN Remote feature is a collection of features that improves the capabilities of the Cisco Easy VPN Remote feature introduced in Cisco IOS Release 12.2(4)YA. The Cisco Easy VPN Remote feature includes the following:

- [Default Inside Interface, page 20](#)—This feature supports the autoconfiguration of the default Easy VPN inside interface for Cisco 800 series routers.
- [Multiple Inside Interfaces, page 21](#)—This feature allows you to configure up to eight inside interfaces on the Cisco Easy VPN remote.
- [Multiple Outside Interfaces, page 21](#)—This feature allows you to configure up to four outside tunnels for outside interfaces.
- [VLAN Support, page 21](#)—This feature allows VLANs to be configured as valid Easy VPN inside interfaces.
- [Multiple Subnet Support, page 22](#)—This feature allows multiple subnets from the Easy VPN inside interface to be included in the Easy VPN tunnel.
- [NAT Interoperability Support, page 22](#)—This feature automatically restores the NAT configuration when the IPsec VPN tunnel is disconnected.
- [Local Address Support, page 22](#)—The Cisco Easy VPN Remote feature is enhanced to support an additional **local-address** attribute that specifies which interface is used to determine the IP address used to source the Easy VPN tunnel traffic.
- [Peer Hostname, page 23](#)—When a peer is defined as a hostname, the hostname is stored and the Domain Name System (DNS) lookup is done at the time of tunnel connection.
- [Proxy DNS Server Support, page 23](#)—This feature allows you to configure the router in a Cisco Easy VPN remote configuration to act as a proxy DNS server for LAN-connected users.
- [Cisco IOS Firewall Support, page 23](#)—This feature supports Cisco IOS Firewall configurations on all platforms.
- [Easy VPN Remote and Server on the Same Interface, page 23](#)—The Easy VPN remote and Easy VPN server are supported on the same interface, which makes it possible to establish a tunnel to another Easy VPN server and terminate the Easy VPN software client on the same interface simultaneously.
- [Easy VPN Remote and Site to Site on the Same Interface, page 23](#)—The Easy VPN Remote and site to site (crypto map) are supported on the same interface, which makes it possible to establish a tunnel to another Easy VPN server and have another site to site on the same interface simultaneously.
- [Cisco Easy VPN Remote Web Managers, page 24](#)—Users can manage the Cisco Easy VPN Remote feature on the Cisco uBR905 and Cisco uBR925 cable access routers using a built-in web interface.
- [Dead Peer Detection Periodic Message Option, page 24](#)—This feature allows you to configure your router to query the liveliness of its IKE peer at regular intervals.
- [Load Balancing, page 24](#)—If a remote device is loaded and unable to accept more traffic, the VPN 3000 will send a notify message that contains an IP address that represents the new IKE server to which the remote should connect.

- [Management Enhancements, page 25](#)—This feature allows for remote management of the VPN remote.
- [PFS Support, page 25](#)—The PFS configuration mode attribute is sent by the server if requested by the VPN remote device.
- [Dial Backup, page 25](#)—This feature allows you to configure a dial backup tunnel connection on your remote device.
- [Virtual IPsec Interface Support, page 27](#)—This feature allows you to selectively send traffic to different Easy VPN concentrators as well as to the Internet (includes a reference to the IPsec Virtual Tunnel Interface feature.)
- [Dual Tunnel Support, page 29](#)—This feature allows you to configure multiple Easy VPN tunnels that share common inside and outside interfaces to connect two peers to two different VPN servers simultaneously.
- [Banner, page 32](#)—The EasyVPN remote device can download a banner that has been pushed by the Easy VPN server. The banner can be used for Xauth and web-based activation. The banner is displayed when the Easy VPN tunnel is “up” on the Easy VPN remote console or as an HTML page in the case of web-based activation.
- [Configuration Management Enhancements \(Pushing a Configuration URL Through a Mode-Configuration Exchange\), page 33](#)—The Easy VPN remote device can download a URL that is pushed by the Easy VPN server, allowing the Easy VPN remote device to download configuration content and apply it to the running configuration.
- [Reactivate Primary Peer, page 33](#)—This feature allows you to designate a primary peer. When an Easy VPN device fails over from the primary peer to a backup peer and the primary peer is again available, connections with the backup peer are torn down and a connection is made with the primary peer.
- [Identical Addressing Support, page 33](#)—This feature integrates Network Address Translation (NAT) with Easy VPN to allow remotes with overlapping internal IP addressing to connect to the Easy VPN server.
- [cTCP Support on Easy VPN Clients, page 34](#)—When cTCP is enabled on a remote device (client) and headend device, IKE and ESP (Protocol 50) traffic is encapsulated in the TCP header so that the firewalls in between the client and the headend device permit this traffic (considering it the same as TCP traffic).

## Default Inside Interface

Easy VPN Remote supports the autoconfiguration of the default Easy VPN inside interface for Cisco 800 series routers. The interface Ethernet 0 is the default inside interface.

If you want to disable the default inside interface and configure another inside interface on the Cisco 800 series router, you must configure the other inside interface first and then disable the default inside interface. You can use the following command to disable the default inside interface:

```
no crypto ipsec client ezvpn name inside
```

If you did not configure the other inside interface first before disabling the default inside interface, you will receive a message such as the following (see lines three and four):

```
Router (config)# interface ethernet0
Router (config-if)# no crypto ipsec client ezvpn hw-client inside
Cannot remove the single inside interface unless
one other inside interface is configured
```

## Multiple Inside Interfaces

Inside interface support is enhanced in the Cisco Easy VPN Remote feature to support multiple inside interfaces for all platforms. Inside interfaces can be configured manually with the enhanced command and subcommand:

```
interface interface-name
 crypto ipsec client ezvpn name [outside | inside]
```

See the “[Configuring Multiple Inside Interfaces](#)” section for information on how to configure more than one inside interface.

Multiple inside interfaces offer the following capabilities:

- Up to eight inside interfaces are supported on the Cisco 800 and Cisco 1700 series routers.
- At least one inside interface must be configured for each outside interface; otherwise, the Cisco Easy VPN Remote feature does not establish a connection.
- Adding a new inside interface or removing an existing inside interface automatically resets the Cisco Easy VPN Remote connection (the currently established tunnel). You must reconnect a manually configured tunnel, and if Xauth is required by the Cisco Easy VPN server, the user is reprompted. If you have set the Cisco Easy VPN Remote configuration to connect automatically and no Xauth is required, no user input is required.
- Inside interfaces that are configured or the default setting can be shown by using the **show crypto ipsec client ezvpn** command.

## Multiple Outside Interfaces

The Easy VPN Remote feature supports one Easy VPN tunnel per outside interface. You can configure up to four Easy VPN tunnels per Cisco router. Each Easy VPN tunnel can have multiple inside interfaces configured, but they cannot overlap with another Easy VPN tunnel unless dial backup is configured. For more information about dial backup, see the section “[Dial Backup](#).” To configure multiple outside interfaces, use the **crypto ipsec client ezvpn** command and **outside** keyword.

To disconnect or clear a specific tunnel, the **clear crypto ipsec client ezvpn** command specifies the IPsec VPN tunnel name. If there is no tunnel name specified, all existing tunnels are cleared.

See the “[Configuring Multiple Outside Interfaces](#)” section for more information on configuring more than one outside interface.

## VLAN Support

Inside interface support on VLANs makes it possible to have valid Easy VPN inside interface support on a VLAN, which was not possible before Cisco IOS Release 12.3(7)XR. With this feature, SAs can be established at connection using the VLAN subnet address or mask as a source proxy.

For the inside interface support on VLANs to work, you must define each VLAN as an Easy VPN inside interface. In addition, IPsec SAs should be established for each inside interface in the same manner as for other inside interfaces. For more information about inside and outside interfaces, see the sections “[Multiple Inside Interfaces](#)” and “[Multiple Outside Interfaces](#).”

Inside interface support on VLANs is supported only on Cisco routers that support VLANs.

## Multiple Subnet Support

For situations in which you have multiple subnets connected to an Easy VPN inside interface, you can optionally include these subnets in the Easy VPN tunnel. First, you must specify the subnets that should be included by defining them in an ACL. To configure an ACL, see “Access control lists, configuring” in the “[Additional References](#)” section. Next, you have to use the **acl** subcommand of the **crypto ipsec client ezvpn** (global) command to link your ACL to the Easy VPN configuration. Easy VPN Remote will automatically create the IPsec SAs for each subnet that is defined in the ACL as well as for the subnets that are defined on the Easy VPN inside interface.

**Note**

---

Multiple subnet support is not supported in client mode.

---

## NAT Interoperability Support

Cisco Easy VPN Remote supports interoperability with NAT. You can have a NAT configuration and a Cisco Easy VPN Remote configuration that coexist. When an IPsec VPN tunnel is down, the NAT configuration works.

In the Cisco Easy VPN Remote feature, the router automatically restores the previous NAT configuration when the IPsec VPN tunnel is torn down. The user-defined access lists are not disturbed. Users can continue to access nontunnel areas of the Internet when the tunnel times out or disconnects.

**Note**

---

NAT interoperability is not supported in client mode with split tunneling.

---

## Local Address Support

The Cisco Easy VPN Remote feature is enhanced to support an additional **local-address** attribute. This attribute specifies which interface is used to determine the IP address that is used to source the Easy VPN Remote tunnel traffic. After specifying the interface with the **local-address** subcommand, you can manually assign a static IP address to the interface or use the **cable-modem dhcp-proxy interface** command to automatically configure the specified interface with a public IP address. See the “[Configuring Proxy DNS Server Support](#)” section for configuration information.

Local Address Support is available for all platforms, but it is more applicable to the Cisco uBR905 and Cisco uBR925 cable access routers in conjunction with the **cable-modem dhcp-proxy interface** command. Typically, the loopback interface is the interface used to source tunnel traffic for the Cisco uBR905 and Cisco uBR925 cable access routers.

In a typical DOCSIS network, the Cisco uBR905 and Cisco uBR925 cable access routers are normally configured with a private IP address on the cable modem interface. In the initial Cisco Easy VPN Remote feature, a public IP address was required on the cable modem interface to support the Easy VPN remote.

In the Cisco Easy VPN Remote feature, cable providers can use the Cable DHCP Proxy feature to obtain a public IP address and assign it to the cable modem interface, which is usually the loopback interface.

For more information on the **cable-modem dhcp-proxy interface** command, see the “[Cable CPE Commands](#)” chapter in the *Cisco Broadband Cable Command Reference Guide*.

**Note**

---

The **cable-modem dhcp-proxy interface** command is supported only for the Cisco uBR905 and Cisco uBR925 cable access routers.

---



## Peer Hostname

The peer in a Cisco Easy VPN Remote configuration can be defined as an IP address or a hostname. Typically, when a peer is defined as a hostname, a DNS lookup is done immediately to get an IP address. In the Cisco Easy VPN Remote feature, the peer hostname operation is enhanced to support DNS entry changes. The text string of the hostname is stored so that the DNS lookup is done at the time of the tunnel connection, not when the peer is defined as a hostname.

See the “[Configuring and Assigning the Easy VPN Remote Configuration](#)” section for information on enabling the peer hostname functionality.

## Proxy DNS Server Support

When the Easy VPN tunnel is down, the DNS addresses of the ISP or cable provider should be used to resolve DNS requests. When the WAN connection is up, the DNS addresses of the enterprise should be used.

As a way of implementing use of the DNS addresses of the cable provider when the WAN connection is down, the router in a Cisco Easy VPN Remote configuration can be configured to act as a proxy DNS server. The router, acting as a proxy DNS server for LAN-connected users, receives DNS queries from local users on behalf of the real DNS server. The DHCP server then can send out the LAN address of the router as the IP address of the DNS server. After the WAN connection comes up, the router forwards the DNS queries to the real DNS server and caches the DNS query records.

See the “[Configuring Proxy DNS Server Support](#)” section for information on enabling the proxy DNS server functionality.

## Cisco IOS Firewall Support

The Cisco Easy VPN Remote feature works in conjunction with Cisco IOS Firewall configurations on all platforms.

## Easy VPN Remote and Server on the Same Interface

This feature allows the Easy VPN remote and Easy VPN server to be supported on the same interface, making it possible to both establish a tunnel to another Easy VPN server and terminate the Easy VPN software client on the same interface simultaneously. A typical application would be a geographically remote location for which Easy VPN Remote is being used to connect to a corporate Easy VPN server and also to terminate local software client users.

For more information about the Easy VPN Remote and Server on the Same Interface feature, see “Easy VPN Remote and Server on the Same Interface” in the section “[Additional References](#).”

## Easy VPN Remote and Site to Site on the Same Interface

This feature allows the Easy VPN remote and site to site (crypto map) to be supported on the same interface, making it possible to both establish a tunnel to another Easy VPN server and have another site to site on the same interface simultaneously. A typical application would be a third-party VPN service provider that is managing a remote router via the site-to-site tunnel and using Easy VPN Remote to connect the remote site to a corporate Easy VPN server.

For more information about the Easy VPN Remote and Site to Site on the Same Interface feature, see “Easy VPN Remote and Site to Site on the Same Interface” in the section “[Additional References](#).”

## Cisco Easy VPN Remote Web Managers

Web interface managers may be used to manage the Cisco Easy VPN Remote feature. One such web interface manager is SDM, which is supported on the Cisco 830 series, Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. SDM enables you to connect or disconnect the tunnel and provides a web interface for Xauth. For more information about SDM, see [Cisco Security Device Manager](#).

A second web interface manager is the Cisco Router Web Setup (CRWS) tool, which is supported on the Cisco 806 router. The CRWS provides a similar web interface as SDM.

A third web interface manager, Cisco Easy VPN Remote Web Manager, is used to manage the Cisco Easy VPN Remote feature for Cisco uBR905 and Cisco uBR925 cable access routers. You do not need access to the CLI to manage the Cisco Easy VPN remote connection.

The web interface managers allow you to do the following:

- See the current status of the Cisco Easy VPN remote tunnel.
- Connect a tunnel that is configured for manual control.
- Disconnect a tunnel that is configured for manual control or reset a tunnel configured for automatic connection.
- Be prompted for Xauth information, if needed.

See the [“Troubleshooting the VPN Connection”](#) section for more information about Cisco Easy VPN Remote Web Manager.

## Dead Peer Detection Periodic Message Option

The dead peer detection periodic message option allows you to configure your router to query the liveness of its IKE peer at regular intervals. The benefit of this approach over the default approach (on-demand dead peer detection) is earlier detection of dead peers. For more information about the dead peer detection periodic message option, see *“Dead peer detection”* in the section [“Additional References.”](#)

## Load Balancing

When the Cisco VPN 3000 concentrator is configured for load balancing, the VPN 3000 will accept an incoming IKE request from the VPN remote on its virtual IP address. If the device is loaded and unable to accept more traffic, the VPN 3000 will send a notify message that contains an IP address that represents the new IKE server to which the remote should connect. The old connection will be torn down and a new connection established to the redirected VPN gateway.

There is no configuration required for load balancing to occur. If the VPN gateway is configured for load balancing, and it notifies the VPN remote that it is performing load balancing, the VPN remote has access to the load balancing feature.

To verify whether load balancing is occurring, use the **debug crypto isakmp**, **debug crypto ipsec client ezvpn**, and **show crypto ipsec** commands. To troubleshoot the load balancing process, use the **show crypto ipsec** command.

## Management Enhancements

Management enhancements for Easy VPN remotes allow for the remote management of the VPN remote. The feature provides for the IPv4 address to be pushed by configuration mode to the VPN remote. The IPv4 address is assigned to the first available loopback interface on the VPN remote, and any existing statically defined loopbacks are not overridden. On disconnect, the address and loopback interface are removed from the list of active interfaces.

After the VPN remote is connected, the loopback interface should be accessible from the remote end of the tunnel. All PAT activities will be translated through this interface IP address.

If a loopback exists, and an IP address is associated with it and its state is unassigned, the interface is a good candidate for mode configuration address management.

**Note**

After you assign an address to the loopback interface, if you save the configuration to NVRAM and reboot the VPN remote, the configuration address is permanently contained in the configuration. If you saved the configuration to NVRAM and rebooted the VPN remote, you must enter configuration mode and remove the IP address from the loopback interface manually.

You can use the **show ip interface** command with the **brief** keyword to verify that a loopback has been removed. The output of this **show** command also displays the interface.

## PFS Support

The PFS configuration mode attribute is sent by the server if requested by the VPN remote device. If any subsequent connection by the remote device shows that PFS is not received by the remote, PFS will not be sent in IPsec proposal suites.

**Note**

The PFS group that will be proposed in the IPsec proposal suites is the same as the group used for IKE.

You can use the **show crypto ipsec client ezvpn** command to display the PFS group and to verify that you are using PFS.

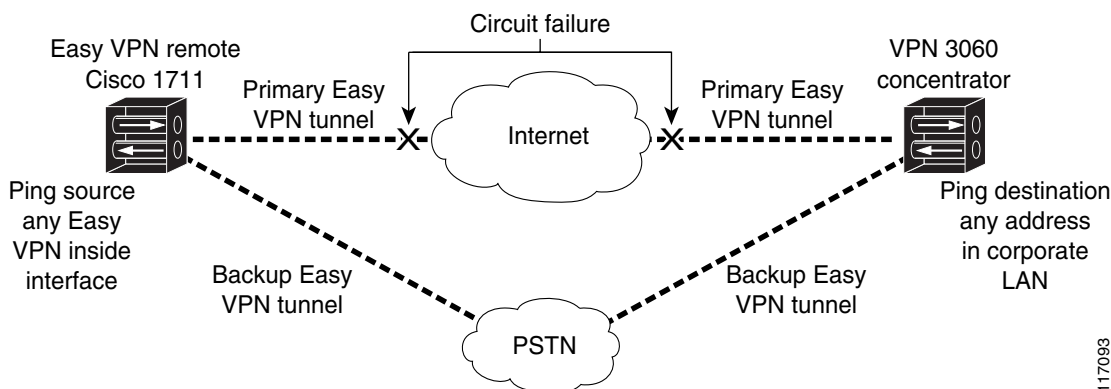
## Dial Backup

**Note**

The Dial Backup feature is not available in Cisco IOS Release 12.3(11)T.

Dial backup for Easy VPN remotes allows you to configure a dial backup tunnel connection on your remote device. The backup feature is “brought up” only when real data has to be sent, eliminating the need for expensive dialup or ISDN links that must be created and maintained even when there is no traffic.

[Figure 10](#) illustrates a typical Easy VPN remote-with-dial-backup scenario. In this scenario, a Cisco 1751 remote device is attempting to connect to another Cisco 1751 (acting as a server). There is a failure in the primary Easy VPN tunnel, and the connection is rerouted through the Easy VPN backup tunnel to the Cisco 1751 server.

**Figure 10** *Dial Backup for Easy VPN Scenario*

## Dial Backup Using a Dial-on-Demand Solution

IP static route tracking enable Cisco IOS software to identify when a Point-to-Point Protocol over Ethernet (PPPoE) or IPsec VPN tunnel “goes down” and initiates a Dial-on-Demand (DDR) connection to a preconfigured destination from any alternative WAN or LAN port (for example, a T1, ISDN, analog, or auxiliary port). The failure may be caused by several catastrophic events (for example, by Internet circuit failures or peer device failure). The remote route has only a static route to the corporate network. The IP static-route-tracking feature allows an object to be tracked (using an IP address or hostname) using Internet Control Message Protocol (ICMP), TCP, or other protocols, and it installs or removes the static route on the basis of the state of the tracked object. If the tracking feature determines that Internet connectivity is lost, the default route for the primary interface is removed, and the floating static route for the backup interface is enabled.

## Dial Backup Using Object Tracking

IP static route tracking must be configured for dial backup on an Easy VPN remote device to work. The object tracking configuration is independent of the Easy VPN remote dial backup configuration. (For more information about object tracking, see the feature guide [Reliable Static Routing Backup Using Object Tracking](#).)

## Easy VPN Remote Dial Backup Support Configuration

You can configure dial backup for your Easy VPN remote using two Easy VPN remote options that allow a connection to the backup Easy VPN configuration and a connection to the tracking system.

- To specify the Easy VPN configuration that will be activated when backup is triggered, use the **backup** subcommand of the **crypto ipsec client ezvpn** (global) command.
- The Easy VPN remote device registers to the tracking system to get the notifications for change in the state of the object. Use the **track** subcommand to inform the tracking process that the Easy VPN remote device is interested in tracking an object, which is identified by the object number. The tracking process, in turn, informs the Easy VPN remote device when the state of this object changes. This notification prompts the Easy VPN remote device when the state of this object changes. This notification prompts the Easy VPN remote device to bring up the backup connection when the tracked object state is DOWN. When the tracked object is UP again, the backup connection is torn down and the Easy VPN remote device will switch back to using the primary connection.

**Note**

Only one backup configuration is supported for each primary Easy VPN configuration. Each inside interface must specify the primary and backup Easy VPN configuration.

## Dynamically Addressed Environments

To allow dial backup to be deployed in dynamically addressed environments, use the IP SLA Pre-Routed ICMP Echo Probe feature. (For more information about this feature, see [Cisco 1700 Series- Cisco IOS Release 12.3\(7\)XR](#) release notes. To use the IP SLA Pre-Routed ICMP Echo Probe feature, use the **icmp-echo** command with the **source-interface** keyword.

## Dial Backup Examples

For examples of dial backup configurations, see the section “[Dial Backup: Examples](#).”

## Virtual IPsec Interface Support

The Virtual IPsec Interface Support feature provides a routable interface to selectively send traffic to different Easy VPN concentrators as well as to the Internet.

Before Cisco IOS Release 12.4(4)T, at the tunnel-up/tunnel-down transition, attributes that were pushed during the mode configuration had to be parsed and applied. When such attributes resulted in the configurations being applied on the interface, the existing configuration had to be overridden. With the Virtual IPsec Interface Support feature, the tunnel-up configuration can be applied to separate interfaces, making it easier to support separate features at tunnel-up time. Features that are applied to the traffic going into the tunnel can be separate from the features that are applied to traffic that is not going through the tunnel (for example, split-tunnel traffic and traffic leaving the device when the tunnel is not up). When the Easy VPN negotiation is successful, the line protocol state of the virtual-access interface gets changed to up. When the Easy VPN tunnel goes down because the security association (SA) expires or is deleted, the line protocol state of the virtual-access interfaces changes to down.

Routes act as traffic selectors in an Easy VPN virtual interface, that is, the routes replace the access list on the crypto map. In a virtual-interface configuration, Easy VPN negotiates a single IPsec SA if the Easy VPN server has been configured with a dynamic virtual IPsec interface. This single SA is created irrespective of the Easy VPN mode that is configured.

After the SA is established, routes that point to the virtual-access interface are added to direct traffic to the corporate network. Easy VPN also adds a route to the VPN concentrator so that IPsec-encapsulated packets get routed to the corporate network. A default route that points to the virtual-access interface is added in the case of a nonsplit mode. When the Easy VPN server “pushes” the split tunnel, the split tunnel subnet becomes the destination to which the routes that point to the virtual access are added. In either case, if the peer (VPN concentrator) is not directly connected, Easy VPN adds a route to the peer.

**Note**

- Most routers that run the Cisco Easy VPN Client software have a default route configured. The default route that is configured should have a metric value greater than 1. The metric value must be greater than 1 because Easy VPN adds a default route that has a metric value of 1. The route points to the virtual-access interface so that all traffic is directed to the corporate network when the concentrator does not “push” the split tunnel attribute.

For more information about the IPsec Virtual Tunnel Interface feature, see the document *IPSec Virtual Tunnel Interface* (URL link provided in the “[Related Documents](#)” section of this document [*General Information on IPsec and VPN*]).

[Table 1](#) presents the different methods of configuring a remote device and the corresponding headend IPsec aggregator configurations. Each row represents a way to configure a remote device. The third column shows the different headend configurations that can be used with IPsec interfaces. See [Table 2](#) for a description of terms that are used in [Table 1](#) and [Table 3](#).

**Table 1** *How Different Remote Device Configurations Interact with Various Headends and Configurations*

| Remote Device Configurations | IOS Headend – Using Crypto Maps                                                                                                                                                                                                                                           | IOS Headend – Using IPsec Interfaces                                                                                                                                                                                                                                         | VPN3000/ASA                                                                                                        |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Crypto maps                  | <ul style="list-style-type: none"> <li>Supported.</li> </ul>                                                                                                                                                                                                              | —                                                                                                                                                                                                                                                                            | —                                                                                                                  |
| Easy VPN virtual interface   | <ul style="list-style-type: none"> <li>Supported.</li> <li>Will create multiple SAs for a split tunnel.</li> <li>Because there is no interface on the headend, interface features cannot be supported.</li> <li>Limited quality of service (QoS) is supported.</li> </ul> | <ul style="list-style-type: none"> <li>Supported.</li> <li>Creates only a single SA in split and no-split tunnels.</li> <li>Route injection is accomplished on the server.</li> <li>Routes are injected on the remote devices to direct traffic to the interface.</li> </ul> | <ul style="list-style-type: none"> <li>Supported.</li> <li>Will create multiple SAs for a split tunnel.</li> </ul> |
| Legacy Easy VPN              | <ul style="list-style-type: none"> <li>Creates a single IPsec SA on the headend when a default policy is pushed.</li> <li>Creates multiple SAs when a split-tunnel policy is pushed to the remote device.</li> </ul>                                                      | <ul style="list-style-type: none"> <li>Not supported.</li> <li>Cannot be used with split tunnels because the headend interface does not support multiple SAs on a single interface.</li> </ul>                                                                               | <ul style="list-style-type: none"> <li>Supported.</li> <li>Creates multiple SAs for split tunnels.</li> </ul>      |
| Static virtual interface     | <ul style="list-style-type: none"> <li>Not supported.</li> </ul>                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>Supported.</li> <li>Can be used with a static interface or dynamic interface on the headend.</li> <li>Routing support is mandatory to reach the network.</li> </ul>                                                                   | <ul style="list-style-type: none"> <li>Not supported.</li> </ul>                                                   |

[Table 2](#) provides a description of the terms used in [Table 1](#) and [Table 3](#).

**Table 2**      **Terms Used in [Table 1](#) and [Table 3](#)**

| Terms                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ASA                                                                     | Cisco Adaptive Security Appliance, a threat-management security appliance.                                                                                                                                                                                                                                                                                                           |
| Crypto maps                                                             | Commonly used for configuring IPsec tunnels. The crypto map is attached to an interface. For more information on crypto maps, see the section “Creating Crypto Map Sets” of the “Configuring Security for VPNs with IPsec” chapter of the <i>Cisco IOS Security Configuration Guide</i> . (URL link provided in the “ <a href="#">Related Documents</a> ” section of this document.) |
| Easy VPN dual tunnel remote device                                      | Two Easy VPN remote device configurations in which both are using a dynamic IPsec virtual tunnel interface.                                                                                                                                                                                                                                                                          |
| Easy VPN virtual interface remote device (Easy VPN virtual interface)   | Easy VPN remote configuration that configures the usage of a dynamic IPsec virtual tunnel interface.                                                                                                                                                                                                                                                                                 |
| IPsec interface                                                         | Consists of static and dynamic IPsec virtual interfaces.                                                                                                                                                                                                                                                                                                                             |
| IPsec Virtual Tunnel Interface                                          | Tunnel interface that is created from a virtual template tunnel interface using mode IPsec. For more information on virtual tunnel interface configurations, see the document <i>IPSec Virtual Tunnel Interface</i> (URL link provided in the “ <a href="#">Related Documents</a> ” section of this document [ <i>General Information on IPsec and VPN</i> ]).                       |
| Legacy Easy VPN                                                         | Easy VPN remote device configuration that uses crypto maps and does not use IPsec interfaces.                                                                                                                                                                                                                                                                                        |
| Static IPsec virtual tunnel interface (static virtual tunnel interface) | Tunnel interface used with mode IPsec that proposes and accepts only an “ipv4 any any” selector. For more information on static virtual tunnel interface configurations, see the document <i>IPSec Virtual Tunnel Interface</i> (URL link provided in the “ <a href="#">Related Documents</a> ” section of this document [ <i>General Information on IPsec and VPN</i> ]).           |
| VPN 3000                                                                | Cisco VPN 3000 series routers.                                                                                                                                                                                                                                                                                                                                                       |

## Dual Tunnel Support

Easy VPN now supports the ability to configure two easy VPN tunnels that have the same inside and outside interfaces. The feature is called the Easy VPN Dual Tunnel. Configuring multiple tunnels on a single remote device can be accomplished in a number of ways, which are listed below in [Table 3](#) along with their configuration and usage considerations. Further discussion in this section refers to only one such method of configuring dual tunnels using Easy VPN tunnels that have virtual interfaces. This method will be referred to as Dual Tunnel Support.

In a dual-tunnel Easy VPN setup, each Easy VPN tunnel is configured using virtual IPsec interface support, as shown in the section “[Virtual IPsec Interface Support](#).” Each Easy VPN tunnel has its unique virtual interface, which is created when the Easy VPN configuration is complete.

There are two possible combinations in which the dual tunnels can be used.

- Dual Easy VPN tunnels that have one tunnel using a nonsplit tunnel policy and the other tunnel using a split tunnel policy that has been pushed from the respective headend.

- Dual Easy VPN tunnel in which both tunnels are using an independent split tunnel policy that has been pushed from the respective headend.

**Note**

It is not permitted to have dual Easy VPN tunnels in which both tunnels are using a nonsplit tunnel policy.

The Easy VPN dual tunnel makes use of route injections to direct the appropriate traffic through the correct Easy VPN virtual tunnel interface. When the Easy VPN tunnel on the remote device “comes up,” it “learns” the split or nonsplit policy from the headend. The Easy VPN remote device injects routes in its routing table that correspond to the nonsplit networks that have been learned. If the headend pushes a nonsplit tunnel policy to the Easy VPN remote device, the Easy VPN remote device installs a default route in its routing table that directs all traffic out of the Easy VPN virtual interface that corresponds to this Easy VPN tunnel. If the headend pushes split-tunnel networks to the remote device, the remote device installs specific routes to the split networks in its routing table, directing the traffic to these networks out of the virtual tunnel interface.

**Note**

Dual Tunnel Easy VPN uses destination-based routing to send traffic to the respective tunnels.

Output features can be applied to this virtual interface. Examples of such output features are Cisco IOS Quality of Service and Cisco IOS Firewall. These features must be configured on the virtual template that is configured in the Easy VPN client configuration.

[Table 3](#) explains how this feature should be used. See [Table 2](#) for a description of terms that are used in [Table 1](#) and [Table 3](#).



**Table 3**      **Dual Tunnel Usage Guidelines**

| <b>Dual Tunnel Combinations</b>                             | <b>Headends Supported</b> | <b>Configuration and Usage Considerations on the Easy VPN Remote Device and Headend</b>                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Two legacy Easy VPN tunnels                                 | IOS, ASA, and VPN 3000    | <ul style="list-style-type: none"> <li>Two tunnels cannot share a common outside interface.</li> <li>Two tunnels cannot share a common inside interface.</li> <li>The two tunnels should use separate inside and outside interfaces.</li> <li>Traffic from an inside interface that belongs to one Easy VPN tunnel cannot be pushed into another tunnel.</li> </ul> |
| One legacy Easy VPN tunnel and one crypto map               | IOS, ASA, and VPN 3000    | The crypto map can share the same outside interface as the legacy Easy VPN client configuration. However, the behavior of the two remote devices depends on the mode of Easy VPN as well as the IPsec selectors of the crypto map and the Easy VPN remote device. This is not a recommended combination.                                                            |
| One legacy Easy VPN tunnel and one static virtual interface | IOS                       | Both tunnels cannot terminate on the same headend. The static virtual interface remote device tunnel has to be terminated on a static virtual interface on the headend router. The legacy Easy VPN remote device tunnel can terminate on the virtual tunnel interface or crypto map that is configured on the headend.                                              |

**Table 3**      **Dual Tunnel Usage Guidelines (continued)**

| <b>Dual Tunnel Combinations</b>                                 | <b>Headends Supported</b> | <b>Configuration and Usage Considerations on the Easy VPN Remote Device and Headend</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| One legacy Easy VPN tunnel and one Easy VPN virtual interface   | IOS, ASA, and VPN 3000    | <ul style="list-style-type: none"> <li>Both tunnels cannot terminate on the same headend.</li> <li>The legacy Easy VPN tunnel and the Easy VPN virtual interface can share a common inside and outside interface.</li> <li>An Easy VPN virtual interface should be used only with split tunneling.</li> <li>Legacy Easy VPN can use a split tunnel or no split tunnel.</li> <li>The Web-Based Activation feature cannot be applied on both Easy VPN tunnels.</li> <li>Using two Easy VPN virtual interfaces is preferable to using this combination.</li> </ul> |
| One Easy VPN virtual interface and one static virtual interface | IOS                       | <ul style="list-style-type: none"> <li>Both tunnels cannot terminate on the same peer. The static virtual interface and the Easy VPN virtual interface can use the same outside interface.</li> <li>The Easy VPN virtual interface should use split tunneling.</li> </ul>                                                                                                                                                                                                                                                                                       |
| Two Easy VPN virtual interfaces                                 | IOS, ASA, and VPN 3000    | <ul style="list-style-type: none"> <li>Both tunnels cannot terminate on the same peer.</li> <li>At least one of the tunnels should use split tunneling.</li> <li>Web-Based Activation cannot be applied to both Easy VPN tunnels.</li> </ul>                                                                                                                                                                                                                                                                                                                    |

## Banner

The Easy VPN server pushes a banner to the Easy VPN remote device. The Easy VPN remote device can use the banner during Xauth and web-based activation. The Easy VPN remote device displays the banner the first time that the Easy VPN tunnel is brought up.

The banner is configured under group configuration on the Easy VPN server.

## Configuration Management Enhancements (Pushing a Configuration URL Through a Mode-Configuration Exchange)

After this feature has been configured on the server using the commands **configuration url** and **configuration version** (subcommands under the **crypto isakmp client configuration group** command), the server can “push” the configuration URL and configuration version number to the Easy VPN remote device. With this information, the Easy VPN remote device can download the configuration content and apply it to its running configuration. For more information about this feature, see the section “Configuration Management Enhancements” in the *Easy VPN Server* feature module.

## Reactivate Primary Peer

The Reactivate Primary Peer feature allows a default primary peer to be defined. The default primary peer (a server) is one that is considered better than other peers for reasons such as lower cost, shorter distance, or more bandwidth. With this feature configured, if Easy VPN fails over during Phase 1 SA negotiations from the primary peer to the next peer in its backup list, and if the primary peer is again available, the connections with the backup peer are torn down and the connection is again made with the primary peer.

Dead Peer Detection is one of the mechanisms that acts as a trigger for primary peer reactivation. Idle timers that are configured under Easy VPN is another triggering mechanism. When configured, the idle timer detects inactivity on the tunnel and tears it down. A subsequent connect (which is immediate in auto mode) is attempted with the primary preferred peer rather than with the peer last used.

**Note**

---

Only one primary peer can be defined.

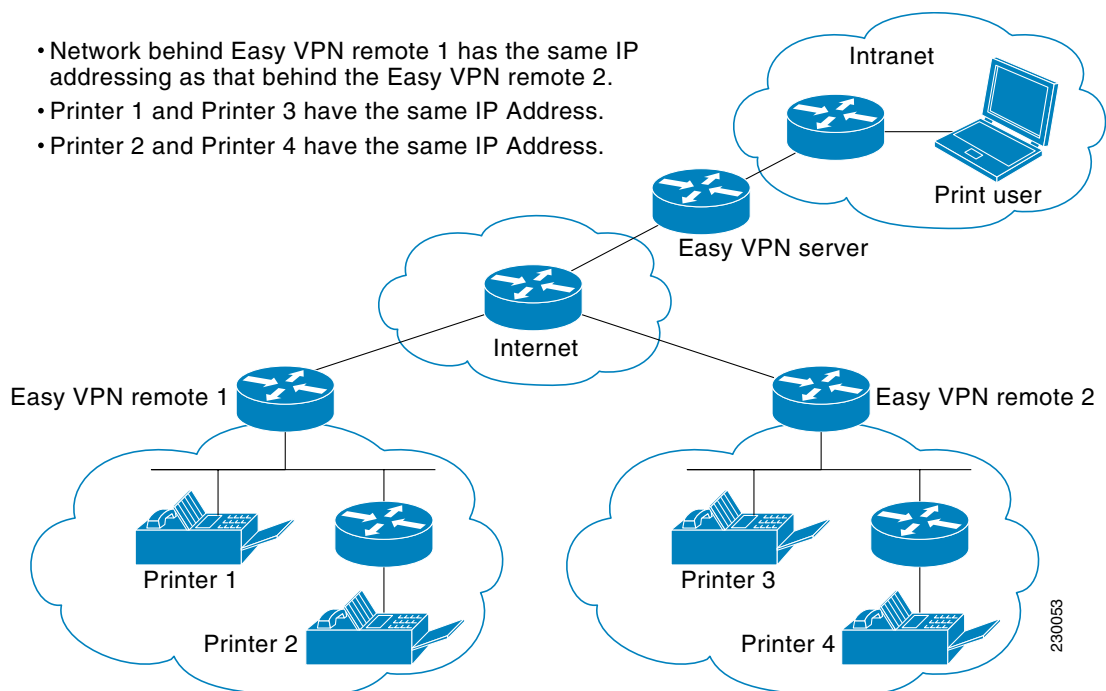
---

## Identical Addressing Support

The Identical Addressing Support feature supports identically addressed LANs on Easy VPN remotes. Network resources, such as printers and web servers on the LAN side of the EasyVPN remotes, that have overlapping addressing with other Easy VPN remotes are now reachable. The Easy VPN Remote feature was enhanced to work with NAT to provide this functionality.

- The Easy VPN server requires no changes to support the Identical Addressing Support feature.
- The Identical Addressing Support feature is supported only in network extension modes (network-extension and network-plus).
- Virtual tunnel interfaces must be configured on the Easy VPN remote before using the Identical Addressing Support feature.

Figure 11 shows an example of the Identical Addressing Support feature configuration.

**Figure 11 Identical Addressing Support**

The Identical Addressing Support feature can be configured with the following command and enhanced subcommands:

```
crypto ipsec client ezvpn <name>
```

#### Enhanced subcommands

- **nat acl** {*acl-name* | *acl-number*}—Enables split tunneling for the traffic specified by the ACL name or the ACL number.
  - The *acl-name* argument is the name of the ACL.
  - The *acl-number* argument is the number of the ACL.
- **nat allow**—Allows NAT to be integrated with Cisco Easy VPN.

For detailed steps on how to configure Identical Addressing Support, see “[Configuring Identical Addressing Support](#).”

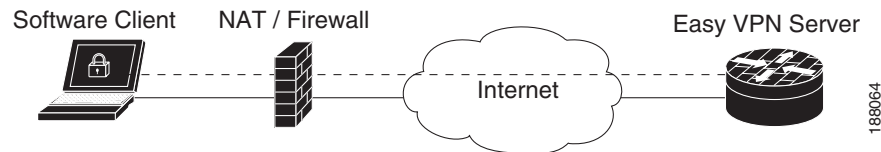
## cTCP Support on Easy VPN Clients

The Cisco Tunneling Control Protocol (cTCP) feature can be used for situations in which an Easy VPN client (remote device) is operating in an environment in which standard IPsec does not function or in which it does not function transparently without modification to existing firewall rules. These situations include the following:

- Small office or home office router performing Network Address Translation (NAT) or Port Address Translation (PAT)
- PAT-provided IP address behind a larger router (for example, in a corporation)
- Non-NAT firewall (packet filtering or stateful)
- Proxy server

Figure 12 illustrates how IPsec traffic that is tunneled inside the cTCP traverses Network Address Translation (NAT) and the firewall (see the dashed line).

**Figure 12** *cTCP on an Easy VPN Remote Device*



For detailed steps on how to configure cTCP on Easy VPN remote devices, see the section “[Configuring cTCP on an Easy VPN Client](#).”

For more information about cTCP support on Easy VPN remote devices, including configuration and troubleshooting examples, see “cTCP on Cisco Easy VPN remote devices” in the section “[Related Documents](#).”

## How to Configure Cisco Easy VPN Remote

This section includes the following required and optional tasks.

### Remote Tasks

- [Configuring and Assigning the Easy VPN Remote Configuration, page 36](#) (required)
- [Verifying the Cisco Easy VPN Configuration, page 38](#) (optional)
- [Configuring Save Password, page 39](#) (optional)
- [Configuring Manual Tunnel Control, page 40](#) (optional)
- [Configuring Automatic Tunnel Control, page 42](#) (optional)
- [Configuring Multiple Inside Interfaces, page 43](#) (optional)
- [Configuring Multiple Outside Interfaces, page 44](#) (optional)
- [Configuring Multiple Subnet Support, page 45](#) (optional)
- [Configuring Proxy DNS Server Support, page 47](#) (optional)
- [Configuring Dial Backup, page 47](#) (optional)
- [Configuring the DHCP Server Pool, page 48](#) (required)
- [Resetting a VPN Connection, page 48](#) (optional)
- [Monitoring and Maintaining VPN and IKE Events, page 49](#) (optional)
- [Configuring a Virtual Interface, page 50](#) (optional)
- [Troubleshooting Dual Tunnel Support, page 51](#) (optional)
- [Configuring Reactivate \(a Default\) Primary Peer, page 52](#) (optional)
- [Configuring Identical Addressing Support, page 53](#) (optional)
- [Configuring cTCP on an Easy VPN Client, page 56](#) (optional)
- [Restricting Traffic When a Tunnel Is Down, page 57](#) (optional)

**Easy VPN Server Tasks**

- [Configuring a Cisco IOS Easy VPN Server, page 58](#) (required)
- [Configuring an Easy VPN Server on a VPN 3000 Series Concentrator, page 58](#) (optional)
- [Configuring an Easy VPN Server on a Cisco PIX Firewall, page 60](#) (optional)

**Web Interface Tasks**

- [Configuring Web-Based Activation, page 61](#) (optional)
- [Monitoring and Maintaining Web-Based Activation, page 61](#) (optional)
- [Using SDM As a Web Manager, page 65](#) (optional)

**Troubleshooting the VPN Connection**

- [Troubleshooting a VPN Connection Using the Cisco Easy VPN Remote Feature, page 65](#) (optional)
- [Troubleshooting the Client Mode of Operation, page 65](#) (optional)
- [Troubleshooting Remote Management, page 66](#) (optional)
- [Troubleshooting Dead Peer Detection, page 66](#) (optional)

## Remote Tasks

### Configuring and Assigning the Easy VPN Remote Configuration

The router acting as the Easy VPN remote must create a Cisco Easy VPN Remote configuration and assign it to the outgoing interface. To configure and assign the remote configuration, perform the following steps.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **group** *group-name* **key** *group-key*
5. **peer** [*ip-address* | *hostname*]
6. **mode** {**client** | **network-extension**}
7. **exit**
8. **interface** *interface*
9. **crypto ipsec client ezvpn** *name* [**outside**]
10. **exit**
11. **exit**

## DETAILED STEPS

|        | Command                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>crypto ipsec client ezvpn name</b><br><br><b>Example:</b><br>Router (config)# crypto ipsec client ezvpn easy client remote                              | Creates a remote configuration and enters Cisco Easy VPN Remote configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 4 | <b>group group-name key group-key</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# group easy-vpn-remote-groupname key easy-vpn-remote-password | Specifies the IPsec group and IPsec key value to be associated with this configuration. <p><b>Note</b> The value of the <i>group-name</i> argument must match the group defined on the Easy VPN server. On Cisco IOS routers, use the <b>crypto isakmp client configuration group</b> and <b>crypto map dynmap isakmp authorization list</b> commands.</p> <p><b>Note</b> The value of the <i>group-key</i> argument must match the key defined on the Easy VPN server. On Cisco IOS routers, use the <b>crypto isakmp client configuration group</b> command.</p> |
| Step 5 | <b>peer [ip-address   hostname]</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# peer 192.185.0.5                                               | Specifies the IP address or hostname for the destination peer (typically the IP address on the outside interface of the destination route). <ul style="list-style-type: none"> <li>Multiple peers may be configured.</li> </ul> <p><b>Note</b> You must have a DNS server configured and available to use the <i>hostname</i> option.</p>                                                                                                                                                                                                                          |
| Step 6 | <b>mode {client   network-extension}</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# mode client                                               | Specifies the type of VPN connection that should be made. <ul style="list-style-type: none"> <li><b>client</b>—Specifies that the router is configured for VPN client operation, using NAT or PAT address translation. Client operation is the default if the type of VPN connection is not specified</li> <li><b>network-extension</b>—Specifies that the router is to become a remote extension of the enterprise network at the destination of the VPN connection.</li> </ul>                                                                                   |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# exit                                                                                   | Exits Cisco Easy VPN Remote configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|         | Command                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                           |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <b>interface</b> <i>interface</i><br><br><b>Example:</b><br>Router (config)# interface Ethernet1                                                                 | Enters interface configuration mode for the interface. <ul style="list-style-type: none"> <li>This interface will become the outside interface for the NAT or PAT translation.</li> </ul>                                                                                                                                                                         |
| Step 9  | <b>crypto ipsec client ezvpn</b> <i>name</i> [ <b>outside</b> ]<br><br><b>Example:</b><br>Router (config-if)# crypto ipsec client ezvpn easy_vpn remotel outside | Assigns the Cisco Easy VPN Remote configuration to the interface. <ul style="list-style-type: none"> <li>This configuration automatically creates the necessary NAT or PAT translation parameters and initiates the VPN connection (if you are in client mode).</li> </ul> <b>Note</b> The inside interface must be specified on Cisco 1700 and higher platforms. |
| Step 10 | <b>exit</b><br><br><b>Example:</b><br>Router (config-if)# exit                                                                                                   | Exits interface configuration mode.                                                                                                                                                                                                                                                                                                                               |
| Step 11 | <b>exit</b><br><br><b>Example:</b><br>Router (config)# exit                                                                                                      | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                  |

## Verifying the Cisco Easy VPN Configuration

To verify that the Cisco Easy VPN Remote configuration has been correctly configured, that the configuration has been assigned to an interface, and that the IPsec VPN tunnel has been established, perform the following steps.

### SUMMARY STEPS

1. **show crypto ipsec client ezvpn**
2. **show ip nat statistics**

### DETAILED STEPS

- Step 1** Display the current state of the Cisco Easy VPN Remote connection using the **show crypto ipsec client ezvpn** command. The following is typical output for a Cisco 1700 series router using client mode:

```
Router# show crypto ipsec client ezvpn
```

```
Tunnel name : hw1
Inside interface list: FastEthernet0/0, Serial0/0,
Outside interface: Serial1/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.0.0.5
Mask: 255.255.255.255
Default Domain: cisco.com
Tunnel name : hw2
Inside interface list: Serial0/1,
Outside interface: Serial1/1
Current State: IPSEC_ACTIVE
```



```
Last Event: SOCKET_UP
Default Domain: cisco.com
```

- Step 2** Display the NAT or PAT configuration that was automatically created for the VPN connection using the **show ip nat statistics** command. The “Dynamic mappings” field of this display gives the details for the NAT or PAT translation that is occurring on the VPN tunnel.

```
Router# show ip nat statistics

Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
 cable-modem0
Inside interfaces:
 Ethernet0
Hits: 1489 Misses: 1
Expired translations: 1
Dynamic mappings:
-- Inside Source
access-list 198 pool enterprise refcount 0
 pool enterprise: netmask 255.255.255.0
 start 192.168.1.90 end 192.168.1.90
 type generic, total addresses 1, allocated 0 (0%), misses 0\
```

If you are seeing IPSEC\_ACTIVE in your output at this point, everything is operating as expected.

---

## Configuring Save Password

To configure the Save Password feature, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **password encryption aes**
4. **crypto ipsec client ezvpn *name***
5. **username *name* password {0 | 6} {*password*}**
6. **exit**
7. **show running-config**

## DETAILED STEPS

|        | Command                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                     | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <b>password encryption aes</b><br><br><b>Example:</b><br>Router (config)# password encryption aes                                          | Enables a type 6 encrypted preshared key.                                                                                                                                                                                                                                                                                                               |
| Step 4 | <b>crypto ipsec client ezvpn name</b><br><br><b>Example:</b><br>Router (config)# crypto ipsec client ezvpn ezvpn1                          | Creates a Cisco Easy VPN remote configuration and enters the Cisco Easy VPN remote configuration mode.                                                                                                                                                                                                                                                  |
| Step 5 | <b>username name password {0   6} {password}</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# username server_1 password 0 blue | Allows you to save your Xauth password locally on the PC.<br><ul style="list-style-type: none"><li>The <b>0</b> keyword specifies that an unencrypted password will follow.</li><li>The <b>6</b> keyword specifies that an encrypted password will follow.</li><li>The <i>password</i> argument is the unencrypted (cleartext) user password.</li></ul> |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# exit                                                                   | Exits the Cisco Easy VPN remote configuration mode.                                                                                                                                                                                                                                                                                                     |
| Step 7 | <b>show running-config</b><br><br><b>Example:</b><br>Router (config)# show running-config                                                  | Displays the contents of the configuration file that is currently running.                                                                                                                                                                                                                                                                              |

## Configuring Manual Tunnel Control

To configure control of IPsec VPN tunnels manually so that you can establish and terminate the IPsec VPN tunnels on demand, perform the following steps.



### Note

CLI is one option for connecting the tunnel. The preferred method is via the web interface (using SDM).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn *name***
4. **connect [auto | manual]**
5. **exit**
6. **exit**
7. **crypto ipsec client ezvpn connect *name***

## DETAILED STEPS

|        | Command                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                         |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                       | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                               | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                               |
| Step 3 | <b>crypto ipsec client ezvpn <i>name</i></b><br><br><b>Example:</b><br>Router (config)# crypto ipsec client<br>ezvpn easy vpn remotel        | Assigns a Cisco Easy VPN remote configuration to an interface and enters Cisco Easy VPN Remote configuration mode.<br><ul style="list-style-type: none"> <li>The <i>name</i> argument specifies the configuration name to be assigned to the interface.</li> </ul>                                                                                                              |
| Step 4 | <b>connect [ auto   manual]</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# connect<br>manual                                    | Connects the VPN tunnel. Specify <b>manual</b> to configure manual tunnel control.<br><ul style="list-style-type: none"> <li>Automatic is the default; you do not need to use the <b>manual</b> keyword if your configuration is automatic.</li> </ul>                                                                                                                          |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# exit                                                                     | Exits Cisco Easy VPN Remote configuration mode.                                                                                                                                                                                                                                                                                                                                 |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router (config)# exit                                                                                  | Exits global configuration mode and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                                |
| Step 7 | <b>crypto ipsec client ezvpn connect <i>name</i></b><br><br><b>Example:</b><br>Router# crypto ipsec client ezvpn connect<br>easy vpn remotel | Connects a given Cisco Easy VPN remote configuration.<br><ul style="list-style-type: none"> <li>The <i>name</i> argument specifies the IPsec VPN tunnel name.</li> </ul> <b>Note</b> If the tunnel name is not specified, the active tunnel is connected. If there is more than one active tunnel, the command fails with an error requesting that you specify the tunnel name. |

## Configuring Automatic Tunnel Control

To configure automatic tunnel control, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **connect** [auto | manual]
5. **exit**
6. **exit**
7. **crypto ipsec client ezvpn connect** *name*

### DETAILED STEPS

|        | Command                                                                                                                               | Purpose                                                                                                                                                                                                                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                        | Enters global configuration mode.                                                                                                                                                                                                          |
| Step 3 | <b>crypto ipsec client ezvpn</b> <i>name</i><br><br><b>Example:</b><br>Router (config)# crypto ipsec client<br>ezvpn easy vpn remotel | Assigns a Cisco Easy VPN remote configuration to an interface and enters Cisco Easy VPN Remote configuration mode. <ul style="list-style-type: none"><li>• Specify the configuration name to be assigned to the interface.</li></ul>       |
| Step 4 | <b>connect</b> [auto   manual]<br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# connect<br>auto                                | Connects the VPN tunnel. <ul style="list-style-type: none"><li>• Specify <b>auto</b> to configure automatic tunnel control. Automatic is the default; you do not need to use this subcommand if your configuration is automatic.</li></ul> |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# exit                                                              | Exits Cisco Easy VPN Remote configuration mode.                                                                                                                                                                                            |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router (config)# exit                                                                           | Exits global configuration mode and enters privileged EXEC mode.                                                                                                                                                                           |

|               | Command                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 7</b> | <b>crypto ipsec client ezvpn connect</b> <i>name</i><br><br><b>Example:</b><br>Router# crypto ipsec client ezvpn connect<br>easy vpn remotel | Connects a given Cisco Easy VPN remote configuration. <ul style="list-style-type: none"> <li>The <i>name</i> argument specifies the IPsec VPN tunnel name.</li> </ul> <b>Note</b> If the tunnel name is not specified, the active tunnel is connected. If there is more than one active tunnel, the command fails with an error requesting that you specify the tunnel name. |

## Configuring Multiple Inside Interfaces

You can configure up to three inside interfaces for all platforms. You need to manually configure each inside interface using the following procedure.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-name*
4. **exit**
5. **crypto ipsec client ezvpn** *name* [outside | inside]
6. **interface** *interface-name*
7. **exit**
8. **crypto ipsec client ezvpn** *name* [outside | inside]

### DETAILED STEPS

|               | Command                                                                                               | Purpose                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>      |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                        | Enters global configuration mode.                                                                                     |
| <b>Step 3</b> | <b>interface</b> <i>interface-name</i><br><br><b>Example:</b><br>Router (config)# interface Ethernet0 | Selects the interface you want to configure by specifying the interface name and enters interface configuration mode. |
| <b>Step 4</b> | <b>exit</b><br><br><b>Example:</b><br>Router (config-if)# exit                                        | Exits interface configuration mode.                                                                                   |

|        | Command                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>crypto ipsec client ezvpn <i>name</i> [outside   inside]</b><br><br><b>Example:</b><br>Router (config)# crypto ipsec client ezvpn easy vpn remote 1 inside | Specifies the Cisco Easy VPN remote configuration name to be assigned to the first inside interface. <ul style="list-style-type: none"> <li>You must specify <b>inside</b> for each inside interface.</li> </ul>                                                                           |
| Step 6 | <b>interface <i>interface-name</i></b><br><br><b>Example:</b><br>Router (config)# interface Ethernet1                                                         | Selects the next interface you want to configure by specifying the next interface name and enters interface configuration mode.                                                                                                                                                            |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router (config-if)# exit                                                                                                | Exits interface configuration mode.                                                                                                                                                                                                                                                        |
| Step 8 | <b>crypto ipsec client ezvpn <i>name</i> [outside   inside]</b><br><br><b>Example:</b><br>Router (config)# crypto ipsec client ezvpn easy vpn remote2 inside  | Specifies the Cisco Easy VPN remote configuration name to be assigned to the next inside interface. <ul style="list-style-type: none"> <li>You must specify <b>inside</b> for each inside interface.</li> </ul> Repeat Step 3 through Step 4 to configure an additional tunnel if desired. |

## Configuring Multiple Outside Interfaces

You can configure multiple tunnels for outside interfaces, setting up a tunnel for each outside interface. You can configure a maximum of four tunnels using the following procedure for each outside interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *interface-name***
4. **exit**
5. **crypto ipsec client ezvpn *name* [outside | inside]**
6. **interface *interface-name***
7. **exit**
8. **crypto ipsec client ezvpn *name* [outside | inside]**

## DETAILED STEPS

|        | Command                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                      |
| Step 3 | <b>interface</b> <i>interface-name</i><br><br><b>Example:</b><br>Router (config)# interface Ethernet0                                                                         | Selects the first outside interface you want to configure by specifying the interface name and enters interface configuration mode.                                                                                                                                                                                                                                                                    |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router (config-if)# exit                                                                                                                | Exits interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                    |
| Step 5 | <b>crypto ipsec client ezvpn</b> <i>name</i> [ <b>outside</b>   <b>inside</b> ]<br><br><b>Example:</b><br>Router (config)# crypto ipsec client ezvpn easy vpn remotel outside | Specifies the Cisco Easy VPN remote configuration name to be assigned to the first outside interface. <ul style="list-style-type: none"><li>Specify <b>outside</b> (optional) for each outside interface. If neither <b>outside</b> nor <b>inside</b> is specified for the interface, the default is <b>outside</b>.</li></ul>                                                                         |
| Step 6 | <b>interface</b> <i>interface-name</i><br><br><b>Example:</b><br>Router (config)# interface Ethernet1                                                                         | Selects the next outside interface you want to configure by specifying the next interface name.                                                                                                                                                                                                                                                                                                        |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router (config-if)# exit                                                                                                                | Exits interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                    |
| Step 8 | <b>crypto ipsec client ezvpn</b> <i>name</i> [ <b>outside</b>   <b>inside</b> ]<br><br><b>Example:</b><br>Router (config)# crypto ipsec client ezvpn easy vpn remote2 outside | Specifies the Cisco Easy VPN remote configuration name to be assigned to the next outside interface. <ul style="list-style-type: none"><li>Specify <b>outside</b> (optional) for each outside interface. If neither <b>outside</b> nor <b>inside</b> is specified for the interface, the default is <b>outside</b>.</li></ul> Repeat Step 3 through Step 4 to configure additional tunnels if desired. |

## Configuring Multiple Subnet Support

When configuring multiple subnet support, you must first configure an access list to define the actual subnets to be protected. Each source subnet or mask pair indicates that all traffic that is sourced from this network to any destination is protected by IPsec. For information about configuring ACLs, see “Access control lists, configuring” in the section “[Additional References](#).”

After you have defined the subnets, you must configure the crypto IPsec client EZVPN profile to use the ACLs.

**Note**

Multiple subnets are not supported in client mode.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface** *interface-name*
4. **exit**
5. **crypto ipsec client ezvpn** *name*
6. **acl** {*acl-name* | *acl-number*}

**DETAILED STEPS**

|        | Command                                                                                                                  | Purpose                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                   | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                           | Enters global configuration mode.                                                                                     |
| Step 3 | <b>interface</b> <i>interface-name</i><br><br><b>Example:</b><br>Router (config)# interface Ethernet1                    | Selects the interface you want to configure by specifying the interface name and enters interface configuration mode. |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router (config-if)# exit                                                           | Exits interface configuration mode.                                                                                   |
| Step 5 | <b>crypto ipsec client ezvpn</b> <i>name</i><br><br><b>Example:</b><br>Router (config)# crypto ipsec client ezvpn ez1    | Creates a Cisco Easy VPN remote configuration and enters crypto Easy VPN configuration mode.                          |
| Step 6 | <b>acl</b> { <i>acl-name</i>   <i>acl-number</i> }<br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# acl acl-list1 | Specifies multiple subnets in a VPN tunnel.                                                                           |



## Configuring Proxy DNS Server Support

As a way of implementing the use of the DNS addresses of the ISP when the WAN connection is down, the router in a Cisco Easy VPN remote configuration can be configured to act as a proxy DNS server. To enable the proxy DNS server functionality with the **ip dns server** command, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dns server**

### DETAILED STEPS

|        | Command                                                                        | Purpose                                                                                                             |
|--------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                   |
| Step 3 | <b>ip dns server</b><br><br><b>Example:</b><br>Router (config)# ip dns server  | Enables the router to act as a proxy DNS server.<br><br><b>Note</b> This definition is IOS specific.                |

### What to Do Next

After configuring the router, you configure the Cisco IOS Easy VPN server as follows:

- Under the **crypto isakmp client configuration group** command, configure the *dns* subcommand as in the following example:

```
dns A.B.C.D A1.B1.C1.D1
```

These DNS server addresses should be pushed from the server to the Cisco Easy VPN remote and dynamically added to or deleted from the running configuration of the router.

For information about general DNS server functionality in Cisco IOS software applications, see [Configuring DNS](#) and [Configuring DNS on Cisco Routers](#).

## Configuring Dial Backup



### Note

The Dial Backup feature is not available in Cisco IOS Release 12.3(11)T.

To configure dial backup, perform the following steps.

## SUMMARY STEPS

1. Create the Easy VPN backup configuration.
2. Add the backup subcommand details to the primary configuration.
3. Apply the backup Easy VPN configuration to the dial backup outside interface.
4. Apply the Easy VPN profile to the inside interfaces.

## DETAILED STEPS

|               | Command                                                                                                               | Purpose                                                                                                                                                                |
|---------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Create the Easy VPN dial backup configuration.                                                                        | For details about the backup configuration, see the section “ <a href="#">Dial Backup</a> .”                                                                           |
| <b>Step 2</b> | Add the backup subcommand details to the primary configuration.                                                       | Use the <b>backup</b> subcommand and <b>track</b> keyword of the <b>crypto ipsec client ezvpn</b> command.                                                             |
| <b>Step 3</b> | Apply the backup Easy VPN configuration to the dial backup outside interface (for example, serial, async, or dialer). | For details about applying the backup configuration to the dial backup outside interface, see the section “ <a href="#">Configuring Multiple Outside Interfaces</a> .” |
| <b>Step 4</b> | Apply the Easy VPN profile to the inside interfaces (there can be more than one).                                     | For details about applying the Easy VPN profile to the inside interfaces, see the section “ <a href="#">Configuring Multiple Inside Interfaces</a> .”                  |

## Configuring the DHCP Server Pool

To configure the Dynamic Host Configuration Protocol (DHCP) server pool, see the chapter “[Configuring DHCP](#)” in the *Cisco IOS IP Configuration Guide*, Release 12.3.

## Resetting a VPN Connection

To reset the VPN connection, perform the following steps. The **clear** commands can be configured in any order or independent of one another.

## SUMMARY STEPS

1. **enable**
2. **clear crypto ipsec client ezvpn**
3. **clear crypto sa**
4. **clear crypto isakmp**

## DETAILED STEPS

|        | Command                                                                                                  | Purpose                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                        |
| Step 2 | <b>clear crypto ipsec client ezvpn</b><br><br><b>Example:</b><br>Router# clear crypto ipsec client ezvpn | Resets the Cisco Easy VPN remote state machine and brings down the Cisco Easy VPN remote connection on all interfaces or on a given interface (tunnel). |
| Step 3 | <b>clear crypto sa</b><br><br><b>Example:</b><br>Router# clear crypto sa                                 | Deletes IPsec SAs.                                                                                                                                      |
| Step 4 | <b>clear crypto isakmp</b><br><br><b>Example:</b><br>Router# clear crypto isakmp                         | Clears active IKE connections.                                                                                                                          |

## Monitoring and Maintaining VPN and IKE Events

To monitor and maintain VPN and IKE events, perform the following steps.

### SUMMARY STEPS

1. enable
2. debug crypto ipsec client ezvpn
3. debug crypto ipsec
4. debug crypto isakmp

### SUMMARY STEPS

|        | Command                                                                                                  | Purpose                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>debug crypto ipsec client ezvpn</b><br><br><b>Example:</b><br>Router# debug crypto ipsec client ezvpn | Displays information showing the configuration and implementation of the Cisco Easy VPN Remote feature.          |

|        | Command                                                                          | Purpose                             |
|--------|----------------------------------------------------------------------------------|-------------------------------------|
| Step 3 | <b>debug crypto ipsec</b><br><br><b>Example:</b><br>Router# debug crypto ipsec   | Displays IPsec events.              |
| Step 4 | <b>debug crypto isakmp</b><br><br><b>Example:</b><br>Router# debug crypto isakmp | Displays messages about IKE events. |

## Configuring a Virtual Interface

To configure a virtual interface, perform the following steps.



### Note

Before the virtual interface is configured, ensure that the Easy VPN profile is not applied on any outside interface. Remove the Easy VPN profile from the outside interface and then configure the virtual interface.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number* **type** *type-of-virtual-template*
4. **tunnel mode ipsec ipv4**
5. **exit**
6. **crypto ipsec client ezvpn** *name*
7. **virtual-interface** *virtual-template-number*

## DETAILED STEPS

|        | Command                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                 | Enters global configuration mode.                                                                                                                                                                                                            |
| Step 3 | <b>interface virtual-template</b> <i>number</i> <b>type</b> <i>type-of-virtual-template</i><br><br><b>Example:</b><br>Router (config)# interface virtual-template1 type tunnel | (Optional) Creates a virtual template of the type tunnel and enters interface configuration mode. <ul style="list-style-type: none"> <li>• Steps 3, 4, and 5 are optional, but if one is configured, they must all be configured.</li> </ul> |

|        | Command                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>tunnel mode ipsec ipv4</b><br><br><b>Example:</b><br>Router (if-config)# tunnel mode ipsec<br>ipv4                           | (Optional) Configures the tunnel that does the IPsec tunneling.                                                                                                                                                                                                                                                                   |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router (if-config)# exit                                                                  | (Optional) Exits interface (virtual-tunnel) configuration mode.                                                                                                                                                                                                                                                                   |
| Step 6 | <b>crypto ipsec client ezvpn name</b><br><br><b>Example:</b><br>Router (config)# crypto ipsec client<br>ezvpn EasyVPN1          | Creates a Cisco Easy VPN remote configuration and enters the Cisco Easy VPN remote configuration mode.                                                                                                                                                                                                                            |
| Step 7 | <b>virtual-interface virtual-template-number</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)#<br>virtual-interface 3 | Instructs the Easy VPN remote to create a virtual interface to be used as an outside interface. If the virtual template number is specified, the virtual-access interface is derived from the virtual interface that was specified. If a virtual template number is not specified, a generic virtual-access interface is created. |

## Troubleshooting Dual Tunnel Support

The following **debug** and **show** commands may be used to troubleshoot your dual-tunnel configuration.

### SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec client ezvpn**
3. **debug ip policy**
4. **show crypto ipsec client ezvpn**
5. **show ip interface**

### DETAILED STEPS

|        | Command                                                                                                  | Purpose                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                   | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>debug crypto ipsec client ezvpn</b><br><br><b>Example:</b><br>Router# debug crypto ipsec client ezvpn | Displays information about Cisco Easy VPN remote connections.                                                         |

|        | Command                                                                                                | Purpose                                                                 |
|--------|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Step 3 | <b>debug ip policy</b><br><br><b>Example:</b><br>Router# debug ip policy                               | Displays IP policy routing packet activity.                             |
| Step 4 | <b>show crypto ipsec client ezvpn</b><br><br><b>Example:</b><br>Router# show crypto ipsec client ezvpn | Displays the Cisco Easy VPN Remote configuration.                       |
| Step 5 | <b>show ip interface</b><br><br><b>Example:</b><br>Router# show ip interface                           | Displays the usability status of interfaces that are configured for IP. |

## Configuring Reactivate (a Default) Primary Peer

To configure a default primary peer, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **peer** {*ip-address* | *hostname*} [**default**]
5. **idle-time** *idle-time*

### DETAILED STEPS

|        | Command                                                                                                               | Purpose                                                                                                            |
|--------|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                        | Enters global configuration mode.                                                                                  |
| Step 3 | <b>crypto ipsec client ezvpn</b> <i>name</i><br><br><b>Example:</b><br>Router (config)# crypto ipsec client ezvpn ez1 | Creates a Cisco Easy VPN remote configuration and enters crypto Easy VPN configuration mode.                       |

|        | Command                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>peer</b> { <i>ip-address</i>   <i>hostname</i> } [ <b>default</b> ]<br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# peer<br>10.2.2.2 default | Sets the peer IP address or hostname for the VPN connection. <ul style="list-style-type: none"> <li>A hostname can be specified only when the router has a DNS server available for hostname resolution.</li> <li>The peer subcommand may be input multiple times. However, only one default or primary peer entry can exist at a time (for example, 10.2.2.2 default).</li> <li>The <b>default</b> keyword defines the peer as the primary peer.</li> </ul> |
| Step 5 | <b>idle-time</b> <i>idle-time</i><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# idle-time<br>60                                               | (Optional) Idle time in seconds after which an Easy VPN tunnel is brought down. <ul style="list-style-type: none"> <li>Idle time=60 through 86400 seconds.</li> </ul> <b>Note</b> If idle time is configured, the tunnel for the primary server is not brought down.                                                                                                                                                                                         |

## Configuring Identical Addressing Support

Configuring Identical Addressing Support comprises the following tasks:

- Defining the Easy VPN remote in network-extension mode and enabling **nat allow**.
- Assigning the Cisco Easy VPN Remote configuration to the Outside interface.
- Creating a loopback interface and assigning the Cisco Easy VPN Remote configuration to the Inside interface of the loopback interface.
- Configuring a one-to-one static NAT translation for each host that needs to be accessible from the EasyVPN server-side network or from other client locations.
- Configuring dynamic overloaded NAT or PAT using an access list for all the desired VPN traffic. The NAT or PAT traffic is mapped to the Easy VPN inside interface IP address.
- And, if split-tunneling is required, using the **nat acl** command to enable split-tunneling for the traffic specified by the *acl-name* or the *acl-number* argument. The ACL is the same as the ACL used by the NAT or PAT mapping in the preceding bullet item.

To configure Identical Addressing Support, perform the following steps on your router.

### Prerequisites

Easy VPN Remote must be configured in network extension mode before you can configure the Identical Addressing Support feature.

### SUMMARY STEPS

- enable**
- configure terminal**
- crypto ipsec client ezvpn** *name*
- mode network-extension**
- nat allow**
- exit**
- interface** *interface*

8. **crypto ipsec client ezvpn name** *outside*
9. **exit**
10. **interface** *interface*
11. **ip address** *ip mask*
12. **crypto ipsec client ezvpn name** *inside*
13. **exit**
14. **ip nat inside source static** *local-ip global-ip*
15. **ip nat inside source list** {*acl-name* | *acl-number*} **interface** *interface* **overload**
16. **crypto ipsec client ezvpn name**
17. **nat acl** {*acl-name* | *acl-number*}
18. **exit**
19. **exit**

## DETAILED STEPS

|        | Command                                                                                                                  | Purpose                                                                                                             |
|--------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                   | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                           | Enters global configuration mode.                                                                                   |
| Step 3 | <b>crypto ipsec client ezvpn name</b><br><br><b>Example:</b><br>Router (config)# crypto ipsec client<br>ezvpn easyclient | Creates a remote configuration and enters Cisco Easy VPN Remote configuration mode.                                 |
| Step 4 | <b>mode network-extension</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# mode<br>network-extension          | Configures Easy VPN client in network-extension mode.                                                               |
| Step 5 | <b>nat allow</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# nat allow                                       | Allows NAT to be integrated with Easy VPN and enables the Identical Addressing feature.                             |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# exit                                                 | Exits Cisco Easy VPN Remote configuration mode.                                                                     |



|         | Command                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                          |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <b>interface</b> <i>interface</i><br><br><b>Example:</b><br>Router (config)# interface Ethernet1                                                                                                                        | Enters interface configuration mode for the interface. <ul style="list-style-type: none"><li>This interface will become the outside interface for the NAT or PAT translation.</li></ul>                                                                                                                                                          |
| Step 8  | <b>crypto ipsec client ezvpn name outside</b><br><br><b>Example:</b><br>Router (config-if)# crypto ipsec client ezvpn easyclient outside                                                                                | Assigns the Cisco Easy VPN Remote configuration to the outside interface. <ul style="list-style-type: none"><li>This configuration automatically creates the necessary NAT or PAT translation parameters and initiates the VPN connection (if you are in client mode).</li></ul>                                                                 |
| Step 9  | <b>exit</b><br><br><b>Example:</b><br>Router (config-if)# exit                                                                                                                                                          | Exits interface configuration mode.                                                                                                                                                                                                                                                                                                              |
| Step 10 | <b>interface</b> <i>interface</i><br><br><b>Example:</b><br>Router (config)# interface Loopback0                                                                                                                        | Enters interface configuration mode for the loopback interface. <ul style="list-style-type: none"><li>This interface will become the inside interface for the NAT or PAT translation.</li></ul>                                                                                                                                                  |
| Step 11 | <b>ip address</b> <i>ip mask</i><br><br><b>Example:</b><br>Router (config-if)# ip address 10.1.1.1 255.255.255.252                                                                                                      | Assigns the IP address and mask to the loopback interface.                                                                                                                                                                                                                                                                                       |
| Step 12 | <b>crypto ipsec client ezvpn name inside</b><br><br><b>Example:</b><br>Router (config-if)# crypto ipsec client ezvpn easyclient inside                                                                                  | Assigns the Cisco Easy VPN Remote configuration to the inside interface.                                                                                                                                                                                                                                                                         |
| Step 13 | <b>exit</b><br><br><b>Example:</b><br>Router (config-if)# exit                                                                                                                                                          | Exits interface configuration mode.                                                                                                                                                                                                                                                                                                              |
| Step 14 | <b>ip nat inside source static</b> <i>local-ip global-ip</i><br><br><b>Example:</b><br>Router (config)# ip nat inside source static 10.10.10.10 5.5.5.5                                                                 | Configure a one-to-one static NAT translation for each host that needs to be accessible from the Easy VPN server side network, or from other client locations.                                                                                                                                                                                   |
| Step 15 | <b>ip nat inside source list</b> <i>{acl-name   acl-number}</i> <b>interface</b> <i>interface</i> <b>overload</b><br><br><b>Example:</b><br>Router (config)# ip nat inside source list 100 interface Loopback0 overload | Configure dynamic overloaded NAT or PAT, which uses an ACL for all the desired VPN traffic. The NAT and PAT traffic is mapped to the Easy VPN inside interface IP address. <ul style="list-style-type: none"><li>The <i>acl-name</i> argument is the name of the ACL.</li><li>The <i>acl-number</i> argument is the number of the ACL.</li></ul> |

|         | Command                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 16 | <b>crypto ipsec client ezvpn</b> <i>name</i><br><br><b>Example:</b><br>Router (config)# crypto ipsec client<br>ezvpn easyclient | (Optional, if using split tunneling) Enters Cisco Easy VPN Remote configuration mode.                                                                                                                                                                                                                                                                                                                    |
| Step 17 | <b>nat acl</b> { <i>acl-name</i>   <i>acl-number</i> }<br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# nat acl 100      | (Optional, if using split tunneling) Enables split-tunneling for the traffic specified by the <i>acl-name</i> or the <i>acl-number</i> argument. The ACL is the same as the ACL used by the NAT or PAT mapping in the Step 15. <ul style="list-style-type: none"><li>• The <i>acl-name</i> argument is the name of the ACL.</li><li>• The <i>acl-number</i> argument is the number of the ACL.</li></ul> |
| Step 18 | <b>exit</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# exit                                                        | Exits Cisco Easy VPN Remote configuration mode.                                                                                                                                                                                                                                                                                                                                                          |
| Step 19 | <b>exit</b><br><br><b>Example:</b><br>Router (config)# exit                                                                     | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                                                         |

## Configuring cTCP on an Easy VPN Client

To configure cTCP on an Easy VPN client (remote device), perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ctcp** [*keepalive number-of-seconds* | **port** *port-number*]
4. **crypto ipsec client ezvpn** *name*
5. **ctcp port** *port-number*

### DETAILED STEPS

|        | Command                                                                        | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                |

|               | Command                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <b>crypto ctcp</b> [ <b>keepalive</b> <i>number-of-seconds</i>   <b>port</b> <i>port-number</i> ]<br><br><b>Example:</b><br>Router (config)# crypto ctcp keepalive 15 | Sets cTCP keepalive interval for the remote device. <ul style="list-style-type: none"> <li><i>number-of-seconds</i>—Number of seconds between keepalives. Value = 5 through 3600.</li> <li><b>port</b> <i>port-number</i>—Port number that cTCP listens to. Up to 10 numbers can be configured.</li> </ul> <b>Note</b> The cTCP client has to send periodic keepalives to the server to keep NAT or firewall sessions alive. |
| <b>Step 4</b> | <b>crypto ipsec client ezvpn</b> <i>name</i><br><br><b>Example:</b><br>Router (config)# crypto ipsec client ezvpn ezvpn1                                              | Creates a Cisco Easy VPN remote configuration and enters Cisco Easy VPN remote configuration mode.                                                                                                                                                                                                                                                                                                                           |
| <b>Step 5</b> | <b>ctcp port</b> <i>port-number</i><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# ctcp port 200                                                             | Sets the port number for cTCP encapsulation for Easy VPN. <ul style="list-style-type: none"> <li><i>port-number</i>—Port number on the hub. Value = 1 through 65535.</li> </ul>                                                                                                                                                                                                                                              |

## Restricting Traffic When a Tunnel Is Down

To restrict the client from sending traffic in clear text when a tunnel is down, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **flow allow acl** [*name* | *number*]

### DETAILED STEPS

|               | Command                                                                        | Purpose                                                                                                          |
|---------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                |

|        | Command                                                                                                                          | Purpose                                                                                                                                                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>crypto ipsec client ezvpn <i>name</i></b><br><br><b>Example:</b><br>Router (config)# crypto ipsec client<br>ezvpn ezvpn1      | Creates a Cisco Easy VPN remote configuration and enters Cisco Easy VPN remote configuration mode.                                                                                                                                     |
| Step 4 | <b>flow allow acl [<i>name</i>   <i>number</i>]</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)#flow allow<br>acl 102 | Restricts the client from sending traffic in clear text when the tunnel is down. <ul style="list-style-type: none"> <li><i>name</i>— Access list name.</li> <li><i>number</i>— Access list number. Value = 100 through 199.</li> </ul> |

## Easy VPN Server Tasks

### Configuring a Cisco IOS Easy VPN Server

For information about configuring the Easy VPN Server, see the following document:

- [Easy VPN Server](#)

### Configuring an Easy VPN Server on a VPN 3000 Series Concentrator

This section describes the guidelines required to configure the Cisco VPN 3000 series concentrator for use with the Cisco Easy VPN Remote feature. As a general rule, you can use the default configuration except for IP addresses, server addresses, routing configurations, and for the following parameters and options:

- [Peer Configuration on a Cisco Easy VPN Remote Using the Hostname](#), page 59
- [Interactive Hardware Client Authentication Version 3.5](#), page 59
- [IPsec Tunnel Protocol](#), page 59
- [IPsec Group](#), page 59
- [Group Lock](#), page 59
- [Xauth](#), page 59
- [Split Tunneling](#), page 60
- [IKE Proposals](#), page 60
- [New IPsec SA](#), page 60



#### Note

You must be using Cisco VPN 3000 series concentrator software Release 3.11 or later to support Cisco Easy VPN software clients and remotes.

## Peer Configuration on a Cisco Easy VPN Remote Using the Hostname

After you have configured the Cisco Easy VPN server on the VPN 3000 concentrator to use hostname as its identity, you must configure the peer on the Cisco Easy VPN remote using the hostname. You can either configure DNS on the client to resolve the peer hostname or configure the peer hostname locally on the client using the **ip host** command. As an example, you can configure the peer hostname locally on an Easy VPN remote as follows:

```
ip host crypto-gw.cisco.com 10.0.0.1
```

Or you can configure the Easy VPN remote to use the hostname with the **peer** command and *hostname* argument, as follows:

```
peer crypto-gw.cisco.com.
```

## Interactive Hardware Client Authentication Version 3.5

The Cisco Easy VPN Remote feature does not support the Interactive Hardware Client Authentication Version 3.5 feature. This feature must be disabled. You can disable the feature on the VPN 3000 series concentrator by clicking the **HW Client** tab on the **Configuration | User Management | Base Group** screen.

## IPsec Tunnel Protocol

IPsec Tunnel Protocol enables the IPsec tunnel protocol so that it is available for users. The IPsec Tunnel Protocol is configured on the Cisco VPN 3000 series concentrator by clicking the **General** tab on the **Configuration | User Management | Base Group** screen.

## IPsec Group

IPsec group configures the Cisco VPN 3000 series concentrator with a group name and password that match the values configured for the Cisco Easy VPN remote configuration on the router. These values are configured on the router with the **group group-name key group-key** subcommand and arguments. The values are configured on the Cisco VPN 3000 series concentrator using the **Configuration | User Management | Groups** screen.

## Group Lock

If you are defining multiple users in multiple groups on the VPN 3000 series concentrator, you must check the **Group Lock** box in the IPsec tab to prevent users in one group from logging in with the parameters of another group. For example, if you have configured one group for split tunneling access and another group without split tunneling access, clicking the **Group Lock** box prevents users in the second group from gaining access to the split tunneling features. The Group Lock checkbox appears in the **IPsec** tab in the **Configuration | User Management | Base Group** screen and in the **IPsec** tab in the **Configuration | User Management | Groups | Add/Modify** screens.

## Xauth

To use Xauth, set the **Authentication** parameter to **None**. The Authentication parameter appears in the **IPsec** tab in the **Configuration | User Management | Base Group** screen and in the **IPsec** tab in the **Configuration | User Management | Groups | Add/Modify** screens.

## Split Tunneling

The **Configuration | User Management | Base Group, Mode Configuration Parameters Tab** screen includes a **Split Tunnel** option with a checkbox that says “Allow the networks in the list to bypass the tunnel.”

## IKE Proposals

The Cisco VPN 3000 series concentrator is preconfigured with a default IKE proposal, CiscoVPNClient-3DES-MD5, that can be used with Cisco Easy VPN remotes. This IKE proposal supports preshared keys with Xauth using the MD5/HMAC-128 algorithm and Diffie-Hellman Group 2.

This IKE proposal is active by default, but you should verify that it is still an active proposal using the **Configuration | System | Tunneling Protocols | IPsec | IKE Proposals** screen.

In addition, as part of configuring the Cisco VPN 3000 series concentrator—for the Cisco Easy VPN Remote image, you do not need to create a new IPsec SA. Use the default IKE and Easy VPN remote lifetime configured on the Cisco VPN 3000 series concentrator.



### Note

You can also use the default IKE proposals IKE-DES-MD5 and IKE-3DES-MD5, but they do not enable Xauth support by default.

## New IPsec SA

You can create a new IPsec SA. Cisco Easy VPN clients use a SA having the following parameters:

- Authentication Algorithm=ESP/MD5/HMAC-128
- Encryption Algorithm=DES-56 or 3DES-168 (recommended)
- Encapsulation Mode=Tunnel
- IKE Proposal=CiscoVPNClient-3DES-MD5 (preferred)

The Cisco VPN 3000 series concentrator is preconfigured with several default security associations (SAs), but they do not meet the IKE proposal requirements. To use an IKE proposal of CiscoVPNClient-3DES-MD5, copy the ESP/IKE-3DES-MD5 SA and modify it to use CiscoVPNClient-3DES-MD5 as its IKE proposal. An IKE proposal is configured on the VPN 3000 series concentrator using the **Configuration | Policy Management | Traffic Management | Security Associations** screen.

## Configuring an Easy VPN Server on a Cisco PIX Firewall

For information about configuring an Easy VPN Server on a Cisco PIX Firewall, see the following document:

- [Easy VPN Server](#)

## Web Interface Tasks

### Configuring Web-Based Activation

To configure a LAN so that any HTTP requests coming from any of the PCs on the private LAN are intercepted, providing corporate users with access to the corporate Web page, perform the following steps.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn *name***
4. **xauth userid mode {http-intercept | interactive | local}**

#### DETAILED STEPS

|        | Command                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                              | Enters global configuration mode.                                                                                                                                                                                                                                  |
| Step 3 | <b>crypto ipsec client ezvpn <i>name</i></b><br><br><b>Example:</b><br>Router (config)# crypto ipsec client<br>ezvpn easy vpn remotel                       | Assigns a Cisco Easy VPN remote configuration to an interface and enters Cisco Easy VPN Remote configuration mode.<br><ul style="list-style-type: none"><li>• The <i>name</i> argument specifies the configuration name to be assigned to the interface.</li></ul> |
| Step 4 | <b>xauth userid mode {http-intercept   interactive   local}</b><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# xauth<br>userid mode http-intercept | Specifies how the VPN device handles Xauth requests or prompts from the server.                                                                                                                                                                                    |

### Monitoring and Maintaining Web-Based Activation

To monitor and maintain web-based activation, perform the following steps. (The **debug** and **show** commands may be used independently, or they may all be configured.)

#### SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec client ezvpn**

3. **debug ip auth-proxy ezvpn**
4. **show crypto ipsec client ezvpn**
5. **show ip auth-proxy config**

## DETAILED STEPS

|        | Command                                                                                                  | Purpose                                                                                                                                                   |
|--------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                   | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                       |
| Step 2 | <b>debug crypto ipsec client ezvpn</b><br><br><b>Example:</b><br>Router# debug crypto ipsec client ezvpn | Displays information about the Cisco Easy VPN connection.                                                                                                 |
| Step 3 | <b>debug ip auth-proxy ezvpn</b><br><br><b>Example:</b><br>Router# debug ip auth-proxy ezvpn             | Displays information related to proxy authentication behavior for web-based activation.                                                                   |
| Step 4 | <b>show crypto ipsec client ezvpn</b><br><br><b>Example:</b><br>Router# show crypto ipsec client ezvpn   | Shows that the username and password used for user credentials during Xauth negotiations will be obtained by intercepting HTTP connections from the user. |
| Step 5 | <b>show ip auth-proxy config</b><br><br><b>Example:</b><br>Router# show ip auth-proxy config             | Displays the auth-proxy rule that has been created and applied by Easy VPN.                                                                               |

## Examples

### Debug Output

The following is sample **debug** output for a typical situation in which a user has opened a browser and connected to the corporate website:

Router# **debug ip auth-proxy ezvpn**

```
Dec 10 12:41:13.335: AUTH-PROXY: New request received by EzVPN WebIntercept
! The following line shows the ip address of the user.
from 10.4.205.205
Dec 10 12:41:13.335: AUTH-PROXY:GET request received
Dec 10 12:41:13.335: AUTH-PROXY:Normal auth scheme in operation
Dec 10 12:41:13.335: AUTH-PROXY:Ezvpn is NOT active. Sending connect-bypass page to user
```

At this point, the user chooses “connect” on his or her browser:

```
Dec 10 12:42:43.427: AUTH-PROXY: New request received by EzVPN WebIntercept
from 10.4.205.205
Dec 10 12:42:43.427: AUTH-PROXY:POST request received
Dec 10 12:42:43.639: AUTH-PROXY:Found attribute <connect> in form
Dec 10 12:42:43.639: AUTH-PROXY:Sending POST data to EzVPN
Dec 10 12:42:43.639: EZVPN(tunnel22): Communication from Interceptor
application.
```



```
Request/Response from 10.4.205.205, via Ethernet0
Dec 10 12:42:43.639: connect: Connect Now
Dec 10 12:42:43.639: EZVPN(tunnel22): Received CONNECT from 10.4.205.205!
Dec 10 12:42:43.643: EZVPN(tunnel22): Current State: CONNECT_REQUIRED
Dec 10 12:42:43.643: EZVPN(tunnel22): Event: CONNECT
Dec 10 12:42:43.643: EZVPN(tunnel22): ezvpn_connect_request
```

#### Easy VPN contacts the server:

```
Dec 10 12:42:43.643: EZVPN(tunnel22): Found valid peer 192.168.0.1
Dec 10 12:42:43.643: EZVPN(tunnel22): Added PSK for address 192.168.0.1

Dec 10 12:42:43.643: EZVPN(tunnel22): New State: READY
Dec 10 12:42:44.815: EZVPN(tunnel22): Current State: READY
Dec 10 12:42:44.815: EZVPN(tunnel22): Event: IKE_PFS
Dec 10 12:42:44.815: EZVPN(tunnel22): No state change
Dec 10 12:42:44.819: EZVPN(tunnel22): Current State: READY
Dec 10 12:42:44.819: EZVPN(tunnel22): Event: CONN_UP
Dec 10 12:42:44.819: EZVPN(tunnel22): ezvpn_conn_up B8E86EC7 E88A8A18 D0D51422
8AFF32B7
```

#### The server requests Xauth information:

```
Dec 10 12:42:44.823: EZVPN(tunnel22): No state change
Dec 10 12:42:44.827: EZVPN(tunnel22): Current State: READY
Dec 10 12:42:44.831: EZVPN(tunnel22): Event: XAUTH_REQUEST
Dec 10 12:42:44.831: EZVPN(tunnel22): ezvpn_xauth_request
Dec 10 12:42:44.831: EZVPN(tunnel22): ezvpn_parse_xauth_msg
Dec 10 12:42:44.831: EZVPN: Attributes sent in xauth request message:
Dec 10 12:42:44.831: XAUTH_TYPE_V2(tunnel22): 0
Dec 10 12:42:44.831: XAUTH_USER_NAME_V2(tunnel22):
Dec 10 12:42:44.831: XAUTH_USER_PASSWORD_V2(tunnel22):
Dec 10 12:42:44.831: XAUTH_MESSAGE_V2(tunnel22) <Enter Username and
Password.>
Dec 10 12:42:44.831: EZVPN(tunnel22): Requesting following info for xauth
Dec 10 12:42:44.831: username:(Null)
Dec 10 12:42:44.835: password:(Null)
Dec 10 12:42:44.835: message:Enter Username and Password.
Dec 10 12:42:44.835: EZVPN(tunnel22): New State: XAUTH_REQ
```

#### The username and password prompt are displayed in the browser of the user:

```
Dec 10 12:42:44.835: AUTH-PROXY: Response to POST is CONTINUE
Dec 10 12:42:44.839: AUTH-PROXY: Displayed POST response successfully
Dec 10 12:42:44.843: AUTH-PROXY:Served POST response to the user
```

#### When the user enters his or her username and password, the following is sent to the server:

```
Dec 10 12:42:55.343: AUTH-PROXY: New request received by EzVPN WebIntercept
from 10.4.205.205
Dec 10 12:42:55.347: AUTH-PROXY:POST request received
Dec 10 12:42:55.559: AUTH-PROXY:No of POST parameters is 3
Dec 10 12:42:55.559: AUTH-PROXY:Found attribute <username> in form
Dec 10 12:42:55.559: AUTH-PROXY:Found attribute <password> in form
Dec 10 12:42:55.559: AUTH-PROXY:Found attribute <ok> in form
Dec 10 12:42:55.563: AUTH-PROXY:Sending POST data to EzVPN
Dec 10 12:42:55.563: EZVPN(tunnel22): Communication from Interceptor application.
Request/Response from 10.4.205.205, via Ethernet0
Dec 10 12:42:55.563: username:http
Dec 10 12:42:55.563: password:<omitted>
Dec 10 12:42:55.563: ok:Continue
Dec 10 12:42:55.563: EZVPN(tunnel22): Received username|password from 10.4.205.205!
Dec 10 12:42:55.567: EZVPN(tunnel22): Current State: XAUTH_PROMPT
Dec 10 12:42:55.567: EZVPN(tunnel22): Event: XAUTH_REQ_INFO_READY
Dec 10 12:42:55.567: EZVPN(tunnel22): ezvpn_xauth_reply
```

```

Dec 10 12:42:55.567: XAUTH_TYPE_V2(tunnel22): 0
Dec 10 12:42:55.567: XAUTH_USER_NAME_V2(tunnel22): http
Dec 10 12:42:55.567: XAUTH_USER_PASSWORD_V2(tunnel22): <omitted>
Dec 10 12:42:55.567: EZVPN(tunnel22): New State: XAUTH_REPLIED
Dec 10 12:42:55.891: EZVPN(tunnel22): Current State: XAUTH_REPLIED
Dec 10 12:42:55.891: EZVPN(tunnel22): Event: XAUTH_STATUS
Dec 10 12:42:55.891: EZVPN(tunnel22): xauth status received: Success

```

After using the tunnel, the user chooses “Disconnect”:

```

Dec 10 12:48:17.267: EZVPN(tunnel22): Received authentic disconnect credential
Dec 10 12:48:17.275: EZVPN(): Received an HTTP request: disconnect
Dec 10 12:48:17.275: %CRYPTO-6-EZVPN_CONNECTION_DOWN: (Client) User=
 Group=tunnel22 Client_public_addr=192.168.0.13 Server_public_addr=192.168.0.1
 Assigned_client_addr=10.3.4.5

```

### Show Output Before the User Is Connected to the Tunnel

The following output from the two **show** commands (**show crypto ipsec client ezvpn** and **show ip auth-proxy config**) displays what you might see before a user is connected to a VPN tunnel:

Router# **show crypto ipsec client ezvpn tunnel22**

```

Tunnel name : tunnel22
Inside interface list: Ethernet0
Outside interface: Ethernet1
Current State: CONNECT_REQUIRED
Last Event: RESET
Save Password: Disallowed
! Note the next line.
 XAuth credentials: HTTP intercepted
 HTTP return code : 200
 IP addr being prompted: 0.0.0.0
Current EzVPN Peer: 192.168.0.1

```

Router# **show ip auth-proxy config**

```

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
! Note that the next line is the Easy VPN-defined internal rule.
 Auth-proxy name ezvpn401***
 Applied on Ethernet0
 http list not specified inactivity-timer 60 minutes

```

### Show Output After the User Is Connected to the Tunnel

The following output from the two **show** commands (**show crypto ipsec client ezvpn** and **show ip auth-proxy config**) displays what you might see after the user has been connected to the tunnel:

Router# **show crypto ipsec client ezvpn tunnel22**

```

Tunnel name : tunnel22
Inside interface list: Ethernet0
Outside interface: Ethernet1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.3.4.5
Mask: 255.255.255.255
Save Password: Disallowed
 XAuth credentials: HTTP intercepted
 HTTP return code : 200
 IP addr being prompted: 192.168.0.0

```

```
Current EzVPN Peer: 192.168.0.1

Router# show ip auth-proxy config

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Auth-proxy name ezvpnWeb*** (EzVPN-defined internal rule)
http list not specified inactivity-timer 60 minutes
```

## Using SDM As a Web Manager

For information about the SDM web manager, see the following document:

- [Cisco Security Device Manager](#)

## Troubleshooting the VPN Connection

### Troubleshooting a VPN Connection Using the Cisco Easy VPN Remote Feature

To troubleshoot a VPN connection created using the Cisco Easy VPN Remote feature, use the following suggested techniques.

- Be aware that any changes to an active Cisco Easy VPN remote configuration or IP address changes to the involved interfaces, such as adding or removing an inside interface, result in a reset of the Cisco Easy VPN Remote connection.
- Enable debugging of the Cisco Easy VPN Remote feature using the **debug crypto ipsec client ezvpn** command.
- Enable debugging of IKE events using the **debug crypto ipsec** and **debug crypto isakmp** commands.
- Display the active IPsec VPN connections using the **show crypto engine connections active** command.
- To reset the VPN connection, use the **clear crypto ipsec client ezvpn** command. If you have debugging enabled, you might prefer to use the **clear crypto sa** and **clear crypto isakmp** commands.

## Troubleshooting the Client Mode of Operation

The following information may be used to troubleshoot the Easy VPN Remote configuration for the client mode of operation.

In client mode, the Cisco Easy VPN Remote feature automatically configures the NAT or PAT translation and access lists that are needed to implement the VPN tunnel. These configurations are automatically created when the IPsec VPN connection is initiated. When the tunnel is torn down, the NAT or PAT and access list configurations are automatically deleted.

The NAT or PAT configuration is created with the following assumptions:

- The **ip nat inside** command is applied to all inside interfaces, including default inside interfaces. The default inside interface is the Ethernet 0 interface (for the Cisco 806, Cisco 826, Cisco 827, Cisco 828, Cisco 831, Cisco 836, and Cisco 837 routers).

- The **ip nat outside** command is applied to the interface that is configured with the Cisco Easy VPN Remote configuration. On the Cisco 800 series and Cisco 1700 series routers, the outside interface is configured with the Cisco Easy VPN Remote configuration. On the Cisco 1700 series routers, Cisco 2600 series routers, Cisco 3600 series routers, and Cisco 3700 series routers, multiple outside interfaces can be configured.

**Tip**

The NAT or PAT translation and access list configurations that are created by the Cisco Easy VPN Remote feature are not written to either the startup configuration or running configuration files. These configurations, however, can be displayed using the **show ip nat statistics** and **show access-list** commands.

## Troubleshooting Remote Management

To troubleshoot remote management of the VPN remote, use the **show ip interface** command. Using the **brief** keyword, you can verify that the loopback has been removed and that the interface is shown correctly.

### Examples

Following is a typical example of output from the **show ip interface** command.

```
Router# show ip interface brief
```

| Interface | IP-Address  | OK? | Method | Status                | Protocol |
|-----------|-------------|-----|--------|-----------------------|----------|
| Ethernet0 | unassigned  | YES | NVRAM  | administratively down | down     |
| Ethernet1 | 10.0.0.11   | YES | NVRAM  | up                    | up       |
| Loopback0 | 192.168.6.1 | YES | manual | up                    | up       |
| Loopback1 | 10.12.12.12 | YES | NVRAM  | up                    | up       |

```
Router# show ip interface brief
```

| Interface | IP-Address  | OK? | Method | Status                | Protocol |
|-----------|-------------|-----|--------|-----------------------|----------|
| Ethernet0 | unassigned  | YES | NVRAM  | administratively down | down     |
| Ethernet1 | 10.0.0.11   | YES | NVRAM  | up                    | up       |
| Loopback1 | 10.12.12.12 | YES | NVRAM  | up                    | up       |

## Troubleshooting Dead Peer Detection

To troubleshoot dead peer detection, use the **show crypto ipsec client ezvpn** command.

### Examples

The following typical output displays the current server and the peers that have been pushed by the Easy VPN server:

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 4
Tunnel name : ez1
Inside interface list: Loopback1,
Outside interface: Ethernet1
```

```
Current State: IPSEC_ACTIVE
Last Event: CONNECT
Address: 192.168.6.5
Mask: 255.255.255.255
DNS Primary: 10.2.2.2
DNS Secondary: 10.2.2.3
NBMS/WINS Primary: 10.6.6.6
Default Domain: cisco.com
Save Password: Allowed
Current EzVPN Peer:10.0.0.110
Backup Gateways
(0): green.cisco.com
(1): blue
```

## Configuration Examples for Cisco Easy VPN Remote

This section provides the following configuration examples.

### Easy VPN Remote Configuration Examples

- [Client Mode Configuration: Examples, page 68](#)
- [Local Address Support for Easy VPN Remote: Example, page 73](#)
- [Network Extension Mode Configuration: Examples, page 74](#)
- [Save Password Configuration: Example, page 78](#)
- [PFS Support: Examples, page 79](#)
- [Dial Backup: Examples, page 79](#)
- [Web-Based Activation: Example, page 85](#)
- [Easy VPN Remote with Virtual IPsec Interface Support Configuration: Examples, page 85](#)
- [Dual Tunnel Configuration: Example, page 90](#)
- [Dual Tunnel Show Output: Examples, page 92](#)
- [Reactivate Primary Peer: Example, page 95](#)
- [Identical Addressing Support Configuration: Example, page 96](#)
- [cTCP on an Easy VPN Client \(Remote Device\): Examples, page 96](#)

### Easy VPN Server Configuration Examples

- [Cisco Easy VPN Server Without Split Tunneling: Example, page 97](#)
- [Cisco Easy VPN Server Configuration with Split Tunneling: Example, page 98](#)
- [Cisco Easy VPN Server Configuration with Xauth: Example, page 100](#)
- [Easy VPN Server Interoperability Support: Example, page 102](#)

# Easy VPN Remote Configuration Examples

## Client Mode Configuration: Examples

The examples in this section show configurations for the Cisco Easy VPN Remote feature in client mode. Also shown are the Cisco IOS Easy VPN server configurations that correspond to these client configurations.

- [Cisco Easy VPN Client in Client Mode \(Cisco 831\): Example, page 68](#)
- [Cisco Easy VPN Client in Client Mode \(Cisco 837\): Example, page 69](#)
- [Cisco Easy VPN Client in Client Mode \(Cisco 1700 Series\): Example, page 71](#)

For more client-mode configuration examples, see *IPSec VPN* (under the “Technical Documents” and “Cisco IOS IPSec Configuration Documents” sections) and to [Cisco Easy VPN Solutions](#).



### Note

Typically, users configure the Cisco 800 series routers with the SDM or CRWS web interface, not by entering CLI commands. However, the configurations shown here for the Cisco 800 series routers display typical configurations that can be used if manual configuration is desired.

### Cisco Easy VPN Client in Client Mode (Cisco 831): Example

In the following example, a Cisco 831 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in client mode. This example shows the following components of the Cisco Easy VPN Remote configuration:

- DHCP server pool—The **ip dhcp pool** command creates a pool of IP addresses to be assigned to the PCs connected to the Ethernet 0 interface of the router. The pool assigns addresses in the class C private address space (192.168.100.0) and configures each PC so that its default route is 192.168.100.1, which is the IP address assigned to the Ethernet interface of the router. The DHCP lease period is one day.
- Cisco Easy VPN remote configuration—The first **crypto ipsec client ezvpn easy vpn remote** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address **192.185.0.5** (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN Remote configuration is configured for the default **client** mode.



### Note

If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn easy vpn remote** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Ethernet 1 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```
! Cisco Router Web Setup Template
!
no service pad
no service tcp-small-servers
no service udp-small-servers
service timestamps debug uptime
service timestamps log uptime
```

```

service password-encryption
!
hostname 806Router
!
!
ip subnet-zero
ip domain-lookup
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool CLIENT
 import all
 network 10.10.10.0 255.255.255.255
 default-router 10.10.10.1
 lease 1 0 0
!
!
crypto ipsec client ezvpn easy_vpn_remote
 peer 192.168.0.5
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode client
!
!
interface Ethernet0
 ip address 10.10.10.1 255.255.255.255
 no cdp enable
 hold-queue 32 in
!
interface Ethernet1
 ip address dhcp
 no cdp enable
 crypto ipsec client ezvpn easy_vpn_remote
!
ip classless
ip http server
!
!
ip route 10.0.0.0 10.0.0.0 Ethernet1
!
line con 0
 exec-timeout 120 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 login local

```

### Cisco Easy VPN Client in Client Mode (Cisco 837): Example

In the following example, a Cisco 837 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in the client mode of operation. This example shows the following components of the Cisco Easy VPN remote configuration:

- **PPPoE configuration**—The ATM 0 interface is configured to support PPPoE connections over the Dialer 1 virtual interface. Because the interfaces use PPPoE, a DHCP IP address pool is not required to provide IP addresses to the connected PCs.
- **Cisco Easy VPN Remote configuration**—The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value of “easy vpn remote-password,” and it sets the peer destination to the IP address 10.0.0.5 (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for the default client mode.



**Note** If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn** command (interface configuration mode) assigns the Cisco Easy VPN remote configuration to the Dialer 1 interface so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

```

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vpdn enable
!
vpdn-group pppoe
 request-dialin
 protocol pppoe
 ip mtu adjust
!!
!
crypto ipsec client ezvpn easy_vpn_remote
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode client
 peer 10.0.0.5
!!
!
interface Ethernet0
 ip address 10.0.0.117 255.0.0.0
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
 pppoe-client dial-pool-number 1
!
 dsl operating-mode auto
!
interface Dialer1
 ip address 10.0.0.3 255.0.0.0
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 crypto ipsec client ezvpn easy_vpn_remote
!
 ip classless
 ip route 0.0.0.0 0.0.0.0 ATM0
 ip route 0.0.0.0 0.0.0.0 Dialer1 permanent
 ip route 10.0.0.0 255.0.0.0 10.0.0.13

```



```
ip http server
ip pim bidir-enable
!
line con 0
 stopbits 1
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

### Cisco Easy VPN Client in Client Mode (Cisco 1700 Series): Example

In the following example, a Cisco 1753 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in the client mode of operation. This example shows a running configuration of a Cisco 1753 that has two inside interfaces and one outside interface on one tunnel. The **connect auto** subcommand manually establishes the IPsec VPN tunnel.

Router# **show running-config**

```
Building configuration...
Current configuration : 881 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mma-1753
!
!
memory-size iomem 15
ip subnet-zero
!!
!
ip ssh time-out 120
ip ssh authentication-retries 3
! !
!
crypto ipsec client ezvpn easy_vpn_remote
connect auto
group ezvpn key ezvpn
mode client
peer 10.6.6.1
! !
!
interface FastEthernet0/0
ip address 10.4.4.2 255.255.255.0
speed auto
crypto ipsec client ezvpn easy_vpn_remote inside
!
interface Serial0/0
ip address 10.6.6.2 255.255.255.0
no fair-queue
crypto ipsec client ezvpn easy_vpn_remote
!
interface Serial1/0
ip address 10.5.5.2 255.255.255.0
clock rate 4000000
crypto ipsec client ezvpn easy_vpn_remote inside
!
ip classless
no ip http server
```

```

ip pim bidir-enable
! !
!
line con 0
line aux 0
line vty 0 4
login
!
end

```

The following example shows a running configuration of a Cisco 1760 router that has two active, automatically connected tunnels, easy vpn remote1 and easy vpn remote2. Tunnel easy vpn remote1 has two configured inside interfaces and one configured outside interface. Tunnel easy vpn remote2 has one configured inside interface and one configured outside interface. The example also shows the output for the **show crypto ipsec client ezvpn** command that lists the tunnel names and the outside and inside interfaces.

Router# **show running-config**

```

Building configuration...
Current configuration : 1246 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1760
!
aaa new-model
!
!
aaa session-id common
!
ip subnet-zero
!!
!
crypto ipsec client ezvpn easy_vpn_remote2
connect auto
group ez key ez
mode network-extension
peer 10.7.7.1
crypto ipsec client ezvpn easy_vpn_remote1
connect auto
group ezvpn key ezvpn
mode client
peer 10.6.6.1
! !
!
interface FastEthernet0/0
ip address 10.5.5.2 255.255.255.0
speed auto
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote1 inside
!
interface Serial0/0
ip address 10.4.4.2 255.255.255.0
no ip route-cache
no ip mroute-cache
no fair-queue
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote1 inside
!

```

```

interface Serial0/1
ip address 10.3.3.2 255.255.255.0
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote2 inside
!
interface Serial1/0
ip address 10.6.6.2 255.255.255.0
clockrate 4000000
no cdp enable
crypto ipsec client ezvpn easy_vpn_remotel
!
interface Serial1/1
ip address 10.7.7.2 255.255.255.0
no keepalive
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote2
!
ip classless
no ip http server
ip pim bidir-enable
!
!
radius-server retransmit 3
radius-server authorization permit missing Service-Type
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end

```

```
Router# show crypto ipsec client ezvpn
```

```

Tunnel name : easy_vpn_remotel
Inside interface list: FastEthernet0/0, Serial0/0,
Outside interface: Serial1/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.0.0.5
Mask: 255.255.255.255
Default Domain: cisco.com
Tunnel name : easy_vpn_remote2
Inside interface list: Serial0/1,
Outside interface: Serial1/1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Default Domain: cisco.com

```

## Local Address Support for Easy VPN Remote: Example

The following example shows that the **local-address** command is used to specify the loopback 0 interface for sourcing tunnel traffic:

```

Router# configure terminal
Router(config)# crypto ipsec client ezvpn telecommuter-client
Router(config-crypto-ezvpn)# local-address loopback0

```

## Network Extension Mode Configuration: Examples

In this section, the following examples demonstrate how to configure the Cisco Easy VPN Remote feature in the network extension mode of operation. Also shown are the Cisco IOS Easy VPN server configurations that correspond to these client configurations.

- [Cisco Easy VPN Client in Network Extension Mode \(Cisco 831\): Example, page 74](#)
- [Cisco Easy VPN Client in Network Extension Mode \(Cisco 837\): Example, page 75](#)
- [Cisco Easy VPN Client in Network Extension Mode \(Cisco 1700 Series\): Example, page 77](#)

For more network extension mode configuration examples, see *IPSec VPN* (under the “Technical Documents” and “Cisco IOS IPSec Configuration Documents” sections) and to *Cisco Easy VPN Solutions*.

### Cisco Easy VPN Client in Network Extension Mode (Cisco 831): Example

In the following example, a Cisco 831 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature. This example shows the following components of the Cisco Easy VPN remote configuration:

- The Ethernet 0 interface is assigned an address in the network address space of the Cisco IOS Easy VPN server. The **ip route** command directs all traffic for this network space from the Ethernet 1 interface to the destination server.
- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address 192.185.0.5 (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for network extension mode.



**Note** If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Ethernet 1 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```
! Cisco Router Web Setup Template
!
no service pad
no service tcp-small-servers
no service udp-small-servers
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Router
!
!
ip subnet-zero
ip domain-lookup
!
!
ip dhcp excluded-address 172.31.1.1
!
ip dhcp pool localpool
```

```

import all
network 172.31.1.0 255.255.255.255
default-router 172.31.1.1
lease 1 0 0
!
!
crypto ipsec client ezvpn easy_vpn_remote
peer 192.168.0.5
group easy_vpn_remote_groupname key easy_vpn_remote_password
mode network-extension
!
!
interface Ethernet0
ip address 172.31.1.1 255.255.255.255
no cdp enable
hold-queue 32 in
!
interface Ethernet1
ip address dhcp
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote
!
ip classless
ip route 172.31.0.0 255.255.255.255 Ethernet1
ip http server
!
!
line con 0
exec-timeout 120 0
stopbits 1
line vty 0 4
exec-timeout 0 0
login local

```

### Cisco Easy VPN Client in Network Extension Mode (Cisco 837): Example

In the following example, a Cisco 837 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in client mode. This example shows the following components of the Cisco Easy VPN remote configuration:

- PPPoE configuration—The ATM 0 interface is configured to support PPPoE connections over the Dialer 1 virtual interface. Because the interfaces use PPPoE, a DHCP IP address pool is not required to provide IP addresses to the connected PCs.
- The Ethernet 0 interface is assigned an address in the network address space of the Cisco IOS Easy VPN server. The **ip route** command directs all traffic for this network space from the Dialer 1 interface to the destination server.
- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address 10.0.0.5 (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for the default network extension mode.



**Note** If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn** command (interface configuration mode) assigns the Cisco Easy VPN remote configuration to the Dialer1 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vpdn enable
!
vpdn-group pppoe
 request-dialin
 protocol pppoe
 ip mtu adjust
!
!
crypto ipsec client ezvpn easy_vpn_remote
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode network-extension
 peer 10.0.0.5
!
!
interface Ethernet0
 ip address 172.16.0.30 255.255.255.192
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
 pppoe-client dial-pool-number 1
!
dsl operating-mode auto
!
interface Dialer1
 ip address 10.0.0.3 255.0.0.0
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 crypto ipsec client ezvpn easy_vpn_remote
!
ip classless
ip route 172.16.0.0 255.255.255.128 Dialer1
ip route 0.0.0.0 0.0.0.0 ATM0
ip route 0.0.0.0 0.0.0.0 Dialer1 permanent
ip route 10.0.0.0 255.0.0.0 10.0.0.13
ip http server
ip pim bidir-enable
!
line con 0
 stopbits 1

```

```

line vty 0 4
 login
!
scheduler max-task-time 5000

```

### Cisco Easy VPN Client in Network Extension Mode (Cisco 1700 Series): Example

In the following example, a Cisco 1700 series router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in the network extension mode of operation. This example shows the following components of the Cisco Easy VPN remote configuration:

- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration that is named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address 10.0.0.2 (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for network extension mode.



**Note** If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn easy vpn remote** command (interface configuration mode) assigns the Cisco Easy VPN remote configuration to the Ethernet 0 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```

!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1710
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
ip dhcp excluded-address 10.0.0.10
!
ip dhcp pool localpool
 import all
 network 10.70.0.0 255.255.255.248
 default-router 10.70.0.10
 lease 1 0 0
!
!
crypto ipsec client ezvpn easy_vpn_remote
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode network-extension
 peer 10.0.0.2
!
!

```

```

interface Ethernet0
 ip address 10.50.0.10 255.0.0.0
 half-duplex
 crypto ipsec client ezvpn easy_vpn_remote
!
interface FastEthernet0
 ip address 10.10.0.10 255.0.0.0
 speed auto
!
ip classless
ip route 10.20.0.0 255.0.0.0 Ethernet0
ip route 10.20.0.0 255.0.0.0 Ethernet0
no ip http server
ip pim bidir-enable
!!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login

```

## Save Password Configuration: Example

The following sample **show running-config** output shows that the Save Password feature has been configured (note the **password encryption aes** command and **username** keywords in the output):

Router# **show running-config**

```

133.CABLEMODEM.CISCO: Oct 28 18:42:07.115: %SYS-5-CONFIG_I: Configured from console by
consolen
Building configuration...

```

```

Current configuration : 1269 bytes
!
! Last configuration change at 14:42:07 UTC Tue Oct 28 2003
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
clock timezone UTC -4
no aaa new-model
ip subnet-zero
no ip routing
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
password encryption aes
!
!

```



```

no crypto isakmp enable
!
!
crypto ipsec client ezvpn remote_vpn_client
 connect auto
 mode client
 username greentree password 6 ARiFgh`SOJfMHLK[MHMQJZagR\M
!
!
interface Ethernet0
 ip address 10.3.66.4 255.255.255.0
 no ip route-cache
 bridge-group 59

```

## PFS Support: Examples

The following **show crypto ipsec client ezvpn** command output shows the group name (“2”) and that PFS is being used:

```
Router# show crypto ipsec client ezvpn
```

```

Easy VPN Remote Phase: 4

Tunnel name : ez1
Inside interface list: Loopback1,
Outside interface: Ethernet1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.6.6
Mask: 255.255.255.255
Using PFS Group: 2
Save Password: Allowed
Current EzVPN Peer:10.0.0.110

```

Note that on a Cisco IOS EasyVPN server, PFS must be included in IPsec proposals by adding to the crypto map, as in the following example:

```

crypto dynamic-map mode 1
 set security-association lifetime seconds 180
 set transform-set client
 set pfs group2
 set isakmp-profile fred
reverse-route

```

## Dial Backup: Examples

### Static IP Addressing

The following example shows that static IP addressing has been configured for a Cisco 1711 router:

```
Router# show running-config
```

```

Building configuration...

Current configuration : 3427 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ph4_R5

```

```

!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username ph4_R8 password 0 cisco
username ph4_R7 password 0 lab
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
aaa new-model
!
!
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
ip cef
ip ids po max-events 100
ip dhcp-client default-router distance 1
no ftp-server write-enable
!
!
track 123 rtr 3 reachability
!
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec client ezvpn backup_profile_vpn3k
connect auto
group hw_client_groupname key password123
mode client
peer 10.0.0.5
username rchu password password123
crypto ipsec client ezvpn hw_client_vpn3k
connect auto
group hw_client_groupname key password123
backup backup_profile_vpn3k track 123
mode client
peer 10.0.0.5
username rchu password password123
!
!
interface Loopback0
ip address 10.40.40.50 255.255.255.255
!
interface Loopback1
ip address 10.40.40.51 255.255.255.255
!
interface Loopback2
no ip address
!
interface FastEthernet0
description Primary Link to 10.0.0.2
ip address 10.0.0.10 255.255.255.0
duplex auto
speed auto
no cdp enable
crypto ipsec client ezvpn hw_client_vpn3k
!
interface FastEthernet1

```

```
no ip address
duplex full
speed 100
no cdp enable
!
interface FastEthernet2
no ip address
no cdp enable
!
interface FastEthernet3
no ip address
no cdp enable
!
interface FastEthernet4
no ip address
no cdp enable
!
interface Vlan1
ip address 10.0.0.1 255.255.255.0
crypto ipsec client ezvpn backup_profile_vpn3k inside
crypto ipsec client ezvpn hw_client_vpn3k inside
!
interface Async1
description Backup Link
no ip address
ip nat outside
ip virtual-reassembly
encapsulation ppp
no ip route-cache cef
dialer in-band
dialer pool-member 1
dialer-group 1
async default routing
async mode dedicated
!
interface Dialer1
ip address 10.30.0.1 255.255.255.0
encapsulation ppp
no ip route-cache cef
dialer pool 1
dialer idle-timeout 60
dialer string 102
dialer hold-queue 100
dialer-group 1
crypto ipsec client ezvpn backup_profile_vpn3k
!
ip local policy route-map policy_for_rtr
ip classless

ip route 0.0.0.0 0.0.0.0 faste0 track 123

ip route 0.0.0.0 0.0.0.0 Dialer1 240
no ip http server
no ip http secure-server
!
!
ip access-list extended dummy1
permit ip host 10.0.0.2 host 10.3.0.1
ip access-list extended important_traffic
permit ip 10.0.0.0 0.0.0.255 10.0.0.2 0.0.0.255
permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255
ip access-list extended important_traffic_2
permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255
```

```

access-list 112 permit icmp any host 10.0.10.2 echo
dialer-list 1 protocol ip permit
no cdp run
!
route-map policy_for_rtr permit 10
 match ip address 112
 set interface Null0
 set ip next-hop 10.0.10.2
!
!
control-plane
!
rtr 2
 type echo protocol ipIcmpEcho 10.0.0.2 source-ipaddr 10.0.0.3
 timeout 10000
 threshold 1000
 frequency 11
rtr schedule 2 life forever start-time now
rtr 3
 type echo protocol ipIcmpEcho 10.0.0.2 source-interface FastEthernet0
 timeout 10000
 threshold 1000
 frequency 11
rtr schedule 3 life forever start-time now
!
line con 0
 exec-timeout 0 0
line 1
 modem InOut
 modem autoconfigure discovery
 transport input all
 autoselect ppp
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 password lab
!

```

### DHCP Configured on Primary Interface and PPP Async As Backup

The following example shows that a Cisco 1711 router has been configured so that DHCP is configured on the primary interface and PPP asynchronous mode is configured as the backup:

Router# **show running-config**

Building configuration...

```

Current configuration : 3427 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ph4_R5
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username ph4_R8 password 0 cisco

```

```
username ph4_R7 password 0 lab
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
aaa new-model
!
!
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
ip cef
ip ids po max-events 100
ip dhcp-client default-router distance 1
no ftp-server write-enable
!
!
track 123 rtr 3 reachability
!
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec client ezvpn backup_profile_vpn3k
connect auto
group hw_client_groupname key password123
mode client
peer 10.0.0.5
username rchu password password123
crypto ipsec client ezvpn hw_client_vpn3k
connect auto
group hw_client_groupname key password123
backup backup_profile_vpn3k track 123
mode client
peer 10.0.0.5
username rchu password password123
!
!
interface Loopback0
ip address 10.40.40.50 255.255.255.255
!
interface Loopback1
ip address 10.40.40.51 255.255.255.255
!
interface Loopback2
no ip address
!
interface FastEthernet0
description Primary Link to 10.0.0.2
ip dhcp client route track 123
ip address dhcp
duplex auto
speed auto
no cdp enable
crypto ipsec client ezvpn hw_client_vpn3k
!
interface FastEthernet1
no ip address
duplex full
speed 100
no cdp enable
!
interface FastEthernet2
```

```

no ip address
no cdp enable
!
interface FastEthernet3
no ip address
no cdp enable
!
interface FastEthernet4
no ip address
no cdp enable
!
interface Vlan1
ip address 10.0.0.1 255.255.255.0
crypto ipsec client ezvpn backup_profile_vpn3k inside
crypto ipsec client ezvpn hw_client_vpn3k inside
!
interface Async1
description Backup Link
no ip address
ip nat outside
ip virtual-reassembly
encapsulation ppp
no ip route-cache cef
dialer in-band
dialer pool-member 1
dialer-group 1
async default routing
async mode dedicated
!
interface Dialer1
ip address 10.0.0.3 255.255.255.0
encapsulation ppp
no ip route-cache cef
dialer pool 1
dialer idle-timeout 60
dialer string 102
dialer hold-queue 100
dialer-group 1
crypto ipsec client ezvpn backup_profile_vpn3k
!
ip local policy route-map policy_for_rtr
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 240
no ip http server
no ip http secure-server
!
!
ip access-list extended dummy1
permit ip host 10.10.0.2 host 10.0.0.1
ip access-list extended important_traffic
permit ip 10.0.0.0 0.0.0.255 10.0.0.2 0.0.0.255
permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255
ip access-list extended important_traffic_2
permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255
access-list 112 permit icmp any host 10.0.0.2 echo
dialer-list 1 protocol ip permit
no cdp run
!
route-map policy_for_rtr permit 10
match ip address 112
set interface Null0
set ip next-hop 10.0.0.2
!
!

```

```
control-plane
!
rtr 2
 type echo protocol ipIcmpEcho 10.0.0.2 source-ipaddr 10.0.0.3
 timeout 10000
 threshold 1000
 frequency 11
rtr schedule 2 life forever start-time now
rtr 3
 type echo protocol ipIcmpEcho 10.0.0.2 source-interface FastEthernet0
 timeout 10000
 threshold 1000
 frequency 11
rtr schedule 3 life forever start-time now
!
line con 0
 exec-timeout 0 0
line 1
 modem InOut
 modem autoconfigure discovery
 transport input all
 autoselect ppp
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 password lab
!
```

## Web-Based Activation: Example

The following example shows that HTTP connections from the user are to be intercepted and that the user can do web-based authentication (192.0.0.13 is the VPN client device and 192.0.0.1 is the server device):

```
crypto ipsec client ezvpn tunnel22
 connect manual
 group tunnel22 key 22tunnel
 mode client
 peer 192.168.0.1
 xauth userid mode http-intercept
!
!
interface Ethernet0
 ip address 10.4.23.15 255.0.0.0
 crypto ipsec client ezvpn tunnel22 inside!
interface Ethernet1
 ip address 192.168.0.13 255.255.255.128
 duplex auto
 crypto ipsec client ezvpn tunnel22
!
```

## Easy VPN Remote with Virtual IPsec Interface Support Configuration: Examples

The following examples indicate that Virtual IPsec Interface Support has been configured on the Easy VPN remote devices.

## Virtual IPsec Interface: Generic Virtual Access

The following example shows an Easy VPN remote device with virtual-interface support using a generic virtual-access IPsec interface.

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone IST 0
ip subnet-zero
no ip dhcp use vrf connected
!
!
crypto ipsec client ezvpn ez
 connect manual
 group easy key cisco
 mode client
 peer 10.3.0.2
 virtual-interface
 xauth userid mode interactive
!
!
interface Ethernet0/0
 ip address 10.1.0.2 255.255.255.0
 no keepalive
 no cdp enable
 crypto ipsec client ezvpn ez inside
!
interface Ethernet1/0
 ip address 10.2.0.1 255.255.255.0
 no keepalive
 no cdp enable
 crypto ipsec client ezvpn ez
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.2 2
no ip http server
no ip http secure-server
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end

```



## Virtual IPsec Interface: Virtual Access Derived from Virtual Template

The following example shows an Easy VPN remote device with virtual-interface support using a virtual-template-derived virtual-access IPsec interface:

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone IST 0
ip subnet-zero
no ip dhcp use vrf connected
!
!
crypto ipsec client ezvpn ez
 connect manual
 group easy key cisco
 mode client
 peer 10.3.0.2
 virtual-interface 1
 xauth userid mode interactive
!
!
interface Ethernet0/0
 ip address 10.1.0.2 255.255.255.0
 no keepalive
 no cdp enable
 crypto ipsec client ezvpn ez inside
!
interface Ethernet1/0
 ip address 10.2.0.1 255.255.255.0
 no keepalive
 no cdp enable
 crypto ipsec client ezvpn ez
!
interface Virtual-Template1 type tunnel
 no ip address
 tunnel mode ipsec ipv4
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.2 2
no ip http server
no ip http secure-server
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

## When the Tunnel Is Down

The result of a virtual-interface configuration on an Easy VPN profile is the creation of a virtual-access interface. This interface provides IPsec encapsulation. The output below shows the configuration of a virtual-access interface when Easy VPN is “down.”

```
Router# show running-config interface virtual-access 2
```

```
Building configuration...
```

```
Current configuration : 99 bytes
```

```
!
interface Virtual-Access2
 no ip address
 tunnel source Ethernet1/0
 tunnel mode ipsec ipv4
end
```

A virtual-interface configuration results in the creation of a virtual-access interface. This virtual-access interface is made automatically outside the interface of the Easy VPN profile. The routes that are added later when the Easy VPN tunnels come up point to this virtual interface for sending the packets to the corporate network. If **crypto ipsec client ezvpn name outside (crypto ipsec client ezvpn name** command and **outside** keyword) is applied on a real interface, that interface is used as the IKE (IPsec) endpoint (that is, IKE and IPsec packets use the address on the interface as the source address).

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 5
```

```
Tunnel name : ez
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.3.0.2
```

Because a virtual interface, or for that matter any interface, is routable, routes act like traffic selectors. When the Easy VPN tunnel is “down,” there are no routes pointing to the virtual interface, as shown in the following example:

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 10.2.0.2 to network 0.0.0.0
```

```
10.0.0.0/24 is subnetted, 2 subnets
C 10.2.0.0 is directly connected, Ethernet1/0
C 10.1.0.0 is directly connected, Ethernet0/0
S* 0.0.0.0/0 [2/0] via 10.2.0.2
```

## When the Tunnel Is Up

In the case of client or network plus mode, Easy VPN creates a loopback interface and assigns the address that is pushed in mode configuration. To assign the address of the loopback to the interface, use the **ip unnumbered** command (**ip unnumbered loopback**). In the case of network extension mode, the virtual access will be configured as **ip unnumbered ethernet0** (the bound interface).

```
Router# show running-config interface virtual-access 2
```

```
Building configuration...
```

```
Current configuration : 138 bytes
```

```
!
interface Virtual-Access2
 ip unnumbered Loopback0
 tunnel source Ethernet1/0
 tunnel destination 10.3.0.2
 tunnel mode ipsec ipv4
end
```

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 5
```

```
Tunnel name : ez
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.5.0.2
Mask: 255.255.255.255
DNS Primary: 10.6.0.2
NBMS/WINS Primary: 10.7.0.1
Default Domain: cisco.com
Using PFS Group: 2
Save Password: Disallowed
Split Tunnel List: 1
 Address : 10.4.0.0
 Mask : 255.255.255.0
 Protocol : 0x0
 Source Port : 0
 Dest Port : 0
Current EzVPN Peer: 10.3.0.2
```

When the tunnels come up, Easy VPN adds either a default route that points to the virtual-access interface or adds routes for all the split attributes of the subnets that point to the virtual-access interface. Easy VPN also adds a route to the peer (destination or concentrator) if the peer is not directly connected to the Easy VPN device.

The following **show ip route** command output examples are for virtual IPsec interface situations in which a split tunnel attribute was sent by the server and a split tunnel attribute was not sent, respectively.

### Split Tunnel Attribute Has Been Sent by the Server

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```

o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.2.0.2 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C 10.2.0.0/24 is directly connected, Ethernet1/0
S 10.3.0.2/32 [1/0] via 10.2.0.2, Ethernet1/0 <<< Route to
peer (EzVPN server)
C 10.1.0.0/24 is directly connected, Ethernet0/0
C 10.5.0.2/32 is directly connected, Loopback0
S 10.4.0.0/24 [1/0] via 0.0.0.0, Virtual-Access2 <<< Split
tunnel attr sent by the server
S* 10.0.0.0/0 [2/0] via 10.2.0.2

```

### Split Tunnel Attribute Has Not Been Sent by the Server

All networks in the split attribute should be shown, as in the following example:

Router# **show ip route**

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.2.0.0/24 is directly connected, Ethernet1/0
! The following line is the route to the peer (the Easy VPN server).
S 10.3.0.2/32 [1/0] via 10.2.0.2, Ethernet1/0
C 10.1.0.0/24 is directly connected, Ethernet0/0
C 10.5.0.3/32 is directly connected, Loopback0
! The following line is the default route.
S* 10.0.0.0/0 [1/0] via 10.0.0.0, Virtual-Access2

```

## Dual Tunnel Configuration: Example

The following is an example of a typical dual-tunnel configuration:

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable password lab
!
no aaa new-model
!
resource policy
!
clock timezone IST 0
ip subnet-zero
!
!

```

```
username lab password 0 lab
!
!
crypto ipsec client ezvpn ezvpn1
 connect manual
 group easy key cisco
 mode network-extension
 peer 10.75.1.2
 virtual-interface 1
 xauth userid mode interactive
crypto ipsec client ezvpn ezvpn2
 connect manual
 group easy key cisco
 mode network-extension
 peer 10.75.2.2
 virtual-interface 1
 xauth userid mode interactive
!
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.255
 no keepalive
 crypto ipsec client ezvpn ezvpn1 inside
 crypto ipsec client ezvpn ezvpn2 inside
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 ip address 10.76.1.2 255.255.255.0
 no keepalive
 crypto ipsec client ezvpn ezvpn1
 crypto ipsec client ezvpn ezvpn2
!
interface Serial2/0
 ip address 10.76.2.2 255.255.255.0
 no keepalive
 serial restart-delay 0
!
interface Virtual-Template1 type tunnel
 no ip address
 tunnel mode ipsec ipv4
!
!
ip classless
ip route 10.0.0.0 10.0.0.0 10.76.1.1 2
no ip http server
no ip http secure-server
!
!
no cdp run
!
!
line con 0
 exec-timeout 0 0
```

```

line aux 0
line vty 0 4
 login local
!
end

```

## Dual Tunnel Show Output: Examples

The following **show** command examples display information about three phases of a dual tunnel that is coming up:

- First Easy VPN tunnel is up
- Second Easy VPN tunnel is initiated
- Both of the Easy VPN tunnels are up

### Before the EzVPN Tunnels Are Up

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 6
```

```

Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.75.1.2

```

```

Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2

```

```
Router# show ip route
```

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

```

The gateway of last resort is 10.76.1.1 to network 0.0.0.0.

```

10.0.0.0/24 is subnetted, 2 subnets
C 10.76.2.0 is directly connected, Serial2/0
C 10.76.1.0 is directly connected, Ethernet1/0
C 192.168.1.0/24 is directly connected, Ethernet0/0
S* 0.0.0.0/0 [2/0] via 10.76.1.1

```



#### Note

The metric of the default route should be greater than 1 so that the default route that is added later by Easy VPN takes precedence and the traffic goes through the Easy VPN virtual-access interface.

**Easy VPN “ezvpn2” Tunnel Is Up**

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 6
```

```
Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.75.1.2
```

```
Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2
```

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route
```

The gateway of last resort is 0.0.0.0 to network 0.0.0.0.

```
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
! The next line is the Easy VPN route.
S 10.75.2.2/32 [1/0] via 10.76.1.1
C 10.76.2.0/24 is directly connected, Serial2/0
C 10.76.1.0/24 is directly connected, Ethernet1/0
C 192.168.1.0/24 is directly connected, Ethernet0/0
! The next line is the Easy VPN route.
S* 0.0.0.0/0 [1/0] via 0.0.0.0, Virtual-Access3
```

One default route and one route to the peer is added as shown above.

**Easy VPN “ezvpn2” Is Up and Easy VPN “ezvpn1” Is Initiated**

```
Router# crypto ipsec client ezvpn connect ezvpn1
```

```
Router# show crypto ipsec cli ent ezvpn
```

```
Easy VPN Remote Phase: 6
```

```
Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: READY
```

```
Last Event: CONNECT
Save Password: Disallowed
Current EzVPN Peer: 10.75.1.2
```

```
Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2
```

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route
```

The gateway of last resort is 10.0.0.0 to network 10.0.0.0.

```
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S 10.75.2.2/32 [1/0] via 10.76.1.1
! The next line is the Easy VPN router.
S 10.75.1.2/32 [1/0] via 10.76.1.1
C 10.76.2.0/24 is directly connected, Serial2/0
C 10.76.1.0/24 is directly connected, Ethernet1/0
C 192.168.1.0/24 is directly connected, Ethernet0/0
S* 10.0.0.0/0 [1/0] via 10.0.0.0, Virtual-Access3
```

The route to 10.75.1.2 is added before the Easy VPN “ezvpn1” tunnel has come up. This route is for reaching the Easy VPN “ezvpn1” peer 10.75.1.2.

### Both Tunnels Are Up

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 6
```

```
Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Split Tunnel List: 1
 Address : 192.168.3.0
 Mask : 255.255.255.255
 Protocol : 0x0
 Source Port : 0
 Dest Port : 0
Current EzVPN Peer: 10.75.1.2
```



```
Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2
```

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route
```

The gateway of last resort is 10.0.0.0 to network 10.0.0.0.

```
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
! The next line is the Easy VPN router (ezvpn2).
S 10.75.2.2/32 [1/0] via 10.76.1.1
! The next line is the Easy VPN router (ezvpn1).
S 10.75.1.2/32 [1/0] via 10.76.1.1
C 10.76.2.0/24 is directly connected, Serial2/0
C 10.76.1.0/24 is directly connected, Ethernet1/0
C 192.168.1.0/24 is directly connected, Ethernet0/0
! The next line is the Easy VPN route (ezvpn1).
S 192.168.3.0/24 [1/0] via 0.0.0.0, Virtual-Access2
! The next line is the Easy VPN (ezvpn2).
S* 10.0.0.0/0 [1/0] via 10.0.0.0, Virtual-Access3
```

The route to split tunnel “192.168.3.0/24” that points to Virtual-Access2 is added for the Easy VPN “ezvpn” tunnel as shown in the above **show** output.

## Reactivate Primary Peer: Example

The following show output illustrates that the default primary peer feature has been activated. The primary default peer is 10.3.3.2.

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 6
```

```
Tunnel name : ezc
Inside interface list: Loopback0
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Primary EzVPN Peer: 10.3.3.2, Last Tried: Dec 30 07:21:23.071
Last Event: CONN_UP
Address: 10.7.7.1
Mask: 255.255.255.255
DNS Primary: 10.1.1.1
NBMS/WINS Primary: 10.5.254.22
```

```

Save Password: Disallowed
Current EzVPN Peer: 10.4.4.2

23:52:44: %CRYPTO-6-EZVPN_CONNECTION_UP(Primary peer):
 User: lab, Group: hw-client-g
 Client_public_addr=10.4.22.103, Server_public_addr=10.4.23.112
 Assigned_client_addr=10.7.7.1

```

## Identical Addressing Support Configuration: Example

In the following example, a Cisco router is configured for the Identical Addressing Support feature:

```

interface Virtual-Template1 type tunnel
 no ip address
 ip nat outside
!
crypto ipsec client ezvpn easy
 connect manual
 group easy key work4cisco
 mode network-extension
 peer 10.2.2.2
 virtual-interface 1
 nat allow
 nat acl 100
!
interface Ethernet1
 ip address 10.0.0.1 255.255.255.0
 ip nat outside
 crypto ipsec client ezvpn easy
!
interface Ethernet0
 ip address 10.0.0.2 255.255.255.0
 ip nat inside
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.252
 ip nat enable
crypto ipsec client ezvpn easy inside
!
ip access-list 100 permit ip 10.0.0.0 0.0.0.255 any
!
ip nat inside source list 100 interface Loopback0 overload
!
ip nat inside source static 10.5.5.5 1.1.1.101

```

## cTCP on an Easy VPN Client (Remote Device): Examples

For configuration and troubleshooting examples, see the topic “cTCP on Cisco Easy VPN remote devices” in the [“Related Documents” section on page 102](#).

## Easy VPN Server Configuration Examples

This section describes basic Cisco Easy VPN server configurations that support the Cisco Easy VPN remote configurations given in the previous sections. For complete information on configuring these servers, see [Easy VPN Server](#) for Cisco IOS Release 12.3(7)T, available on Cisco.com.

- [Cisco Easy VPN Server Without Split Tunneling: Example, page 97](#)
- [Cisco Easy VPN Server Configuration with Split Tunneling: Example, page 98](#)
- [Cisco Easy VPN Server Configuration with Xauth: Example, page 100](#)
- [Easy VPN Server Interoperability Support: Example, page 102](#)

## Cisco Easy VPN Server Without Split Tunneling: Example

The following example shows the Cisco Easy VPN server that is the destination peer router for the Cisco Easy VPN remote network extension mode configurations shown earlier in this section. In addition to the other IPsec configuration commands, the **crypto isakmp client configuration group** command defines the attributes for the VPN group that was assigned to the Easy VPN remote router. This includes a matching key value (easy vpn remote password), and the appropriate routing parameters, such as DNS server, for the Easy VPN remotes.

To support the network extension mode of operation, the **ip route** command instructs that incoming packets for the 172.168.0.0 network be directed from the cable modem interface to the Cisco Easy VPN remote. Other **ip route** commands might be needed, depending on the topology of your network.



### Note

This example shows a Cisco uBR925 cable access router, but typically the destination Easy VPN remote is a router, such as a Cisco VPN 3000 concentrator or a Cisco IOS router, that supports the Easy VPN Server feature.

```

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model
!
!
aaa authorization network easy vpn remote-groupname local
aaa session-id common
!
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool
!
crypto isakmp client configuration group easy vpn remote-groupname
 key easy vpn remote-password
 dns 172.16.0.250 172.16.0.251
 wins 172.16.0.252 172.16.0.253
 domain cisco.com
 pool dynpool
!
```

```

!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
 reverse-route
!
!
crypto map dynmap isakmp authorization list easy vpn remote-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0
 ip address 172.16.0.129 255.255.255.128
!
interface cable-modem0
 no cable-modem compliant bridge
 crypto map dynmap
!
interface usb0
 no ip address
 arp timeout 0
!
ip local pool dynpool 172.16.0.65 172.16.0.127
ip classless
! Add the appropriate ip route commands for network-extension mode
ip route 172.16.1.0 255.255.255.248 cable-modem0
no ip http server
no ip http cable-monitor
!
snmp-server manager
!
line con 0
 exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000

```

## Cisco Easy VPN Server Configuration with Split Tunneling: Example

The following example shows a Cisco Easy VPN server that is configured for a split tunneling configuration with a Cisco Easy VPN remote. This example is identical to that shown in the “[Cisco Easy VPN Server Without Split Tunneling: Example](#)” except for access list 150, which is assigned as part of the **crypto isakmp client configuration group** command. This access list allows the Cisco Easy VPN remote to use the server to access one additional subnet that is not part of the VPN tunnel without compromising the security of the IPsec connection.

To support network extension mode, the **ip route** command instructs that incoming packets for the 172.168.0.0 network be directed from the cable modem interface to the Cisco Easy VPN remote. Other **ip route** commands might be necessary, depending on the topology of your network.



### Note

This example shows a Cisco uBR925 cable access router, but typically the destination Easy VPN remote will be a router, such as a VPN 3000 concentrator or a Cisco IOS router, that supports the Easy VPN Server feature.

```

version 12.2
no service pad
service timestamps debug uptime

```

```
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model
!
!
aaa authorization network easy vpn remote-groupname local
aaa session-id common
!
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool
!
crypto isakmp client configuration group easy vpn remote-groupname
 key easy vpn remote-password
 dns 172.16.0.250 172.16.0.251
 wins 172.16.0.252 172.16.0.253
 domain cisco.com
 pool dynpool
ac1 150
!
!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
 reverse-route
!
!
crypto map dynmap isakmp authorization list easy vpn remote-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0
 ip address 172.16.0.129 255.255.255.255
!
interface cable-modem0
 no cable-modem compliant bridge
 crypto map dynmap
!
interface usb0
 no ip address
 arp timeout 0
!
ip local pool dynpool 172.16.0.65 172.16.0.127
ip classless
! Add the appropriate ip route commands for network-extension mode
ip route 172.16.1.0 255.255.255.255 cable-modem0
no ip http server
no ip http cable-monitor
!
access-list 150 permit ip 172.16.0.128 10.0.0.127 any
```

```
snmp-server manager
!
line con 0
 exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000
end
```

## Cisco Easy VPN Server Configuration with Xauth: Example

The following example shows a Cisco Easy VPN server configured to support Xauth with the Cisco Easy VPN Remote feature. This example is identical to that shown in the “[Cisco Easy VPN Server Configuration with Split Tunneling: Example](#)” except for the following commands that enable and configure Xauth:

- **aaa authentication login userlist local**—Specifies the local username database for authentication at login time. You could also specify the use of RADIUS servers by first using the **aaa authentication login userlist group radius** command and then by specifying the RADIUS servers using the **aaa group server radius** command.
- **crypto isakmp xauth timeout**—Specifies the amount of time, in seconds, that the user has to enter the appropriate username and password to authenticate the session.
- **crypto map dynmap client authentication list userlist**—Creates a crypto map named “**dynmap**” that enables Xauth.
- **username cisco password 7 cisco**—Creates an entry in the local username database for a user with the username of “**cisco**” and an encrypted password of “**cisco**.” This command should be repeated for each separate user that accesses the server.

The following commands, which are also present in the non-Xauth configurations, are also required for Xauth use:

- **aaa authorization network easy vpn remote-groupname local**—Requires authorization for all network-related service requests for users in the group named “**easy vpn remote-groupname**” using the local username database.
- **aaa new-model**—Specifies that the router should use the new AAA authentication commands.
- **aaa session-id common**—Specifies that a unique and common session ID should be used for AAA sessions.
- **crypto map dynmap 1 ipsec-isakmp dynamic dynmap**—Specifies that IKE should be used to establish the IPsec SAs, using the crypt map named “**dynmap**” as the policy template.
- **crypto map dynmap client configuration address respond**—Enables IKE negotiation, accepting requests from any requesting peers.
- **crypto map dynmap isakmp authorization list easy vpn remote-groupname**—Configures the crypto map named “**dynmap**” to use IKE Shared Secret using the group named “**easy vpn remote-groupname**.”



### Tip

This configuration shows the server configured for split tunneling, but Xauth can also be used with nonsplit tunnel configurations as well.

**Note**

This example shows a Cisco uBR925 cable access router, but typically the destination Easy VPN server is a router such as a VPN 3000 concentrator or a Cisco IOS router that supports the Easy VPN Server feature.

```

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model
!
!
aaa authentication login userlist local
aaa authorization network easy vpn remote-groupname local
aaa session-id common
!
username cisco password 7 cisco
!
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool
crypto isakmp xauth timeout 60
!
crypto isakmp client configuration group easy vpn remote-groupname
 key easy vpn remote-password
 dns 172.16.0.250 172.16.0.251
 wins 172.16.0.252 172.16.0.253
 domain cisco.com
 pool dynpool
 acl 150
!
!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
 reverse-route
!
!
crypto map dynmap client authentication list userlist
crypto map dynmap isakmp authorization list easy vpn remote-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!!
!
interface Ethernet0
 ip address 172.16.0.129 255.255.255.128
!
interface cable-modem0

```

```

no cable-modem compliant bridge
crypto map dynmap
!
interface usb0
no ip address
arp timeout 0
!
ip local pool dynpool 172.16.0.65 172.16.0.127
ip classless
ip route 172.16.1.0 255.255.255.248 cable-modem0
no ip http server
no ip http cable-monitor
!
access-list 150 permit ip 172.16.0.128 0.0.0.127 any
snmp-server manager
!
line con 0
exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000
end

```

## Easy VPN Server Interoperability Support: Example

For information about this feature, see “General information on IPSec and VPN” in the section “[Additional References](#)” (*Managing VPN Remote Access*).

## Additional References

The following sections provide references related to Cisco Easy VPN Remote.

## Related Documents

| Related Topic                   | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Platform-specific documentation |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Cisco 800 series routers        | <ul style="list-style-type: none"> <li>• <a href="#">Cisco 800 Series Routers</a></li> <li>• <a href="#">Cisco 806 Router and SOHO 71 Router Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 806 Router Software Configuration Guide</a></li> <li>• <a href="#">Cisco 826, 827, 828, 831, 836, and 837 and SOHO 76, 77, 78, 91, 96, and 97 Routers Software Configuration Guide</a></li> <li>• <a href="#">Cisco 826 and SOHO 76 Router Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 827 and SOHO 77 Routers Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 828 and SOHO 78 Routers Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 837 ADSL Broadband Router</a></li> </ul> |



| Related Topic                                                       | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco uBR905 and Cisco uBR925 cable access routers                  | <ul style="list-style-type: none"> <li>• <a href="#">Cisco uBR925 Cable Access Router Hardware Installation Guide</a></li> <li>• <a href="#">Cisco uBR905 Hardware Installation Guide</a></li> <li>• <a href="#">Cisco uBR905/uBR925 Cable Access Router Software Configuration Guide</a></li> <li>• <a href="#">Cisco uBR905 Cable Access Router Subscriber Setup Quick Start Card</a></li> <li>• <a href="#">Cisco uBR925 Cable Access Router Subscriber Setup Quick Start Card</a></li> <li>• <a href="#">Cisco uBR925 Cable Access Router Quick Start User Guide</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Cisco 1700 series routers                                           | <ul style="list-style-type: none"> <li>• <a href="#">Cisco 1700 Series Router Software Configuration Guide</a></li> <li>• <a href="#">Cisco 1710 Security Router Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 1710 Security Router Software Configuration Guide</a></li> <li>• <a href="#">Cisco 1711 Security Access Router</a></li> <li>• <a href="#">Cisco 1720 Series Router Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 1721 Access Router Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 1750 Series Router Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 1751 Router Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 1751 Router Software Configuration Guide</a></li> <li>• <a href="#">Cisco 1760 Modular Access Router Hardware Installation Guide</a></li> </ul> <p>Also see the Cisco IOS release notes for Cisco IOS Release 12.2(4)YA:</p> <ul style="list-style-type: none"> <li>• <a href="#">SOHO 70 and Cisco 800 Series—Release Notes for Release 12.2(4)YA</a></li> <li>• <a href="#">Release Notes for Cisco uBR905 and Cisco uBR925 Cable Access Routers for Cisco IOS Release 12.2 YA</a></li> <li>• <a href="#">Cisco 1700 Series—Release Notes for Release 12.2(4)YA</a></li> </ul> |
| Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers | <ul style="list-style-type: none"> <li>• <a href="#">Cisco 2600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 2600 Series Routers Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 3600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 3600 Series Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 3700 Series Multiservice Access Routers</a></li> <li>• <a href="#">Cisco 3700 Series Routers Hardware Installation Guide</a></li> <li>• <a href="#">Cisco 2600 Series, 3600 Series, and 3700 Series Regulatory Compliance and Safety Information on Cisco.com</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| IPsec and VPN documentation                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Related Topic                                                                                            | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 802.1x authentication                                                                                    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Cisco IOS Easy VPN Remote with 802.1X Authentication</a> (white paper)</li> <li>• <a href="#">VPN Access Control Using 802.1X Local Authentication</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Access control lists, configuring                                                                        | <ul style="list-style-type: none"> <li>• <a href="#">IP Access List Overview</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Configuration information (additional in-depth)                                                          | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Security Command Reference</a>—Provides a reference for each of the Cisco IOS commands used to configure IPsec encryption and related security features.</li> <li>• <a href="#">SSL VPN</a>—Provides information about SSL VPN.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| cTCP on Cisco Easy VPN remote devices                                                                    | <ul style="list-style-type: none"> <li>• <a href="#">EFT Deployment Guide for Cisco Tunnel Control Protocol on Cisco EasyVPN</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Dead peer detection                                                                                      | <ul style="list-style-type: none"> <li>• <a href="#">IPSec Dead Peer Detection Periodic Message Option</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| DHCP, configuring                                                                                        | <ul style="list-style-type: none"> <li>• “Configuring the Cisco IOS DHCP Client” in the <a href="#">Cisco IOS IP Addressing Configuration Guide</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Digital certificates (RSA signature support)                                                             | <ul style="list-style-type: none"> <li>• <a href="#">Easy VPN Remote RSA Signature Support</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| DNS, configuring                                                                                         | <ul style="list-style-type: none"> <li>• <a href="#">Configuring DNS on Cisco Routers</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Easy VPN Server feature, which provides Cisco Unity client support for the Cisco Easy VPN Remote feature | <ul style="list-style-type: none"> <li>• <a href="#">Easy VPN Server</a></li> <li>• <a href="#">Cisco Easy VPN</a></li> <li>• <a href="#">Configuring NAC with IPsec Dynamic Virtual Tunnel Interface</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Encrypted Preshared Key feature                                                                          | <ul style="list-style-type: none"> <li>• <a href="#">Encrypted Preshared Key</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| IPsec and VPN, general information                                                                       | <ul style="list-style-type: none"> <li>• <a href="#">Deploying IPsec</a>—Provides an overview of IPsec encryption and its key concepts, along with sample configurations. Also provides a link to many other documents on related topics.</li> <li>• <a href="#">Configuring Authorization and Revocation of Certificates in a PKI</a>—Describes the concept of digital certificates and how they are used to authenticate IPsec users.</li> <li>• <a href="#">Configuring Authentication Proxy</a></li> <li>• <a href="#">An Introduction to IP Security (IPsec) Encryption</a>—Provides a step-by-step description of how to configure IPsec encryption.</li> <li>• <a href="#">Configuring VPN Settings</a>—Provides information about configuring a PIX firewall to operate as a Cisco Secure VPN client.</li> <li>• <a href="#">Configuring Security for VPNs with IPsec</a>—Provides information about configuring crypto maps.</li> <li>• <a href="#">IPsec Virtual Tunnel Interface</a>—Provides information about IPsec virtual tunnel interfaces.</li> <li>• IP technical tips sections on Cisco.com.</li> </ul> |
| Object tracking                                                                                          | <ul style="list-style-type: none"> <li>• <a href="#">Reliable Static Routing Backup Using Object Tracking</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Note** Additional documentation on IPsec becomes available on [Cisco.com](#) as new features and platforms are added. Cisco Press also publishes several books on IPsec—go to <http://www.ciscopress.com> for more information on Cisco Press books.

## Standards

| Standards                                                   | Title |
|-------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature. | —     |

## MIBs

| MIBs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | MIBs Link                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>CISCO-IPSEC-FLOW-MONITOR-MIB—Contains attributes describing IPsec-based VPNs (Internet Engineering Task Force (IETF) IPsec Working Group Draft).</li><li>CISCO-IPSEC-MIB—Describes Cisco implementation-specific attributes for Cisco routers implementing IPsec VPNs.</li><li>CISCO-IPSEC-POLICY-MAP-MIB—Extends the CISCO-IPSEC-FLOW-MONITOR-MIB to map dynamically created structures to the policies, transforms, cryptomaps, and other structures that created or are using them.</li></ul> | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                   | Title |
|--------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html)

For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **ctcp port**
- **clear crypto ipsec client ezvpn**
- **crypto ctp**
- **crypto ipsec client ezvpn (global)**
- **crypto ipsec client ezvpn (interface)**
- **crypto ipsec client ezvpn connect**
- **crypto ipsec client ezvpn xauth**
- **debug crypto ipsec client ezvpn**
- **debug ip auth-proxy ezvpn**
- **icmp-echo**
- **ip http ezvpn**
- **show crypto ipsec client ezvpn**
- **show tech-support**
- **type echo protocol ipIcmpEcho**
- **xauth userid mode**

# Feature Information for Easy VPN Remote

Table 4 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 4** Feature Information for Easy VPN Remote

| Feature Name    | Releases                                 | Feature Information                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Easy VPN Remote | 12.2(4)YA<br>Cisco IOS XE<br>Release 2.1 | Support for Cisco Easy VPN Remote (Phase I) of this feature was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.<br><br>In Cisco IOS XE Release 2.1, support for this feature was introduced on Cisco ASR 1000 Series Routers.                                           |
|                 | 12.2(13)T                                | Cisco Easy VPN Remote was integrated into Cisco IOS Release 12.2(13)T.                                                                                                                                                                                                                                                                                                            |
|                 | 12.2(8)YJ                                | Support for Cisco Easy VPN Remote (Phase II) of this feature was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.                                                                                                                                                        |
|                 | 12.2(15)T                                | The Cisco Easy VPN Remote (Phase II) feature was integrated into Cisco IOS Release 12.2(15)T. Support for the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers was added.                                                                                                                                                                                      |
|                 | 12.3(2)T                                 | The Type 6 Password in the IOS Configuration feature was added.                                                                                                                                                                                                                                                                                                                   |
|                 | 12.3(4)T                                 | The Save Password and Multiple Peer Backup features were added.<br><br>The following sections provide information about the Save Password feature: <ul style="list-style-type: none"> <li>• <a href="#">Using Xauth, page 9</a></li> <li>• <a href="#">Configuring Save Password, page 39</a></li> <li>• <a href="#">Save Password Configuration: Example, page 78</a></li> </ul> |

**Table 4**      *Feature Information for Easy VPN Remote (continued)*

| Feature Name | Releases   | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | 12.3(7)T   | <p>The following feature was introduced in this release:</p> <ul style="list-style-type: none"> <li>• <a href="#">Dead Peer Detection Periodic Message Option, page 24</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|              | 12.3(7)XR  | <p>The following features were introduced: Dead Peer Detection with Stateless Failover (Object Tracking with Easy VPN)—Backup Server List Local Configuration and Backup Server List Auto Configuration, Management Enhancements, Load Balancing, VLAN Support, Multiple Subnet Support, Traffic-Triggered Activation, Perfect Forward Secrecy (PFS) Via Policy Push, 802.1x Authentication, Certificate (PKI) Support, Easy VPN Remote and Server on the Same Interface, and Easy VPN Remote and Site to Site on the Same Interface.</p> <p>The following sections provide information about these features:</p> <ul style="list-style-type: none"> <li>• <a href="#">802.1x Authentication, page 16</a></li> <li>• <a href="#">Traffic-Triggered Activation, page 17</a></li> <li>• <a href="#">Backup Server List Local Configuration, page 18</a></li> <li>• <a href="#">Backup Server List Auto Configuration, page 18</a></li> <li>• <a href="#">VLAN Support, page 21</a></li> <li>• <a href="#">Easy VPN Remote and Server on the Same Interface, page 23</a></li> <li>• <a href="#">Easy VPN Remote and Site to Site on the Same Interface, page 23</a></li> <li>• <a href="#">Load Balancing, page 24</a></li> <li>• <a href="#">Management Enhancements, page 25</a></li> <li>• <a href="#">PFS Support, page 25</a></li> </ul> <p><b>Note</b> Cisco 800 series routers are not supported in Cisco IOS Release 12.3(7)XR.</p> <p><b>Note</b> These features are available only in Cisco Release 12.3(7)XR2.</p> |
|              | 12.3(7)XR2 | <p>The features in Cisco IOS Release 12.3(7)XR were introduced on Cisco 800 series routers.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|              | 12.3(8)YH  | <p>The Dial Backup, Traffic-Triggered Activation, and Web-Based Activation features were introduced on the Cisco 1812 router.</p> <p>The following sections provide information about these features:</p> <ul style="list-style-type: none"> <li>• <a href="#">Dial Backup, page 25</a></li> <li>• <a href="#">Dial Backup: Examples, page 79</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Table 4**      *Feature Information for Easy VPN Remote (continued)*

| Feature Name | Releases                | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | 12.3(11)T               | Except for the Dial Backup and Traffic-Triggered Activation features, all features introduced in Cisco IOS Releases 12.3(7)XR and 12.3(7)XR2 were integrated into Cisco IOS Release 12.3(11)T.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|              | 12.3(14)T               | Dial Backup and Traffic-Triggered Activation features were integrated into Cisco IOS Release 12.3(14)T. In addition, the Web-Based Activation feature was integrated into this release.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|              | 12.3(8)YI               | The Dial Backup, Traffic-Triggered Activation, and Web-Based Activation features were introduced on the Cisco 1800 series fixed configuration routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|              | 12.3(8)YI1              | The Dial Backup, Traffic-Triggered Activation, and Web-Based Activation features were introduced on the Cisco 870 series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|              | 12.4(2)T<br>12.2(33)SXH | <p>The following features were added in this release: Banner, Auto-Update, and Browser-Proxy Enhancements.</p> <p>The following section provides information about these features:</p> <ul style="list-style-type: none"> <li>• <a href="#">Banner, page 32</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|              | 12.4(4)T<br>12.2(33)SXH | <p>The following features were added in this release: Dual Tunnel Support, Configuration Management Enhancements (Pushing a Configuration URL Through a Mode-Configuration Exchange), Reactivate Primary Peer, and Virtual IPsec Interface Support. In addition, the <b>flow allow acl</b> subcommand was added so that traffic can be blocked when a tunnel is down.</p> <p>The following sections provide information about these features:</p> <ul style="list-style-type: none"> <li>• <a href="#">Virtual IPsec Interface Support, page 27</a></li> <li>• <a href="#">Dual Tunnel Support, page 29</a></li> <li>• <a href="#">Configuration Management Enhancements (Pushing a Configuration URL Through a Mode-Configuration Exchange), page 33</a></li> <li>• <a href="#">Reactivate Primary Peer, page 33</a></li> <li>• <a href="#">Restricting Traffic When a Tunnel Is Down, page 57</a></li> </ul> |
|              | 12.2(33)SRA             | Cisco Easy VPN Remote was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|              | 12.4(11)T               | <p>The following feature was added in this release:</p> <ul style="list-style-type: none"> <li>• Identical Addressing Support</li> </ul> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>– <a href="#">Identical Addressing Support, page 33</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Table 4**      *Feature Information for Easy VPN Remote (continued)*

| Feature Name | Releases  | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | 12.4(20)T | <p>The following features were added in this release:</p> <ul style="list-style-type: none"> <li>• cTCP Support on Easy VPN Clients</li> </ul> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>– <a href="#">cTCP Support on Easy VPN Clients, page 34</a></li> <li>– <a href="#">Configuring cTCP on an Easy VPN Client, page 56</a></li> <li>– <a href="#">cTCP on an Easy VPN Client (Remote Device): Examples, page 96</a></li> </ul> <p>The following commands were introduced or modified for this feature: <b>crypto ctcp</b>, <b>ctcp port</b></p> |



# Glossary

**AAA**—authentication, authorization, and accounting. Framework of security services that provide the method for identifying users (authentication); for remote access control (authorization); and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

**aggressive mode**—Mode that eliminates several steps during Internet Key Exchange (IKE) authentication negotiation between two or more IPsec peers. Aggressive mode is faster than main mode but is not as secure.

**authorization**—Method for remote access control, including one-time authorization or authorization for each service; per-user account list and profile; user group support; and support of IP, IPX, ARA, and Telnet. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the actual capabilities and restrictions of the user. The database can be located locally on the access server or router, or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. All authorization methods must be defined through AAA.

**CA**—certificate authority. An entity in a network that issues and manages security credentials and public keys (in the form of X509v3 certificates) for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the information of the requestor, the CA can then issue a certificate. Certificates generally include the public key of the owner, the expiration date of the certificate, the name of the owner, and other information about the public key owner.

**CRWS**—Cisco Router Web Setup Tool. Tool that provides web interface capabilities.

**cTCP**—Cisco Tunneling Control Protocol. When cTCP is enabled on a remote device (client) and headend device, IKE and ESP (Protocol 50) traffic is encapsulated in the TCP header so that the firewalls in between the client and the headend device permits this traffic (considering it the same as TCP traffic).

**DPD**—dead peer detection. Queries the liveliness of the Internet Key Exchange (IKE) peer of a router at regular intervals.

**DSLAM**—digital subscriber line access multiplexer. A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines.

**IKE**—Internet Key Exchange. Key management protocol standard that is used in conjunction with the IP Security (IPsec) standard. IPsec is an IP security feature that provides robust authentication and encryption of IP packets. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.

**IPsec**—IP Security Protocol. Framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

**main mode**—Mode that ensures the highest level of security when two or more IPsec peers are negotiating IKE authentication. It requires more processing time than aggressive mode.

**MIB**—Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as Simple Network Management Protocol (SNMP) or Common Management Information Protocol (CMIP). The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a graphical user interface (GUI) network management system (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**peer**—Router or device that participates as an endpoint in IPsec and IKE.

**preshared key**—Shared, secret key that uses IKE for authentication.

**QoS**—quality of service. Capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay; Asynchronous Transfer Mode (ATM); Ethernet; and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies.

**RADIUS**—Remote Authentication Dial-In User Service. Distributed client or server system that secures networks against unauthorized access. RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

**SA**—security association. Instance of security policy and keying material applied to a data flow. Both IKE and IPsec use SAs, although SAs are independent of one another. IPsec SAs are unidirectional, and they are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPsec SA, it is bi-directional. IKE negotiates and establishes SAs on behalf of IPsec. A user can also establish IPsec SAs manually.

A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports encapsulating security payload (ESP) between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPsec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

**SDM**—Security Device Manager. Web interface manager that enables you to connect or disconnect a VPN tunnel and that provides a web interface for extended authentication (Xauth).

**SNMP**—Simple Network Management Protocol. Application-layer protocol that provides a message format for communication between SNMP managers and agents.

**trap**—Message sent by an SNMP agent to a network management system, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

**VPN**—virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunnels to encrypt all information at the IP level.



#### Note

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

---

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.





# Easy VPN Remote RSA Signature Support

---

**First Published: March 1, 2004**

**Last Updated: August 21, 2007**

The Easy VPN Remote RSA Signature Support feature provides for the support of Rivest, Shamir, and Adelman (RSA) signatures on Easy VPN remote devices. The support is provided through RSA certificates that can be stored on or off the remote device.

## **Finding Feature Information in This Module**

*Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Easy VPN Remote RSA Signature Support](#)” section on page 6.*

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Easy VPN Remote RSA Signature Support, page 1](#)
- [Restrictions for Easy VPN Remote RSA Signature Support, page 2](#)
- [Information About Easy VPN Remote RSA Signature Support, page 2](#)
- [How to Configure Easy VPN Remote RSA Signature Support, page 2](#)
- [Additional References, page 3](#)

## Prerequisites for Easy VPN Remote RSA Signature Support

- You must have a Cisco Virtual Private Network (VPN) remote device and be familiar with configuring the device.



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- You must have a certification authority (CA) available to your network before you configure this interoperability feature. The CA must support the public key infrastructure (PKI) protocol of Cisco Systems, which is the Simple Certificate Enrollment Protocol (SCEP) (formerly called certificate enrollment protocol [CEP]).
- You should be familiar with IP Security (IPSec) and PKI.
- You should be familiar with configuring RSA key pairs.
- You should be familiar with configuring CAs.

## Restrictions for Easy VPN Remote RSA Signature Support

- This feature should be configured only when you also configure both IPSec and Internet Key Exchange (IKE) in your network.
- The Cisco IOS software does not support CA server public keys greater than 2048 bits.

## Information About Easy VPN Remote RSA Signature Support

To configure the Easy VPN Remote RSA Signature Support feature, you should understand the following concept:

- [Easy VPN Remote RSA Signature Support Overview, page 2](#)

## Easy VPN Remote RSA Signature Support Overview

The Easy VPN Remote RSA Signature Support feature allows you to configure RSA signatures on your Easy VPN remote device. The signatures can be stored on or off your remote device.

## How to Configure Easy VPN Remote RSA Signature Support

This section contains the following procedure:

- [Configuring Easy VPN Remote RSA Signature Support, page 2](#)

## Configuring Easy VPN Remote RSA Signature Support

The RSA signatures for an Easy VPN remote device are configured the same way that you would configure RSA signatures for any other Cisco device. (For information about configuring RSA signatures, refer to the “Configuring Certification Authority Interoperability” chapter of the “IP Security and Encryption” section of the *Cisco IOS Security Configuration Guide*, Release 12.4.)

To enable the RSA signatures, when you are configuring the Easy VPN remote and assigning the configuration to the outgoing interface, you must omit the **group** command. The content of the first Organizational Unit (OU) field will be used as the group. (For information about configuring Cisco Easy VPN remote devices, refer to the feature document “[Cisco Easy VPN Remote](#),” Release 12.4(11)T.)

To troubleshoot your Easy VPN remote RSA signature configuration, you can use the following **debug** commands. The **debug** commands can be used in any order or individually.

## SUMMARY STEPS

1. `enable`
2. `debug crypto ipsec client ezvpn`
3. `debug crypto isakmp`

## DETAILED STEPS

|        | Command or Action                                                                                                           | Purpose                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <code>debug crypto ipsec client ezvpn</code><br><br><b>Example:</b><br>Router# <code>debug crypto ipsec client ezvpn</code> | Displays information about the VPN tunnel as it relates to the Easy VPN remote configuration.                    |
| Step 3 | <code>debug crypto isakmp</code><br><br><b>Example:</b><br>Router# <code>debug crypto isakmp</code>                         | Displays messages about IKE events.                                                                              |

## Additional References

The following sections provide references related to Easy VPN Remote RSA Signature Support.

## Related Documents

| Related Topic                                    | Document Title                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring Internet Key Exchange for IPSec VPNs | <a href="#">Configuring Internet Key Exchange for IPsec VPNs</a>                                                                                                                                                                                                                                           |
| Deploying RSA keys                               | <a href="#">Deploying RSA Keys Within a PKI</a>                                                                                                                                                                                                                                                            |
| Certificate Authorities                          | <ul style="list-style-type: none"> <li>• <a href="#">Easy VPN Server</a></li> <li>• <a href="#">Cisco IOS PKI Overview: Understanding and Planning a PKI</a></li> <li>• <a href="#">Deploying RSA Keys Within a PKI</a></li> <li>• <a href="#">Configuring Certificate Enrollment for a PKI</a></li> </ul> |
| Configuring a Cisco Easy VPN remote device       | <a href="#">Cisco Easy VPN Remote</a>                                                                                                                                                                                                                                                                      |
| Security commands                                | <a href="#">Cisco IOS Security Command Reference</a>                                                                                                                                                                                                                                                       |

## Standards

| Standards                                                            | Title |
|----------------------------------------------------------------------|-------|
| There are no new or modified standards associated with this feature. | —     |

## MIBs

| MIBs                                                            | MIBs Link                                                                                                                                                                                                                         |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| There are no new or modified MIBs associated with this feature. | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFCs                                                            | Title |
|-----------------------------------------------------------------|-------|
| There are no new or modified RFCs associated with this feature. | —     |



## Technical Assistance

| Description                                                                                                                                                                                                                                                                                    | Link                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Technical Support &amp; Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for Easy VPN Remote RSA Signature Support

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Easy VPN Remote RSA Signature Support

| Feature Name                            | Releases                                | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Easy VPN Remote RSA Signature Support   | 12.3(7)T1<br>12.2(33)SRA<br>12.2(33)SXH | The Easy VPN Remote RSA Signature Support feature provides for the support of Rivest, Shamir, and Adelman (RSA) signatures on Easy VPN remote devices. The support is provided through RSA certificates that can be stored on or off the remote device.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>“Easy VPN Remote RSA Signature Support Overview” section on page 2</li> <li>“Configuring Easy VPN Remote RSA Signature Support” section on page 2</li> </ul> |
| Easy VPN Client RSA - Signature Support | Cisco IOS XE Release 2.1                | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

---

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

---

© 2009 Cisco Systems, Inc. All rights reserved.





# Easy VPN Server

---

**First Published: February 25, 2002**

**Last Updated: November 4, 2008**

The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x and later software clients and Cisco VPN hardware clients (such as the Cisco 800, Cisco 900, Cisco 1700, VPN 3002, and PIX 501 devices). This feature allows a remote end user to communicate using IP Security (IPsec) with any Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPsec policies are “pushed” to the client device by the server, minimizing configuration by the end user.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Easy VPN Server](#)” section on [page 75](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Restrictions for Easy VPN Server, page 2](#)
- [Information About Easy VPN Server, page 3](#)
- [How to Configure Easy VPN Server, page 19](#)
- [Configuration Examples for Easy VPN Server, page 53](#)
- [Additional References, page 71](#)
- [Command Reference, page 73](#)
- [Feature Information for Easy VPN Server, page 75](#)
- [Glossary, page 79](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2008 Cisco Systems, Inc. All rights reserved.

# Restrictions for Easy VPN Server

## Nonsupported Protocols

Table 1 outlines IPsec protocol options and attributes that currently are *not* supported by Cisco VPN clients, so these options and attributes should not be configured on the router for these clients.

**Table 1** *Nonsupported IPsec Protocol Options and Attributes*

| Options                     | Attributes                                                                    |
|-----------------------------|-------------------------------------------------------------------------------|
| Authentication Types        | Authentication with public key encryption<br>Digital Signature Standard (DSS) |
| Diffie-Hellman (D-H) groups | 1                                                                             |
| IPsec Protocol Identifier   | IPSEC_AH                                                                      |
| IPsec Protocol Mode         | Transport mode                                                                |
| Miscellaneous               | Manual keys<br>Perfect Forward Secrecy (PFS)                                  |

## Cisco Secure VPN Client 1.x Restrictions

When used with this feature, the Cisco Secure VPN Client 1.x has the following restrictions:

- It does not support dead peer detection (DPD) or any other keepalive scheme.
- It does not support initial contact.

This feature cannot use per-group attribute policy profiles such as IP addresses, and Domain Name Service (DNS). Thus, customers must continue to use existing, globally defined parameters for IP address assignment, Windows Internet Naming Service (WINS) and DNS, and preshared keys.

## Multicast and Static NAT

Multicast and static NAT are supported only for Easy VPN servers using dynamic virtual tunnel interfaces (DVTIs).

## Virtual IPsec Interface Restrictions

The Virtual IPsec Interface Support feature works only with a Cisco software VPN Client that is version 4.x or later, and an Easy VPN remote device that is configured to use a virtual interface.

## cTCP Restrictions

- If a port is being used for Cisco Tunnel Control Protocol (cTCP), it cannot be used for other applications.
- cTCP can be used on only ten ports at a time.
- cTCP is supported on only Cisco IOS Easy VPN servers.
- If a cTCP connection is set up on a port, cTCP cannot be disabled on that port because doing so would cause the existing connection to stop receiving traffic.
- High Availability of cTCP is not currently supported on the Easy VPN server.

# Information About Easy VPN Server

Before using the Easy VPN Server Enhancements feature, you should understand the following concepts:

- [How It Works, page 3](#)
- [RADIUS Support for Group Profiles, page 4](#)
- [RADIUS Support for User Profiles, page 7](#)
- [Supported Protocols, page 8](#)
- [Functions Supported by Easy VPN Server, page 9](#)

## How It Works

When the client initiates a connection with a Cisco IOS VPN device, the “conversation” that occurs between the peers consists of device authentication via Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (Xauth), VPN policy push (using Mode Configuration), and IPsec security association (SA) creation. An overview of this process is as follows:

- The client initiates IKE Phase 1 via aggressive mode (AM) if a preshared key is to be used for authentication; the client initiates main mode (MM) if digital certificates are used. If the client identifies itself with a preshared key, the accompanying group name entered in the configuration GUI (ID\_KEY\_ID) is used to identify the group profile associated with this client. If digital certificates are used, the organizational unit (OU) field of a distinguished name (DN) is used to identify the group profile.

**Note**

Because the client may be configured for preshared key authentication, which initiates IKE AM, it is recommended that the administrator change the identity of the Cisco IOS VPN device via the **crypto isakmp identity hostname** command. This will not affect certificate authentication via IKE MM.

- The client attempts to establish an IKE SA between its public IP address and the public IP address of the Cisco IOS VPN device. To reduce the amount of manual configuration on the client, every combination of encryption and hash algorithms, in addition to authentication methods and D-H group sizes, is proposed.
- Depending on its IKE policy configuration, the Cisco IOS VPN device will determine which proposal is acceptable to continue negotiating Phase 1.

**Tip**

IKE policy is global for the Cisco IOS VPN device and can consist of several proposals. In the case of multiple proposals, the Cisco IOS VPN device will use the first match, so you should always list your most secure policies first.

**Note**

Device authentication ends and user authentication begins at this point.

- After the IKE SA is successfully established, and if the Cisco IOS VPN device is configured for Xauth, the client waits for a “username/password” challenge and then responds to the challenge of the peer. The information that is entered is checked against authentication entities using

authentication, authorization, and accounting (AAA) protocols such as RADIUS and TACACS+. Token cards may also be used via AAA proxy. During Xauth, it is also possible for a user-specific attribute to be retrieved if the credentials of that user are validated via RADIUS.



**Note** VPN devices that are configured to handle remote clients should always be configured to enforce user authentication.

- If the Cisco IOS VPN device indicates that authentication was successful, the client requests further configuration parameters from the peer. The remaining system parameters (for example, IP address, DNS, and split tunnel attributes) are pushed to the client at this time using Mode Configuration.



**Note** The IP address pool and group preshared key (if Rivest, Shamir, and Adelman [RSA] signatures are not being used) are the only required parameter in a group profile, all other parameters are optional.

- After each client is assigned an internal IP address via Mode Configuration, it is important that the Cisco IOS VPN device knows how to route packets through the appropriate VPN tunnel. Reverse route injection (RRI) will ensure that a static route is created on the Cisco IOS VPN device for each client internal IP address.



**Note** It is recommended that you enable RRI on the crypto map (static or dynamic) for the support of VPN clients unless the crypto map is being applied to a Generic Routing Encapsulation (GRE) tunnel that is already being used to distribute routing information.

- After the configuration parameters have been successfully received by the client, IKE quick mode is initiated to negotiate IPsec SA establishment.
- After IPsec SAs are created, the connection is complete.

## RADIUS Support for Group Profiles

Group policy information is stored in a profile that can be defined locally in the router configuration or on a RADIUS server that is accessible by the Cisco IOS VPN device. If RADIUS is used, you must configure access to the server and allow the Cisco IOS VPN device to send requests to the server.

To define group policy attributes for RADIUS, you must do the following task on your RADIUS server:

- Define a user that has a name equal to the group name as defined in the client graphical user interface (GUI). For example, if users will be connecting to the Cisco IOS VPN device using the group name “sales,” you will need a user whose name is “sales.” The password for this user is “cisco,” which is a special identifier that is used by the router for RADIUS purposes. The username must then be made a member of a group in which the correct policy is defined. For simplicity, it is recommended that the group name be the same as the username.

## For a Cisco Secure Access Control Server

If you are using a Cisco Secure access control server (ACS), you may configure your remote access VPN group profiles on this server. To perform this task, you must ensure that Internet Engineering Task Force (IETF) RADIUS attributes are selected for group configuration as shown in [Figure 1](#). (This figure also



shows the compulsory attributes required for a remote access VPN group.) All values must be entered except the Tunnel-Password attribute, which is actually the preshared key for IKE purposes; if digital certificates are preferred, this attribute may be omitted.

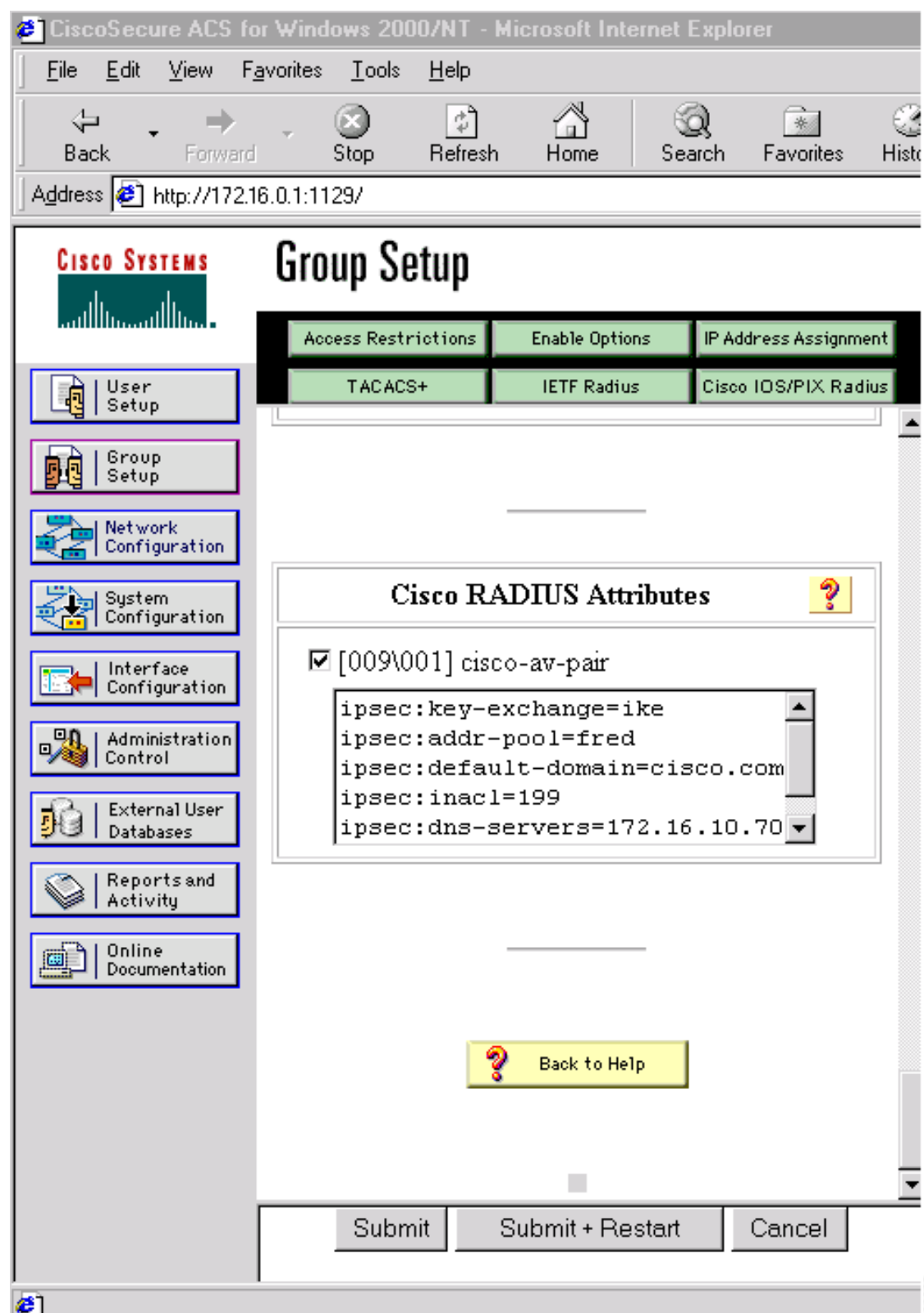
**Figure 1** IETF RADIUS Attributes Selection for Group Configuration

The screenshot displays the Cisco Systems Group Setup web interface. On the left is a navigation menu with icons and labels for: User Setup, Group Setup (highlighted), Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "Group Setup" and contains a tabbed interface with three tabs: "Access Restrictions", "Enable Options", and "IP Address Assignment". The "Enable Options" tab is active, showing a sub-tabbed interface with "TACACS+", "IETF Radius" (selected), and "Cisco IOS/PIX Radius". Below these tabs is the "IETF RADIUS Attributes" section, which includes a list of attributes with checkboxes and input fields:

- ☒ [006] Service-Type: Outbound (dropdown)
- ☐ [027] Session-Timeout: 0 (text input)
- ☐ [028] Idle-Timeout: 0 (text input)
- ☒ [064] Tunnel-Type:
  - Tag 1: 1 (dropdown), Value: IP ESP (dropdown)
  - Tag 2: 2 (dropdown), Value: (dropdown)
- ☐ [065] Tunnel-Medium-Type:
  - Tag 1: 1 (dropdown), Value: (dropdown)
  - Tag 2: 2 (dropdown), Value: (dropdown)
- ☒ [069] Tunnel-Password:
  - Tag 1: 1 (dropdown), Value: cisco (text input)
  - Tag 2: 2 (dropdown), Value: (text input)

At the bottom of the form are three buttons: "Submit", "Submit + Restart", and "Cancel".

In addition to the compulsory attributes shown in [Figure 1](#), other values can be entered that represent the group policy that is pushed to the remote client via Mode Configuration. [Figure 2](#) shows an example of a group policy. All attributes are optional except the addr-pool, key-exchange=preshared-key, and key-exchange=ike attributes. The values of the attributes are the same as the setting that is used if the policy is defined locally on the router rather than in a RADIUS server. (These values are explained in the section “[Defining Group Policy Information for Mode Configuration Push](#)” later in this document.)

**Figure 2** CiscoSecure ACS Group Policy Setup

After the group profile is created, a user who is a member of the group should be added. (Remember that the username that is defined maps to the group name as defined on the remote client, and the password defined for the username in the RADIUS database must be “cisco.”) If digital certificates are the preferred method of IKE authentication, the username should reflect the OU field in the certificate presented by the remote client.

## For All Other RADIUS Servers

Ensure that your RADIUS server allows you to define attribute-value (AV) pairs. (For an example, see the section “[Configuring Cisco IOS for Easy VPN Server: Example](#)” later in this document).

**Note**

If digital certificates are used, the username defined in RADIUS must be equal to the OU field of the DN of the certificate of the client.

## RADIUS Support for User Profiles

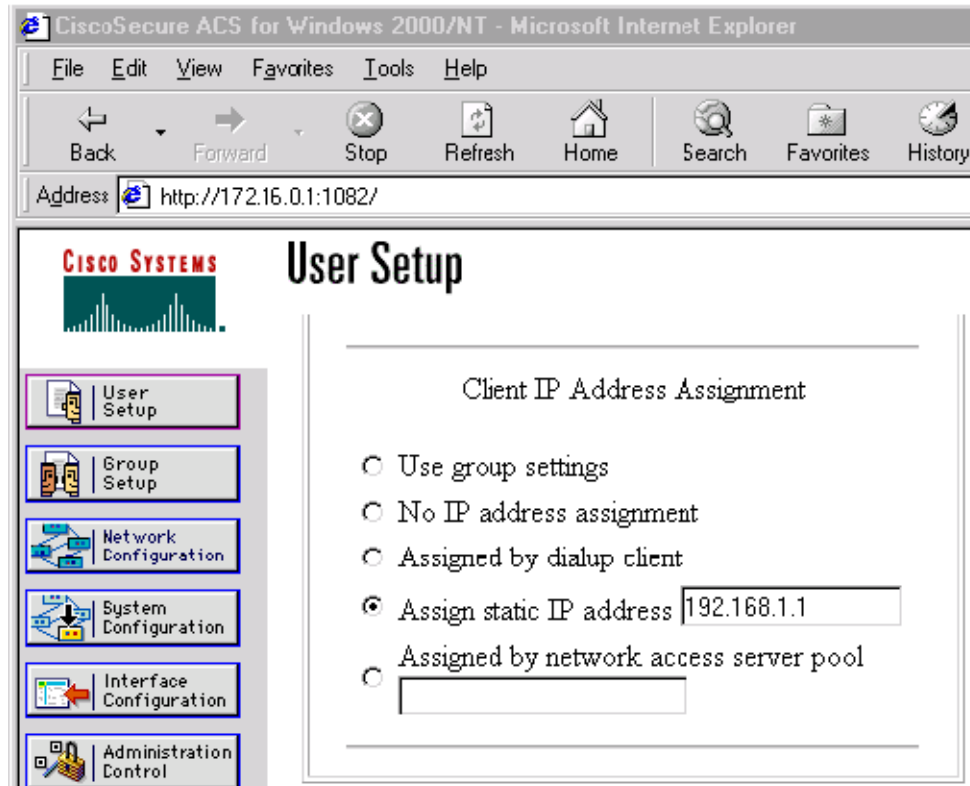
Attributes may also be applied on a per-user basis. If you apply attributes on a per-user basis, you can override a group attribute value with an individual user attribute. The attributes are retrieved at the time that user authentication via Xauth occurs. The attributes are then combined with group attributes and applied during Mode Configuration.

User-based attributes are available only if RADIUS is being used for user authentication.

To define user policy attributes for RADIUS, you must do the following task on your RADIUS server:

- Define a user or add attributes to the existing profile of a user in your RADIUS database. The password for the user will be used during Xauth user authentication, or you may proxy to a third-party server, such as a token card server.

[Figure 3](#) shows how CiscoSecure ACS may be used for user authentication and for the assignment of a Framed-IP-Address attribute that may be pushed to the client. The presence of this attribute means that the local address pool defined for the group to which that user belongs will be overridden.

**Figure 3** CiscoSecure ACS User Profile Setup

## For All Other RADIUS Servers

Ensure that your RADIUS server allows you to define AV pairs. (For an example, see the [“Configuring Cisco IOS for Easy VPN Server: Example”](#) section later in this document.)

## Supported Protocols

[Table 2](#) outlines supported IPsec protocol options and attributes that can be configured for this feature. (See [Table 1](#) for nonsupported options and attributes.)

**Table 2** Supported IPsec Protocol Options and Attributes

| Options                   | Attributes                                                                                                                                                               |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Algorithms | <ul style="list-style-type: none"> <li>Hashed Message Authentication Codes with Message Digest 5 (HMAC-MD5)</li> <li>HMAC-Secure Hash Algorithm 1 (HMAC-SHA1)</li> </ul> |
| Authentication Types      | <ul style="list-style-type: none"> <li>Preshared keys</li> <li>RSA digital signatures</li> </ul>                                                                         |

**Table 2**      **Supported IPsec Protocol Options and Attributes (continued)**

| Options                       | Attributes                                                                                                                           |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| D-H groups                    | <ul style="list-style-type: none"> <li>• 2</li> <li>• 5</li> </ul>                                                                   |
| Encryption Algorithms (IKE)   | <ul style="list-style-type: none"> <li>• Data Encryption Standard (DES)</li> <li>• Triple Data Encryption Standard (3DES)</li> </ul> |
| Encryption Algorithms (IPsec) | <ul style="list-style-type: none"> <li>• DES</li> <li>• 3DES</li> <li>• NULL</li> </ul>                                              |
| IPsec Protocol Identifiers    | <ul style="list-style-type: none"> <li>• Encapsulating Security Payload (ESP)</li> <li>• IP LZS compression (IPCOMP-LZS)</li> </ul>  |
| IPsec Protocol Mode           | Tunnel mode                                                                                                                          |

## Functions Supported by Easy VPN Server

- [Mode Configuration Version 6 Support, page 10](#)
- [Xauth Version 6 Support, page 10](#)
- [IKE DPD, page 10](#)
- [Split Tunneling Control, page 10](#)
- [Initial Contact, page 10](#)
- [Group-Based Policy Control, page 11](#)
- [User-Based Policy Control, page 11](#)
- [Session Monitoring for VPN Group Access, page 12](#)
- [Virtual IPsec Interface Support on a Server, page 13](#)
- [Virtual Tunnel Interface Per-User Attribute Support, page 13](#)
- [Banner, Auto-Update, and Browser Proxy, page 13](#)
- [Configuration Management Enhancements, page 14](#)
- [Per User AAA Policy Download with PKI, page 15](#)
- [Per-User Attribute Support for Easy VPN Servers, page 15](#)
- [Syslog Message Enhancements, page 16](#)
- [Network Admission Control Support for Easy VPN, page 16](#)
- [Central Policy Push Firewall Policy Push, page 17](#)
- [Password Aging, page 18](#)
- [Split DNS, page 18](#)
- [cTCP, page 18](#)
- [VRF Assignment by a AAA Server, page 19](#)

## Mode Configuration Version 6 Support

Mode Configuration version 6 is now supported for more attributes (as described in an IETF draft submission).

## Xauth Version 6 Support

Cisco IOS has been enhanced to support version 6 of Xauth. Xauth for user authentication is based on an IETF draft submission.

## IKE DPD

The client implements a new keepalives scheme—IKE DPD.

DPD allows two IPsec peers to determine whether the other is still “alive” during the lifetime of a VPN connection. DPD is useful because a host may reboot, or the dialup link of a remote user may disconnect without notifying the peer that the VPN connection has gone away. When an IPsec host determines that a VPN connection no longer exists, the host can notify a user, attempt to switch to another IPsec host, or clean up valuable resources that were allocated for the peer that no longer exists.

A Cisco IOS VPN device can be configured to send and reply to DPD messages. DPD messages are sent if no other traffic is being passed through the VPN tunnel. If a configured amount of time has lapsed since the last inbound data was received, DPD will send a message (“DPD R-U-THERE”) the next time it sends outbound IPsec data to the peer. DPD messages are unidirectional and are automatically sent by Cisco VPN clients. DPD *must* be configured on the router *only* if the router wishes to send DPD messages to the VPN client to determine the health of the client.

## Split Tunneling Control

Remote clients can support split tunneling, which enables a client to have intranet and Internet access at the same time. If split tunneling is not configured, the client will direct all traffic through the tunnel, even traffic destined for the Internet.



### Note

---

The split tunnel access control list (ACL) has a limit of 50 access control entries (ACE). If more than 50 ACEs are configured in a split tunnel ACL, only the first 50 ACEs are considered. These ACEs are sent to the client during mode configuration.

---

## Initial Contact

If a client is suddenly disconnected, the gateway may not be notified. Consequently, removal of connection information (IKE and IPsec SAs) for that client will not immediately occur. Thus, if the client attempts to reconnect to the gateway again, the gateway will refuse the connection because the previous connection information is still valid.

To avoid such a scenario, a new capability called initial contact has been introduced; it is supported by all Cisco VPN products. If a client or router is connecting to another Cisco gateway for the first time, an initial contact message is sent that tells the receiver to ignore and delete any old connection information that has been maintained for that newly connecting peer. Initial contact ensures that connection attempts are not refused because of SA synchronization problems, which are often identified via invalid security parameter index (SPI) messages and which require devices to have their connections cleared.

## Group-Based Policy Control

Policy attributes such as IP addresses, DNS, and split tunnel access can be provided on a per-group or per-user basis.

## User-Based Policy Control

Attributes may also be applied on a per-user basis. You can override a group attribute value with an individual user attribute. The attributes are retrieved at the time that user authentication via Xauth occurs. They are then combined with group attributes and applied during Mode Configuration.

From Cisco IOS Release 12.3(4)T forward, attributes can be applied on a per-user basis after the user has been authenticated. These attributes can override any similar group attributes. User-based attributes are available only if RADIUS is used as the database.

### Framed-IP-Address

To select the Framed-IP-Address attribute for CiscoSecure for NT, do the following: Under the user profile, choose the “use this IP address” option under addressing and manually enter the address. (You should check the method of configuring a framed IP address with your own RADIUS server because this procedure will vary.)

**Note**

If a framed IP address is present, and there is also a local pool address configured for the group that the user belongs to, the framed IP address will override the local pool setting.

### DHCP Client Proxy

Easy VPN servers currently assign an IP address to a remote device using either a local pool that is configured on the router or the framed IP address attribute that is defined in RADIUS. Effective with Cisco IOS Release 12.4(9)T, the DHCP Client Proxy feature provides the option of configuring an Easy VPN server to obtain an IP address from a DHCP server. The IP address is pushed to the remote device using mode configuration.

**Note**

This feature does not include functionality for the DHCP server to push the DNS, WINS server, or domain name to the remote client.

To configure DHCP Client Proxy, see the section [“Configuring an Easy VPN Server to Obtain an IP Address from a DHCP Server.”](#)

#### Benefits of DHCP Client Proxy

- The functionality provided with this feature helps in the creation of DDNS (dynamic Domain Name System) entries when a DNS server exists in conjunction with the DHCP server.
- The user is not restricted to IP address pools.

### User-Save-Password

As per the group description, the User-Save-Password attribute can be received in addition to the group variant (Save-Password), but if it is received, it will override the value asserted by the group.

The following is an output example of a RADIUS AV pair for the User-Save-Password attribute:

```
ipsec:user-save-password=1
```

## User-Include-Local-LAN

As per the group description, the User-Include-Local-LAN attribute can be received in addition to the group variant (Include-Local-LAN), but if it is received, it will override the value asserted by the group.

The following is an output example of a RADIUS AV pair for the User-Include-Local LAN attribute:

```
ipsec:user-include-local-lan=1
```

## User-VPN-Group

The User-VPN-Group attribute is a replacement for the [Group-Lock](#) attribute. It allows support for both preshared key and RSA signature authentication mechanisms such as certificates.

If you need to check that the group a user is attempting to connect to is indeed the group the user belongs to, use the User-VPN-Group attribute. The administrator sets this attribute to a string, which is the group that the user belongs to. The group the user belongs to is matched against the VPN group as defined by group name (ID\_KEY\_ID) for preshared keys or by the OU field of a certificate. If the groups do not match, the client connection is terminated.

This feature works only with AAA RADIUS. Local Xauth authentication must still use the Group-Lock attribute.

The following is an output example of a RADIUS AV pair for the Use-VPN-Group attribute:

```
ipsec:user-vpn-group=cisco
```

## Group-Lock

If you are only using pre-shared keys (no certificates or other RSA signature authentication mechanisms) with RADIUS or local AAA, you can continue to use the Group-Lock attribute. If you are only using pre-shared keys (no certificates or other RSA signature authentication mechanisms) with RADIUS, you can either continue to use the Group-Lock attribute or you can use the new [User-VPN-Group](#) attribute.



### Caution

Do not use the Group-Lock attribute if you are using RSA signature authentication mechanisms such as certificates. Use the [User-VPN-Group](#) attribute instead.

## Session Monitoring for VPN Group Access

It is possible to mimic the functionality provided by some RADIUS servers for limiting the maximum number of connections to a specific server group and also for limiting the number of simultaneous logins for users in that group. After user-defined thresholds are defined in each VPN group, connections will be denied until counts drop below these thresholds.

If you use a RADIUS server, such as CiscoSecure ACS, it is recommended that you enable this session control on the RADIUS server if the functionality is provided. In this way, usage can be controlled across a number of servers by one central repository. When enabling this feature on the router itself, only connections to groups on that specific device are monitored. Load-sharing scenarios are not accurately accounted for.

To configure session monitoring using command-line interface (CLI), use the **crypto isakmp client configuration group** command and the **max-users** and **max-logins** subcommands.

The following is an output example of RADIUS AV pairs that have been added to the relevant group:

```
ipsec:max-users=1000
```



```
ipsec:max-logins=1
```

## Virtual IPsec Interface Support on a Server

Virtual IPsec Interface Support on a Server allows you to selectively send traffic to different Easy VPN concentrators (servers) as well as to the Internet.

Before Cisco IOS Release 12.4(4)T, at the tunnel-up/tunnel-down transition, attributes that were pushed during the mode configuration had to be parsed and applied. When such attributes resulted in the configurations being applied on the interface, the existing configuration had to be overridden.

With the Virtual IPsec Interface Support feature, the tunnel-up configuration can be applied to separate interfaces, making it easier to support separate features at tunnel-up. Features that are applied to the traffic going into the tunnel can be separate from the features that are applied to traffic that is not going through the tunnel (for example, split-tunnel traffic and traffic leaving the device when the tunnel is not up). When the Easy VPN negotiation is successful, the line protocol state of the virtual-access interface gets changed to up. When the Easy VPN tunnel goes down because the SA expires or is deleted, the line protocol state of the virtual-access interfaces changes to down.



### Note

This feature does not support multicast.

For more information about this feature, see the document [Cisco Easy VPN Remote](#). (This feature is configured on the Easy VPN remote device.)

For information about the IPsec Virtual Tunnel Interface feature, see the document “IPSec Virtual Tunnel Interface” (link in the “[Related Documents](#)” section of this document).

## Virtual Tunnel Interface Per-User Attribute Support

Effective with Cisco IOS Release 12.4(9)T, Virtual Tunnel Interface provides per-user attribute support for Easy VPN servers.

For more information about this feature, see the document [IPsec Virtual Tunnel Interface](#).

## Banner, Auto-Update, and Browser Proxy

The following features provide support for attributes that aid in the management of the Cisco Easy VPN remote device.

### Banner

An Easy VPN server can be configured to push the banner to the Easy VPN remote device. A banner is needed for the web-based activation feature. The banner is displayed when the Easy VPN tunnel is up on the Easy VPN remote console or as a HTML page in the case of web-based activation.

### Auto-Update

An Easy VPN server can be configured to provide an automated mechanism for software and firmware upgrades on an Easy VPN remote device.

## Browser Proxy

An Easy VPN server can be configured so that an Easy VPN remote device can access resources on the corporate network. Using this feature, the user does not have to manually modify the proxy settings of his or her web browser when connecting to the corporate network using Cisco IOS VPN Client or manually revert the proxy settings upon disconnecting.

## Configuration Management Enhancements

### Pushing a Configuration URL Through a Mode-Configuration Exchange

When remote devices connect to a corporate gateway for creating an IPsec VPN tunnel, some policy and configuration information has to be applied to the remote device when the VPN tunnel is active to allow the remote device to become a part of the corporate VPN.

The Pushing a Configuration URL Through a Mode-Configuration Exchange feature provides for a mode-configuration attribute that “pushes” a URL from the concentrator (server) to the Cisco IOS Easy VPN remote device. The URL contains the configuration information that the remote device has to download and apply to the running configuration, and it contains the Cisco IOS CLI listing. (For more information about a Cisco IOS CLI listing, see Cisco IOS documentation for the **configuration url** command.) The CLI for this feature is configured on the concentrator.

The configuration that is pushed to the remote device is persistent by default. That is, the configuration is applied when the IPsec tunnel is “up,” but it is not withdrawn when the IPsec tunnel goes “down.” However, it is possible to write a section of configuration that is transient in nature, in which case the configuration of the section is reverted when the tunnel is disconnected.

There are no restrictions on where the configuration distribution server is physically located. However, it is recommended that a secure protocol such as HTTPS (Secure HTTP) be used to retrieve the configuration. The configuration server can be located in the corporate network, so because the transfer happens through the IPsec tunnel, insecure access protocols (HTTP) can be used.

Regarding backward compatibility: the remote device asks for the CONFIGURATION-URL and CONFIGURATION-VERSION attributes. Because the CONFIGURATION-URL and CONFIGURATION-VERSION attributes are not mandatory attributes, the server sends them only if it has them configured for the group. There is no built-in restriction to push the configuration, but bootstrap configurations (such as for the IP address) cannot be sent because those configurations are required to set up the Easy VPN tunnel, and the CONFIGURATION-URL comes into effect only after the Easy VPN tunnel comes up.

### After the Configuration Has Been Acquired by the Easy VPN Remote Device

After the configuration has been acquired by the Easy VPN remote device, the remote device sends a new ISAKMP notification to the Easy VPN server. The notification contains several manageability information messages about the client (remote device). The Easy VPN server takes two actions when this information is received:

- The Easy VPN server caches the information in its peer database. The information can be displayed by using the **show crypto isakmp peer config** command. This command output displays all manageability information that is sent by the client (remote device).
- If accounting is enabled, the Easy VPN server sends an accounting update record that contains the manageability information messages about the remote device to the accounting RADIUS server. This accounting update is later available in the accounting log of the RADIUS server.

## How to Configure This Feature

The commands that are used to configure this feature and the attributes CONFIGURATION-URL and CONFIGURATION-VERSION are described in the **crypto isakmp client configuration group** command documentation.

## Per User AAA Policy Download with PKI

With the Support of Per User AAA Policy Download with PKI feature, user attributes are obtained from the AAA server and pushed to the remote device through mode configuration. The username that is used to get the attributes is retrieved from the remote device certificate.

## Per-User Attribute Support for Easy VPN Servers

The Per-User Attribute Support for Easy VPN Servers feature provides users with the ability to support per-user attributes on Easy VPN servers. These attributes are applied on the virtual access interface.

### Local Easy VPN AAA Server

For a local Easy VPN AAA server, the per-user attributes can be applied at the group level or at the user level using the command-line interface (CLI).

To configure per-user attributes for a local Easy VPN server, see “[Configuring Per-User Attributes on a Local Easy VPN AAA Server](#).”

### Remote Easy VPN AAA Server

Attribute value (AV) pairs can be defined on a remote Easy VPN AAA server as shown in this example:

```
cisco-avpair = "ip:outacl#101=permit tcp any any established"
```

### Per-User Attributes

The following per-user attributes are currently defined in the AAA server and are applicable to IPsec:

- inacl
- interface-config
- outacl
- route
- rte-fltr-in
- rte-fltr-out
- sub-policy-In
- sub-policy-Out
- policy-route
- prefix

## Syslog Message Enhancements

Some new syslog messages have been added for Easy VPN in Cisco IOS Release 12.4(4)T. The syslog messages can be enabled on your server by using the command-line interface (CLI). The format of the syslog messages is as follows:

```
timestamp: %CRYPTO-6-VPN_TUNNEL_STATUS: (Server) <event message> User=<username>
Group=<groupname> Client_public_addr=<ip_addr> Server_public_addr=<ip_addr>
```

For an authentication-passed event, the syslog message looks like the following:

```
Jul 25 23:33:06.847: %CRYPTO-6-VPN_TUNNEL_STATUS: (Server) Authentication PASS
ED User=blue Group=Cisco1760group Client_public_addr=10.20.20.1
Server_public_addr=10.20.20.2
```

Three of the messages (Max users, Max logins, and Group does not exist) are authorization issues and are printed only with the group name in the format. The reason for only the group name being printed is that authorization check happens much before mode configuration happens. Therefore, the peer information is not yet present and cannot be printed. The following is an example of a “Group does not exist” message.

```
*Jun 30 18:02:58.107: %CRYPTO-6-VPN_TUNNEL_STATUS: Group: group_1 does not exist
```

## Easy VPN Syslog Messages That Are Supported

Both `ezvpn_connection_up` and `ezvpn_connection_down` were already supported in a previous release of syslog messages. The enhancements in Cisco IOS Release 12.4(4)T follow the same format, but new syslogs are introduced. The added syslogs are as follows:

- Authentication Passed
- Authentication Rejected
  - Group Lock Enabled
  - Incorrect Username or Password
  - Max Users exceeded/Max Logins exceeded
  - No. of Retries exceeded
- Authentication Failed (AAA Not Contactable)
- IP Pool Not present/No Free IP Address available in the pool
- ACL associated with Ezvpn policy but NOT defined (hence, no split tunneling possible)
- Save password Turned ON
- Incorrect firewall record being sent by Client (incorrect vendor | product | capability)
- Authentication Rejected
  - Access restricted via incoming interface
  - Group does not exist

## Network Admission Control Support for Easy VPN

Network Admission Control was introduced in Cisco IOS Release 12.3(8)T as a way to determine whether a PC client should be allowed to connect to the LAN. Network Admission Control uses Extensible Authentication Protocol over UDP (EAPoUDP) to query the Cisco trust agent on the PC and allows a PC to access the network if the client status is healthy. Different policies can be applied on the server to deny or limit access of PCs that are infected.

Effective with Cisco IOS Release 12.4(4)T, Network Admission Control can now be used to monitor the status of remote PC clients as well. After the Easy VPN tunnel comes up and the PC starts to send traffic, the traffic is intercepted at the Easy VPN server, and the posture validation process starts. The posture validation process consists of sending an EAPoUDP request over the Easy VPN tunnel and querying the Cisco trust agent. The authentication server is configured inside the trusted network, behind the IPsec aggregator.

The configuration of an Easy VPN server that has Network Admission Control enabled is shown in the output in [Network Admission Control: Example, page 64](#).

## Central Policy Push Firewall Policy Push

The Easy VPN server supports Central Policy Push (CPP) Firewall Policy Push. This feature allows administrators to push policies that enforce security to the Cisco Easy VPN (software) Client and related firewall software.

A split tunnel enables access to corporate networks, but it also allows a remote device to be exposed to attacks from the Internet. This feature enables the server to determine whether to allow or deny a tunnel if the remote device does not have a required firewall, thereby reducing exposure to attacks.

The following firewall types are supported:

- Cisco-Integrated-firewall (central-policy-push)
- Cisco-Security-Agent (check-presence)
- Zonelabs-Zonealarm (both)
- Zonelabs-ZonealarmPro (both)

The server can be used either to check the presence of a firewall on the client (remote device) using the check-presence option or to specify the specifics of the firewall policies that must be applied by the client using the central-policy-push.



### Note

The **policy check-presence command and keyword, which are used with this feature, replace the firewall are-u-there command functionality that was supported before Cisco IOS Release 12.4(6)T. The firewall are-u-there command will continue to be supported for backward compatibility.**

To enable this feature, see the sections “[Defining a CPP Firewall Policy Push Using a Local AAA Server](#)” and “[Applying a CPP Firewall Policy Push to the Configuration Group](#).”

## Syslog Support for CPP Firewall Policy Push

Syslog support can be enabled using the **crypto logging ezvpn** command on your router. CPP syslog messages will be printed for the following error conditions:

- If policy is configured on a group configuration (using the **firewall policy** command), but a global policy with the same name is not defined (using the **crypto isakmp client firewall** command). The syslog message is as follows:

```
Policy enabled on group configuration but not defined
```

Tunnel setup proceeds as normal (with the firewall).

- If an incorrect firewall request (vendor/product/cap incorrect order) is received, the syslog message is as follows:

```
Incorrect firewall record received from client
```

- If a policy mismatch occurs between the Cisco VPN Client and the server, the syslog is as follows:  
`CPP policy mismatch between client and headend`

## Password Aging

Prior to Cisco IOS Release 12.4(6)T, EasyVPN remote devices (clients) sent username and password values to the Easy VPN server, which in turn sent them to the AAA subsystem. The AAA subsystem generated an authentication request to the RADIUS server. If the password had expired, the RADIUS server replied with an authentication failure. The reason for the failure was not passed back to the AAA subsystem. The user was denied access due to authentication failure, but he or she did not know that the failure was due to password expiration.

Effective with Cisco IOS Release 12.4(6)T, if you have configured the Password Aging feature, the EasyVPN client is notified when a password has expired, and you are prompted to enter a new password. To configure the Password Aging feature, see the section “[Configuring Password Aging](#).”

For more information about Password Aging, see the reference for “Password Aging” in the section [Additional References](#) (subsection “Related Documents”).

## Split DNS

Effective with Cisco IOS Release 12.4(9)T, split DNS functionality is available on Easy VPN servers. This feature enables the Easy VPN hardware client to use primary and secondary DNS values to resolve DNS queries. These values are pushed by the Easy VPN server to the Easy VPN remote device. To configure this feature on your server, use the **split-dns** command (see the section “[Defining Group Policy Information for Mode Configuration Push](#)”). Configuring this command adds the split-dns attribute to the policy group. The attribute will include the list of domain names that you configured. All other names will be resolved using the public DNS server.

For more information about configuring split DNS, see “Configuring Split and Dynamic DNS on the Cisco VPN 3000” at the following URL:

[http://www.cisco.com/warp/public/471/dns\\_split\\_dynam.pdf](http://www.cisco.com/warp/public/471/dns_split_dynam.pdf)

## cTCP

The Cisco Tunneling Control Protocol (cTCP) feature can be used for situations in which an Easy VPN remote device is operating in an environment in which standard IPsec does not function or in which it does not function transparently without modification to existing firewall rules. These situations include the following:

- Small or home office router performing Network Address Translation (NAT) or Port Address Translation (PAT)
- PAT-provided IP address behind a larger router (for example, in a corporation)
- Non-NAT firewall (packet filtering or stateful)
- Proxy server

The firewall should be configured to allow the headend to accept cTCP connections on the configured cTCP port. This configuration is enabled on the Easy VPN server. If the firewall is not configured, it will not allow the cTCP traffic.

**Note**

cTCP traffic is actually Transmission Control Protocol (TCP) traffic. cTCP packets are IKE or Encapsulating Security Payload (ESP) packets that are being transmitted over TCP.

## VRF Assignment by a AAA Server

To assign VRF to Easy VPN users, the following attributes should be enabled on a AAA server:

```
Cisco-avpair "ip:interface-config=ip vrf forwarding example1"
Cisco-avpair "ip:interface-config=ip unnumbered loopback10"
```

# How to Configure Easy VPN Server

This section includes the following procedures:

- [Enabling Policy Lookup via AAA, page 20](#) (required)
- [Defining Group Policy Information for Mode Configuration Push, page 21](#) (required)
- [Enabling VPN Session Monitoring, page 24](#) (optional)
- [Verifying a VPN Session, page 25](#) (optional)
- [Applying Mode Configuration and Xauth, page 26](#) (required)
- [Enabling Reverse Route Injection for the Client, page 27](#) (optional)
- [Enabling IKE Dead Peer Detection, page 29](#) (optional)
- [Configuring RADIUS Server Support, page 29](#) (optional)
- [Verifying Easy VPN Server, page 30](#) (optional)
- [Configuring a Banner, page 31](#) (optional)
- [Configuring Auto Upgrade, page 31](#) (optional)
- [Configuring Browser Proxy, page 32](#) (optional)
- [Configuring the Pushing of a Configuration URL Through a Mode-Configuration Exchange, page 33](#) (optional)
- [Configuring Per User AAA Download with PKI—Configuring the Crypto PKI Trustpoint, page 34](#) (optional)
- [Configuring the Actual Per User AAA Download with PKI, page 36](#) (optional)
- [Configuring Per-User Attributes on a Local Easy VPN AAA Server, page 38](#)
- [Configuring Per-User Attributes on a Local Easy VPN AAA Server, page 38](#) (optional)
- [Defining a CPP Firewall Policy Push Using a Local AAA Server, page 40](#) (optional)
- [Applying a CPP Firewall Policy Push to the Configuration Group, page 41](#) (optional)
- [Defining a CPP Firewall Policy Push Using a Remote AAA Server, page 42](#) (optional)
- [Adding the VSA CPP-Policy Under the Group Definition, page 42](#) (optional)
- [Verifying CPP Firewall Policy Push, page 43](#) (optional)
- [Configuring Password Aging, page 43](#) (optional)
- [Configuring Split DNS, page 45](#) (optional)

- [Verifying Split DNS, page 46](#) (optional)
- [Monitoring and Maintaining Split DNS, page 47](#) (optional)
- [Configuring an Easy VPN Server to Obtain an IP Address from a DHCP Server, page 48](#) (optional)
- [Verifying DHCP Client Proxy, page 49](#) (optional)
- [Monitoring and Maintaining DHCP Client Proxy, page 50](#) (optional)
- [Configuring cTCP, page 50](#) (optional)
- [Verifying cTCP, page 51](#) (optional)
- [Monitoring and Maintaining a cTCP Configuration, page 51](#) (optional)
- [Troubleshooting a cTCP Configuration, page 53](#) (optional)

## Enabling Policy Lookup via AAA

To enable policy lookup via AAA, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication password-prompt** *text-string*
5. **aaa authentication username prompt** *text-string*
6. **aaa authentication login** [*list-name method1*] [*method2...*]
7. **aaa authorization network** *list-name* **local group radius**
8. **username** *name* **password** *encryption-type* *encrypted-password*

### DETAILED STEPS

|        | Command                                                                        | Purpose                                                                                                               |
|--------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                     |
| Step 3 | <b>aaa new-model</b><br><br><b>Example:</b><br>Router (config)# aaa new-model  | Enables AAA.                                                                                                          |



|        | Command                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>aaa authentication password-prompt</b><br><i>text-string</i><br><br><b>Example:</b><br>Router (config)# aaa authentication password-prompt "Enter your password now:"                       | (Optional) Changes the text displayed when users are prompted for a password.                                                                                                                                             |
| Step 5 | <b>aaa authentication username-prompt</b><br><i>text-string</i><br><br><b>Example:</b><br>Router (config)# aaa authentication username-prompt "Enter your name here:"                          | (Optional) Changes the text displayed when users are prompted to enter a username.                                                                                                                                        |
| Step 6 | <b>aaa authentication login</b> [ <i>list-name</i> <i>method1</i> ] [ <i>method2...</i> ]<br><br><b>Example:</b><br>Router (config)# aaa authentication login userlist local group radius      | Sets AAA authentication at login. <ul style="list-style-type: none"> <li>A local and RADIUS server may be used together and will be tried in order.</li> </ul> <b>Note</b> This command must be enabled to enforce Xauth. |
| Step 7 | <b>aaa authorization network</b> <i>list-name</i> <b>local</b><br><b>group</b> <b>radius</b><br><br><b>Example:</b><br>Router (config)# aaa authorization network grouplist local group radius | Enables group policy lookup. <ul style="list-style-type: none"> <li>A local and RADIUS server may be used together and will be tried in order.</li> </ul>                                                                 |
| Step 8 | <b>username</b> <i>name</i> <b>password</b> <i>encryption-type</i><br><i>encrypted-password</i><br><br><b>Example:</b><br>Router (config)# username server_r password 7 121F0A18               | (Optional) Defines local users for Xauth if RADIUS or TACACS+ is not used. <b>Note</b> Use this command only if no external validation repository will be used.                                                           |

## Defining Group Policy Information for Mode Configuration Push

Although users can belong to only one group per connection, they may belong to specific groups with different policy requirements. Thus, users may decide to connect to the client using a different group ID by changing their client profile on the VPN device. To define the policy attributes that are pushed to the client via Mode Configuration, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** {*group-name* | **default**}
4. **key** *name*
5. **dns** *primary-server* *secondary-server*
6. **wins** *primary-server* *secondary-server*

7. **domain** *name*
8. **pool** *name*
9. **netmask** *name*
10. **acl** *number*
11. **access-restrict** {*interface-name*}
12. **policy check-presence**  
or  
**firewall are-u-there**
13. **group-lock**
14. **include-local-lan**
15. **save-password**
16. **backup-gateway**
17. **pfs**

## DETAILED STEPS

|        | Command                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                            | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>crypto isakmp client configuration group</b> { <i>group-name</i>   <b>default</b> }<br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group group1 | Specifies the policy profile of the group that will be defined and enters Internet Security Association Key Management Protocol (ISAKMP) group configuration mode.<br><ul style="list-style-type: none"><li>If no specific group matches and a default group is defined, users will automatically be given the policy of a default group.</li></ul> |
| Step 4 | <b>key</b> <i>name</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# key group1                                                                                         | Specifies the IKE preshared key for group policy attribute definition.<br><b>Note</b> This command <i>must</i> be enabled if the client identifies itself with a preshared key.                                                                                                                                                                     |
| Step 5 | <b>dns</b> <i>primary-server secondary-server</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# dns 10.2.2.2 10.3.3.3                                                   | (Optional) Specifies the primary and secondary DNS servers for the group.                                                                                                                                                                                                                                                                           |

|         | Command                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <b>wins</b> <i>primary-server secondary-server</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# wins<br>10.10.10.10 10.12.12.12                                                                                        | (Optional) Specifies the primary and secondary WINS servers for the group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 7  | <b>domain</b> <i>name</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# domain<br>domain.com                                                                                                                            | (Optional) Specifies the DNS domain to which a group belongs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 8  | <b>pool</b> <i>name</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# pool green                                                                                                                                        | Defines a local pool address. <ul style="list-style-type: none"> <li>Although a user must define at least one pool name, a separate pool may be defined for each group policy.</li> </ul> <b>Note</b> This command <i>must</i> be defined and refer to a valid IP local pool address or the client connection will fail.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 9  | <b>netmask</b> <i>name</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# netmask<br>255.255.255.255                                                                                                                     | (Optional) Specifies that a subnet mask be downloaded to the client for local connectivity. <b>Note</b> Some VPN clients use the default mask for their particular classes of address. However, for a router, the host-based mask is typically used (/32). If you want to override the default mask, use the <b>netmask</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 10 | <b>acl</b> <i>number</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# acl 199                                                                                                                                          | (Optional) Configures split tunneling. <ul style="list-style-type: none"> <li>The <i>number</i> argument specifies a group of access control list (ACL) rules that represent protected subnets for split tunneling purposes.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 11 | <b>access-restrict</b> { <i>interface-name</i> }<br><br><b>Example:</b><br>Router (config-isakmp-group)#<br>access-restrict fastethernet0/0                                                                                       | Restricts clients in a group to an interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 12 | <b>policy check-presence</b><br><br>or<br><br><b>firewall are-u-there</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# policy<br>check-presence<br><br>or<br><br>Router (config-isakmp-group)# firewall<br>are-u-there | (Optional) Denotes that the server should check for the presence of the specified firewall (as shown as the firewall type on the client).<br><br>or<br><br>Adds the firewall are-u-there attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls. <b>Note</b> The <b>policy</b> command and <b>check-presence</b> keyword were added to Cisco IOS documentation in Cisco IOS 12.4(6)T. It is recommended that the <b>policy</b> command be used instead of the <b>firewall are-u-there</b> command because the <b>policy</b> command is supported in local AAA and remote AAA configurations. The <b>firewall are-u-there</b> command can be figured only locally, but it is still supported for backward compatibility. |

|         | Command                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 13 | <b>group-lock</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# group-lock               | Enforces the group lock feature.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 14 | <b>include-local-lan</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# include-local-lan | (Optional) Configures the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client.                                                                                                                                                                                                                                                                                                                                   |
| Step 15 | <b>save-password</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# save-password         | (Optional) Saves your Xauth password locally on your PC.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 16 | <b>backup-gateway</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# backup gateway       | (Optional) Rather than have backup gateways added to client configurations manually, it is possible to have the server “push down” a list of backup gateways to the client device. <ul style="list-style-type: none"> <li>These gateways are tried in order in the case of a failure of the previous gateway. The gateways may be specified using IP addresses or host names.</li> </ul>                                                                                                        |
| Step 17 | <b>pfs</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# pfs                             | (Optional) Notifies the client of the central-site policy regarding whether PFS is required for any IPsec SA. <ul style="list-style-type: none"> <li>Because the client device does not have a user interface option to enable or disable PFS negotiation, the server will notify the client device of the central site policy using this parameter. The Diffie-Hellman (D-H) group that is proposed for PFS will be the same that was negotiated in Phase 1 of the IKE negotiation.</li> </ul> |

## Enabling VPN Session Monitoring

If you wish to set restrictions on the maximum number of connections to the router per VPN group and the maximum number of simultaneous logins per user, add the following attributes to the VPN group.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **exit**
5. **max-logins** *number-of-logins*
6. **max-users** *number-of-users*

## DETAILED STEPS

|        | Command                                                                                                                                                            | Purpose                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                             | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                     | Enters global configuration mode.                                                                                                                                                                                                                    |
| Step 3 | <b>crypto isakmp client configuration group</b><br><i>group-name</i><br><br><b>Example:</b><br>Router (config)# crypto isakmp client<br>configuration group group1 | Specifies the policy profile of the group that will be defined and enters ISAKMP group configuration mode.<br><ul style="list-style-type: none"><li><i>group-name</i>—Group definition that identifies which policy is enforced for users.</li></ul> |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# exit                                                                                           | Exits ISAKMP group configuration mode.                                                                                                                                                                                                               |
| Step 5 | <b>max-logins</b> <i>number-of-logins</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# max-logins<br>10                                                 | (Optional) Limits the number of simultaneous logins for users in a specific server group.                                                                                                                                                            |
| Step 6 | <b>max-users</b> <i>number-of-users</i><br><br><b>Example:</b><br>Router (config)# max-users 1000                                                                  | (Optional) Limits the number of connections to a specific server group.                                                                                                                                                                              |

## Verifying a VPN Session

To verify a VPN session, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show crypto session group**
3. **show crypto session summary**

## DETAILED STEPS

|        | Command                                                                                          | Purpose                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                           | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>      |
| Step 2 | <b>show crypto session group</b><br><br><b>Example:</b><br>Router# show crypto session group     | Displays groups that are currently active on the VPN device.                                                           |
| Step 3 | <b>show crypto session summary</b><br><br><b>Example:</b><br>Router# show crypto session summary | Displays groups that are currently active on the VPN device and the users that are connected for each of those groups. |

## Applying Mode Configuration and Xauth

Mode Configuration and Xauth must be applied to a crypto map to be enforced. To apply Mode Configuration and Xauth to a crypto map, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map tag client configuration address [initiate | respond]**
4. **crypto map map-name isakmp authorization list list-name**
5. **crypto map map-name client authentication list list-name**

## DETAILED STEPS

|        | Command                                                                        | Purpose                                                                                                           |
|--------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                 |

|        | Command                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>crypto map tag client configuration address [initiate   respond]</b><br><br><b>Example:</b><br>Router (config)# crypto map dyn client configuration address initiate | Configures the router to initiate or reply to Mode Configuration requests.<br><br><b>Note</b> Cisco clients require the <b>respond</b> keyword to be used; however, if the Cisco Secure VPN Client 1.x is used, the <b>initiate</b> keyword must be used; <b>initiate</b> and <b>respond</b> keywords may be used simultaneously. |
| Step 4 | <b>crypto map map-name isakmp authorization list list-name</b><br><br><b>Example:</b><br>Router (config)# crypto map ikessaaamap isakmp authorization list ikessaaalist | Enables IKE querying for group policy when requested by the client.<br><br><ul style="list-style-type: none"> <li>The <i>list-name</i> argument is used by AAA to determine which storage source is used to find the policy (local or RADIUS) as defined in the <b>aaa authorization network</b> command.</li> </ul>              |
| Step 5 | <b>crypto map map-name client authentication list list-name</b><br><br><b>Example:</b><br>Router (config)# crypto map xauthmap client authentication list xauthlist     | Enforces Xauth.<br><br><ul style="list-style-type: none"> <li>The <i>list-name</i> argument is used to determine the appropriate username and password storage location (local or RADIUS) as defined in the <b>aaa authentication login</b> command.</li> </ul>                                                                   |

## Enabling Reverse Route Injection for the Client

To enable RRI on the crypto map (static or dynamic) for VPN client support, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic map-name seq-num**  
or  
**crypto map map-name seq-num ipsec-isakmp**
4. **set peer ip-address**
5. **set transform-set transform-set-name**
6. **reverse-route**
7. **match-address**

## DETAILED STEPS

|        | Command                                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                  | Enables privileged EXEC mode <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                          | Enters global configuration mode.                                                                                                                                                                                                                                                                     |
| Step 3 | <b>crypto dynamic map-name seq-num</b><br><br>or<br><b>crypto map map-name seq-num ipsec-isakmp</b><br><br><b>Example:</b><br>Router (config)# crypto dynamic mymap 10<br><br>or<br>Router (config)# crypto map yourmap 15 ipsec-isakmp | Creates a dynamic crypto map entry and enters crypto map configuration mode.<br><br>or<br><br>Adds a dynamic crypto map set to a static crypto map set and enters crypto map configuration mode.                                                                                                      |
| Step 4 | <b>set peer ip-address</b><br><br><b>Example:</b><br>Router (config-crypto-map)# set peer 10.20.20.20                                                                                                                                   | Specifies an IPsec peer IP address in a crypto map entry. <ul style="list-style-type: none"> <li>This step is optional when configuring dynamic crypto map entries.</li> </ul>                                                                                                                        |
| Step 5 | <b>set transform-set transform-set-name</b><br><br><b>Example:</b><br>Router (config-crypto-map)# set transform-set dessha                                                                                                              | Specifies which transform sets are allowed for the crypto map entry. <ul style="list-style-type: none"> <li>Lists multiple transform sets in order of priority (highest priority first).</li> </ul> <b>Note</b> This list is the only configuration statement required in dynamic crypto map entries. |
| Step 6 | <b>reverse-route</b><br><br><b>Example:</b><br>Router (config-crypto-map)# reverse-route                                                                                                                                                | Creates source proxy information.                                                                                                                                                                                                                                                                     |
| Step 7 | <b>match address</b><br><br><b>Example:</b><br>Router (config-crypto-map)# match address                                                                                                                                                | Specifies an extended access list for a crypto map entry. <ul style="list-style-type: none"> <li>This step is optional when configuring dynamic crypto map entries.</li> </ul>                                                                                                                        |



## Enabling IKE Dead Peer Detection

To enable a Cisco IOS VPN gateway (instead of the client) to send IKE DPD messages, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp keepalive *secs retries***

### DETAILED STEPS

|        | Command                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>crypto isakmp keepalive <i>secs retries</i></b><br><br><b>Example:</b><br>Router (config)# crypto isakmp keepalive 20 10 | Allows the gateway to send DPD messages to the router.<br><ul style="list-style-type: none"> <li>• The <i>secs</i> argument specifies the number of seconds between DPD messages (the range is from 1 to 3600 seconds); the <i>retries</i> argument specifies the number of seconds between retries if DPD messages fail (the range is from 2 to 60 seconds).</li> </ul> |

## Configuring RADIUS Server Support

To configure access to the server and allow the Cisco IOS VPN device to send requests to the server, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius server host *ip-address* [*auth-port port-number*] [*acct-port port-number*] [*key string*]**

## DETAILED STEPS

|        | Command                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                           | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                   | Enters global configuration mode.                                                                                                        |
| Step 3 | <b>radius server host</b> <i>ip-address</i> [ <b>auth-port</b> <i>port-number</i> ] [ <b>acct-port</b> <i>port-number</i> ] [ <b>key</b> <i>string</i> ]<br><br><b>Example:</b><br>Router (config)# radius server host<br>192.168.1.1. auth-port 1645 acct-port 1646<br>key XXXX | Specifies a RADIUS server host.<br><b>Note</b> This step is required if you choose to store group policy information in a RADIUS server. |

## Verifying Easy VPN Server

To verify your configurations for this feature, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show crypto map** [*interface interface* | **tag** *map-name*]

### DETAILED STEPS

|        | Command                                                                                                                                                          | Purpose                                                                                                           |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                           | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| Step 2 | <b>show crypto map</b> [ <b>interface</b> <i>interface</i>   <b>tag</b> <i>map-name</i> ]<br><br><b>Example:</b><br>Router# show crypto map interface ethernet 0 | Displays the crypto map configuration.                                                                            |

## Configuring a Banner

To configure an Easy VPN server to push a banner to an Easy VPN remote device, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *{group-name}*
4. **banner c** *{banner-text}* **c**

### DETAILED STEPS

|        | Command                                                                                                                                                        | Purpose                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                 | Enters global configuration mode.                                                                                   |
| Step 3 | <b>crypto isakmp client configuration group</b> <i>{group-name}</i><br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group Group1 | Specifies to which group a policy profile will be defined and enters crypto ISAKMP group configuration mode.        |
| Step 4 | <b>banner c</b> <i>{banner-text}</i> <b>c</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# banner c The quick brown fox jumped over the lazy dog c  | Specifies the text of the banner.                                                                                   |

## Configuring Auto Upgrade

To configure an Easy VPN server to provide an automated mechanism to make software and firmware upgrades automatically available to an Easy VPN remote device, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto isakmp client configuration group** {group-name}
4. **auto-update client** {type-of-system} {url url} {rev review-version}

## DETAILED STEPS

|        | Command                                                                                                                                                                                                                         | Purpose                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                          | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                  | Enters global configuration mode.                                                                                   |
| Step 3 | <b>crypto isakmp client configuration group</b> {group-name}<br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group Group2                                                                         | Specifies to which group a policy profile will be defined and enters crypto ISAKMP group configuration mode.        |
| Step 4 | <b>auto-update client</b> {type-of-system} {url url} {rev review-version}<br><br><b>Example:</b><br>Router (config-isakmp-group)# auto-update client Win2000 url http:www.ourcompanysite.com/newclient rev 3.0.1(Rel), 3.1(Rel) | Configures auto-update parameters for an Easy VPN remote device.                                                    |

## Configuring Browser Proxy

To configure an EasyVPN server so that the Easy VPN remote device can access resources on the corporate network when using Cisco IOS VPN Client software, perform the following steps. With this configuration, the user does not have to manually modify the proxy settings of his or her web browser when connecting and does not have to manually revert the proxy settings when disconnecting.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration browser-proxy** {browser-proxy-name}
4. **proxy** {proxy-parameter}

## DETAILED STEPS

|        | Command                                                                                                                                                                                  | Purpose                                                                                                               |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                   | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                           | Enters global configuration mode.                                                                                     |
| Step 3 | <b>crypto isakmp client configuration browser-proxy</b> { <i>browser-proxy-name</i> }<br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration browser-proxy bproxy | Configures browser-proxy parameters for an Easy VPN remote device and enters ISAKMP Browser Proxy configuration mode. |
| Step 4 | <b>proxy</b> { <i>proxy-parameter</i> }<br><br><b>Example:</b><br>Router (config-ikmp-browser-proxy)# proxy auto-detect                                                                  | Configures proxy parameters for an Easy VPN remote device.                                                            |

## Configuring the Pushing of a Configuration URL Through a Mode-Configuration Exchange

To configure an Easy VPN server to push a configuration URL through a Mode-Configuration Exchange, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** {*group-name*}
4. **configuration url** {*url*}
5. **configuration version** {*version-number*}

## DETAILED STEPS

|        | Command                                                                                                                                                 | Purpose                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                          | Enters global configuration mode.                                                                                                                                                                                                                     |
| Step 3 | <b>crypto isakmp client configuration group</b> {group-name}<br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group Group1 | Specifies to which group a policy profile will be defined and enters crypto ISAKMP group configuration mode.                                                                                                                                          |
| Step 4 | <b>configuration url</b> {url}<br><br><b>Example:</b><br>Router (config-isakmp-group)# configuration url http://10.10.88.8/easy.cfg                     | Specifies the URL the remote device must use to get the configuration from the server. <ul style="list-style-type: none"><li>The URL must be a non-NULL terminated ASCII string that specifies the complete path of the configuration file.</li></ul> |
| Step 5 | <b>configuration version</b> {version-number}<br><br><b>Example:</b><br>Router (config-isakmp-group)# configuration version 10                          | Specifies the version of the configuration. <ul style="list-style-type: none"><li>The version number will be an unsigned integer in the range 1 through 32767.</li></ul>                                                                              |

## Configuring Per User AAA Download with PKI—Configuring the Crypto PKI Trustpoint

To configure a AAA server to push user attributes to a remote device, perform the following steps.

### Prerequisites

Before configuring a AAA server to push user attributes to a remote device, you must have configured AAA. The crypto PKI trustpoint must also be configured (see the first configuration task below). It is preferable that the trustpoint configuration contain the **authorization username** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*

5. **revocation-check none**
6. **rsa-keypair** *key-label*
7. **authorization username** {**subjectname** *subjectname*}
8. **exit**

## DETAILED STEPS

|        | Command                                                                                                                                                                           | Purpose                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                    | Enters global configuration mode.                                                                                |
| Step 3 | <b>crypto pki trustpoint</b> <i>name</i><br><br><b>Example:</b><br>Router (config)# crypto pki trustpoint<br>ca-server                                                            | Declares the trustpoint that your router should use and enters ca-trustpoint configuration mode.                 |
| Step 4 | <b>enrollment url</b> <i>url</i><br><br><b>Example:</b><br>Router (config-ca-trustpoint)# enrollment<br>url http://10.7.7.2:80                                                    | Specifies the URL of the certification authority (CA) server to which to send enrollment requests.               |
| Step 5 | <b>revocation-check none</b><br><br><b>Example:</b><br>Router (config-ca-trustpoint)#<br>revocation-check none                                                                    | Checks the revocation status of a certificate.                                                                   |
| Step 6 | <b>rsa-keypair</b> <i>key-label</i><br><br><b>Example:</b><br>Router (config-ca-trustpoint)# rsa-keypair<br>rsa-pair                                                              | Specifies which key pair to associate with the certificate.                                                      |
| Step 7 | <b>authorization username</b> { <b>subjectname</b> <i>subjectname</i> }<br><br><b>Example:</b><br>Router (config-ca-trustpoint)# authorization<br>username subjectname commonname | Specifies the parameters for the different certificate fields that are used to build the AAA username.           |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router (config-ca-trustpoint)# exit                                                                                                         | Exits ca-trustpoint configuration mode.                                                                          |

## Configuring the Actual Per User AAA Download with PKI

To configure the actual per-user download with PKI, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy** *priority*
4. **group** {1 | 2}
5. **exit**
6. **crypto isakmp profile** *profile-name*
7. **match certificate** *certificate-map*
8. **client pki authorization list** *listname*
9. **client configuration address** {*initiate* | *respond*}
10. **virtual-template** *template-number*
11. **exit**
12. **crypto ipsec transform-set** [*transform-set-name transform1*] [*transform2*] [*transform3*] [*transform4*]
13. **crypto ipsec profile** *name*
14. **set transform-set** *transform-set-name*

### DETAILED STEPS

|        | Command                                                                                                        | Purpose                                                                                                           |
|--------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                 | Enters global configuration mode.                                                                                 |
| Step 3 | <b>crypto isakmp policy</b> <i>priority</i><br><br><b>Example:</b><br>Router (config)# crypto isakmp policy 10 | Defines an IKE policy and enters ISAKMP policy configuration mode.                                                |
| Step 4 | <b>group</b> {1   2}<br><br><b>Example:</b><br>Router (config-isakmp-policy)# group 2                          | Specifies the Diffie-Hellman group identifier within an IKE policy.                                               |



|         | Command                                                                                                                                                                                                                           | Purpose                                                                                                                                                                |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5  | <b>exit</b><br><br><b>Example:</b><br>Router (config-isakmp-policy)# exit                                                                                                                                                         | Exits ISAKMP policy configuration mode.                                                                                                                                |
| Step 6  | <b>crypto isakmp profile</b> <i>profile-name</i><br><br><b>Example:</b><br>Router (config)# crypto isakmp profile<br>ISA-PROF                                                                                                     | Defines an ISAKMP profile and audits IPsec user sessions and enters crypto ISAKMP profile configuration mode.                                                          |
| Step 7  | <b>match certificate</b> <i>certificate-map</i><br><br><b>Example:</b><br>Router (config-isakmp-profile)# match<br>certificate cert_map                                                                                           | Assigns an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate.                                                               |
| Step 8  | <b>client pki authorization list</b> <i>listname</i><br><br><b>Example:</b><br>Router (config-isakmp-profile)# client pki<br>authorization list usrgrp                                                                            | Specifies the authorization list of AAA servers that will be used for obtaining per-user AAA attributes on the basis of the username constructed from the certificate. |
| Step 9  | <b>client configuration address</b> { <b>initiate</b>   <b>respond</b> }<br><br><b>Example:</b><br>Router (config-isakmp-profile)# client<br>configuration address respond                                                        | Configures IKE configuration mode in the ISAKMP profile.                                                                                                               |
| Step 10 | <b>virtual-template</b> <i>template-number</i><br><br><b>Example:</b><br>Router(config-isakmp-profile)#<br>virtual-template 2                                                                                                     | Specifies which virtual template will be used to clone virtual access interfaces.                                                                                      |
| Step 11 | <b>exit</b><br><br><b>Example:</b><br>Router(config-isakmp-profile)# exit                                                                                                                                                         | Exits crypto ISAKMP profile configuration mode.                                                                                                                        |
| Step 12 | <b>crypto ipsec transform-set</b><br><i>transform-set-name transform1 [transform2]</i><br><i>[transform3] [transform4]</i><br><br><b>Example:</b><br>Router (config)# crypto ipsec transform-set<br>trans2 esp-3des esp-sha-hmac1 | Defines a transform set—an acceptable combination of security protocols and algorithms.                                                                                |

|         | Command                                                                                                                | Purpose                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Step 13 | <b>crypto ipsec profile</b> <i>name</i><br><br><b>Example:</b><br>Router (config)# crypto ipsec profile<br>IPSEC_PROF  | Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers. |
| Step 14 | <b>set transform-set</b> <i>transform-set-name</i><br><br><b>Example:</b><br>Router (config)# set transform-set trans2 | Specifies which transform sets can be used with the crypto map entry.                            |

## Configuring Per-User Attributes on a Local Easy VPN AAA Server

To configure per-user attributes on a local Easy VPN AAA server, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa attribute list** *list-name*
4. **attribute type** *name value* [**service** *service*] [**protocol** *protocol*]
5. **exit**
6. **crypto isakmp client configuration group** *group-name*
7. **crypto aaa attribute list** *list-name*

### DETAILED STEPS

|        | Command or Action                                                                                             | Purpose                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                | Enters global configuration mode.                                                                                  |
| Step 3 | <b>aaa attribute list</b> <i>list-name</i><br><br><b>Example:</b><br>Router(config)# aaa attribute list list1 | Defines a AAA attribute list locally on a router and enters attribute list configuration mode.                     |

|        | Command or Action                                                                                                                                                                   | Purpose                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Step 4 | <b>attribute type name value [service service] [protocol protocol]</b><br><br><b>Example:</b><br>Router(config-attr-list)# attribute type<br>attribute xxxx service ike protocol ip | Defines an attribute type that is to be added to an attribute list locally on a router.               |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-attr-list)# exit                                                                                                                | Exits attribute list configuration mode.                                                              |
| Step 6 | <b>crypto isakmp client configuration group group-name</b><br><br><b>Example:</b><br>Router (config)# crypto isakmp client<br>configuration group group1                            | Specifies to which group a policy profile will be defined and enters ISAKMP group configuration mode. |
| Step 7 | <b>crypto aaa attribute list list-name</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# crypto aaa<br>attribute list listname1                                           | Defines a AAA attribute list locally on a router.                                                     |

## Enabling Easy VPN Syslog Messages

To enable Easy VPN syslog messages on a server, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto logging ezvpn group group-name**

### DETAILED STEPS

|        | Command                                                | Purpose                                                                                                            |
|--------|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |

|        | Command                                                               | Purpose                                                                                                                                                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 2 | <b>configure terminal</b>                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                         |
|        | <b>Example:</b><br>Router# configure terminal                         |                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>crypto logging ezvpn</b> [ <i>group group-name</i> ]               | Enables Easy VPN syslog messages on a server.                                                                                                                                                                                                                                                                             |
|        | <b>Example:</b><br>Router (config)# crypto logging ezvpn group group1 | <ul style="list-style-type: none"> <li>The <b>group</b> keyword and <i>group-name</i> argument are optional. If a group name is not provided, syslog messages are enabled for all Easy VPN connections to the server. If a group name is provided, syslog messages are enabled for that particular group only.</li> </ul> |

## Defining a CPP Firewall Policy Push Using a Local AAA Server

To define a CPP firewall policy push on a server to allow or deny a tunnel on the basis of whether a remote device has a required firewall for a local AAA server, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client firewall** {*policy-name*} {**required** | **optional**} {*firewall-type*}
4. **policy** {**check-presence** | **central-policy-push** {**access-list** {**in** | **out**} *access-list-name* | *access-list-number*}}

### DETAILED STEPS

|        | Command                                       | Purpose                                                                            |
|--------|-----------------------------------------------|------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode.                                                      |
|        | <b>Example:</b><br>Router> enable             | <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                  |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                    |

|        | Command                                                                                                                                                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <p><b>crypto isakmp client firewall</b> {<i>policy-name</i>}<br/>{<b>required</b>   <b>optional</b>} {<i>firewall-type</i>}</p> <p><b>Example:</b><br/>Router (config)# crypto isakmp client<br/>firewall hw-client-g-cpp required<br/>Cisco-Security-Agent</p>                                                                                                    | <p>Defines the CPP firewall push policy on a server and enters ISAKMP client firewall configuration mode.</p> <p>The arguments and keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>policy-name</b>—Uniquely identifies a policy. A policy name can be associated with the Easy VPN client group configuration of the server (local group configuration) or on the AAA server.</li> <li>• <b>required</b>—Policy is mandatory. If the CPP policy is defined as mandatory and is included in the Easy VPN server configuration, the tunnel setup is allowed only if the client confirms this policy. Otherwise, the tunnel is terminated.</li> <li>• <b>optional</b>—Policy is optional. If the CPP policy is defined as optional, and is included in the Easy VPN server configuration, the tunnel setup is continued even if the client does not confirm the defined policy.</li> <li>• <b>firewall-type</b>—Type of firewall (see the <b>crypto isakmp client firewall</b> command for a list of firewall types).</li> </ul> |
| Step 4 | <p><b>policy</b> {<b>check-presence</b>   <b>central-policy-push</b> {<b>access-list</b> {<b>in</b>   <b>out</b>} <i>access-list-name</i>   <i>access-list-number</i>}}</p> <p><b>Example:</b><br/>Router (config-ikmp-client-fw)# policy<br/>central-policy-push access-list out acl1</p> <p>or<br/>Router (config-ikmp-client-fw)# policy<br/>check-presence</p> | <p>Defines the CPP firewall policy push.</p> <p>The arguments and keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>check-presence</b>—Denotes that the server should check for the presence of the specified firewall as shown by the value of the <i>firewall-type</i> argument on the client.</li> <li>• <b>central-policy-push</b>—The configuration following this keyword specifies the actual policy, such as the input and output access lists that have to be applied by the client firewall, which is of the type specified by the value of the <i>firewall-type</i> argument.</li> <li>• <b>access-list {in   out}</b>—Defines the inbound and outbound access lists.</li> <li>• <b>access-list-name   access-list-number</b>—Name or number of the access list.</li> </ul>                                                                                                                                                                                                                                          |

## What to Do Next

Apply the CPP firewall policy push to the configured group.

## Applying a CPP Firewall Policy Push to the Configuration Group

Now that the CPP firewall policy push has been defined, it must be applied to the configuration group by performing the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *{group-name}*
4. **firewall policy** *{policy-name}*

## DETAILED STEPS

|        | Command                                                                                                                                                             | Purpose                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                              | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                      | Enters global configuration mode.                                                                                                   |
| Step 3 | <b>crypto isakmp client configuration group</b> <i>{group-name}</i><br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group hw-client-g | Specifies to which group a policy profile will be defined and enters ISAKMP group configuration mode.                               |
| Step 4 | <b>firewall policy</b> <i>{policy-name}</i><br><br><b>Example:</b><br>Router (crypto-isakmp-group)# firewall policy hw-client-g-cpp                                 | Specifies the CPP firewall push policy name for the crypto ISAKMP client configuration group on a local authentication, AAA server. |

## Defining a CPP Firewall Policy Push Using a Remote AAA Server

To define a CPP firewall policy push using a remote AAA server, see the section “[Defining a CPP Firewall Policy Push Using a Local AAA Server](#).” The steps are the same for this configuration.

## What to Do Next

After defining the CPP firewall policy push, you should add the VSA cpp-policy under the group definition.

## Adding the VSA CPP-Policy Under the Group Definition

To add the the VSA cpp-policy under the group definition that is defined in RADIUS, perform the following step.

## SUMMARY STEPS

1. Add the VSA cpp-policy under the group definition that is defined in RADIUS.

## DETAILED STEPS

|        | Command                                                                                                                                         | Purpose                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Step 1 | Add the VSA “cpp-policy” under the group definition that is defined in RADIUS.<br><br><b>Example:</b><br>ipsec:cpp-policy=”Enterprise Firewall” | Defines the CPP firewall push policy for a remote server. |

## Verifying CPP Firewall Policy Push

To verify the CPP firewall push policy on a local or remote AAA server, perform the following steps.

## SUMMARY STEPS

1. enable
2. debug crypto isakmp

## DETAILED STEPS

|        | Command                                                                          | Purpose                                                                                                               |
|--------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                           | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>debug crypto isakmp</b><br><br><b>Example:</b><br>Router# debug crypto isakmp | Displays messages about IKE events.                                                                                   |

## Configuring Password Aging

To configure Password Aging so that the Easy VPN client is notified if the password has expired, perform the following steps.

## Restrictions

The following restrictions apply to the Password Aging feature:

- It works only with VPN software clients. It does not work with VPN client hardware.
- It works only with RADIUS servers.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login {list-name} password-expiry method1 [method2...]**
5. **radius-server host {ip-address} auth-port port-number acct-port port-number key string}**
6. Configure the ISAKMP profile
7. **client authentication list {list-name}**

## DETAILED STEPS

|        | Command                                                                                                                                                                                                                                                                | Purpose                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                 | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                         | Enters global configuration mode.                                                                                   |
| Step 3 | <b>aaa new-model</b><br><br><b>Example:</b><br>Router (config)# aaa new-model                                                                                                                                                                                          | Enables AAA.                                                                                                        |
| Step 4 | <b>aaa authentication login {list-name} password-expiry method1 [method2...]</b><br><br><b>Example:</b><br>Router (config)# aaa authentication login userauth paswd-expiry group radius                                                                                | Configures the authentication list so that the Password Aging feature is enabled.                                   |
| Step 5 | <b>radius-server host {ip-address} auth-port port-number acct-port port-number key string}</b><br><br><b>Example:</b><br>Router (config)# radius-server host 172.19.217.96 255.255.255.0 auth-port 1645 acct-port 1646 key cisco radius-server vsa send authentication | Configures the RADIUS server.                                                                                       |



|        | Command                                                                                                                                           | Purpose                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | Configure the ISAKMP profile.<br><br><b>Example:</b><br>see the section “ <a href="#">Configuring Password Aging: Example</a> ”                   | Configures the ISAKMP profile and enters ISAKMP profile configuration mode (see the section “ <a href="#">Configuring Password Aging: Example</a> ”). |
| Step 7 | <code>client authentication list {list-name}</code><br><br><b>Example:</b><br>Router (config-isakmp-profile)# client authentication list userauth | Configures IKE extended authentication (Xauth) in an ISAKMP profile and includes the authentication list that was defined above.                      |

## Configuring Split DNS

To configure Split DNS, perform the following steps.

### Prerequisites

Before the Split DNS feature can work, the following commands should have been configured on the Easy VPN remote:

- `ip dns server`
- `ip domain-lookup`

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto isakmp client configuration group group-name`
4. `dns primary-server secondary-server`
5. `split-dns domain-name`

### DETAILED STEPS

|        | Command                                                                              | Purpose                                                                                                             |
|--------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                   |

|        | Command                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>crypto isakmp client configuration group</b> <i>{group-name   default}</i><br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group group1 | Specifies the policy profile of the group that will be defined and enters ISAKMP group configuration mode. <ul style="list-style-type: none"> <li>If no specific group matches and a default group is defined, users will automatically be given the policy of a default group.</li> </ul> |
| Step 4 | <b>dns</b> <i>primary-server secondary-server</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# dns 10.2.2.2 10.3.3.3                                          | Specifies the primary and secondary DNS servers for the group.                                                                                                                                                                                                                             |
| Step 5 | <b>split-dns</b> <i>domain-name</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# split-dns green.com                                                          | Specifies a domain name that must be tunneled or resolved to the private network.                                                                                                                                                                                                          |

## Verifying Split DNS

To verify a split DNS configuration, perform the following steps (the **show** commands can be used one at a time or together).

### SUMMARY STEPS

1. **enable**
2. **show ip dns name-list** *[name-list-number]*
3. **show ip dns view** *[vrf vrf-name] [default | view-name]*
4. **show ip dns view-list** *[view-list-name]*

### DETAILED STEPS

|        | Command                                                                                                          | Purpose                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show ip dns name-list</b> <i>[name-list-number]</i><br><br><b>Example:</b><br>Router# show ip dns name-list 1 | Displays information about DNS name lists.                                                                       |

|        | Command                                                                                                                                                 | Purpose                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| Step 3 | <b>show ip dns view</b> [ <b>vrf</b> <i>vrf-name</i> ] [ <b>default</b>   <i>view-name</i> ]<br><br><b>Example:</b><br>Router# show ip dns view default | Displays information about DNS views.      |
| Step 4 | <b>show ip dns view-list</b> [ <i>view-list-name</i> ]<br><br><b>Example:</b><br>Router# show ip dns view-list<br>ezvpn-internal-viewlist               | Displays information about DNS view lists. |

## Monitoring and Maintaining Split DNS

To monitor and maintain the split DNS configuration on Easy VPN remote devices, perform the following steps.

### SUMMARY STEPS

1. enable
2. debug ip dns name-list
3. debug ip dns view
4. debug ip dns view-list

### DETAILED STEPS

|        |                                                                                        |                                                                                                                    |
|--------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>debug ip dns name-list</b><br><br><b>Example:</b><br>Router# debug ip dns name-list | Enables debugging output for Domain Name System (DNS) name-list events.                                            |
| Step 3 | <b>debug ip dns view</b><br><br><b>Example:</b><br>Router# debug ip dns view           | Enables debugging output for DNS view events.                                                                      |
| Step 4 | <b>debug ip dns view-list</b><br><br><b>Example:</b><br>Router# debug ip dns view-list | Enables debugging output for DNS view-list events.                                                                 |

## Configuring an Easy VPN Server to Obtain an IP Address from a DHCP Server

When the Easy VPN server selects the method for address assignment, it does so in the following order of precedence:

1. Selects the Framed IP address
2. Uses the IP address from the authentication server (group/user)
3. Uses the global IKE address pools
4. Uses DHCP



### Note

To enable the Easy VPN server to obtain an IP address from a DHCP server, remove other address assignments.

To configure an Easy VPN server to obtain an IP address from a DHCP server, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **dhcp server** {*ip-address* | *hostname*}
5. **dhcp timeout** *time*
6. **dhcp giaddr** *scope*

### DETAILED STEPS

|                                                                                                              |                                                                   |                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b><br><br><br><b>Example:</b><br>Router> enable                                                   | <b>enable</b>                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                |
| <b>Step 2</b><br><br><br><b>Example:</b><br>Router# configure terminal                                       | <b>configure terminal</b>                                         | Enters global configuration mode.                                                                                                                                                                                                               |
| <b>Step 3</b><br><br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group group1 | <b>crypto isakmp client configuration group</b> <i>group-name</i> | Specifies to which group a policy profile will be defined. <p><b>Note</b> Entering this command places the CLI in ISAKMP group configuration mode. From this mode, you can use subcommands to specify characteristics for the group policy.</p> |
| <b>Step 4</b><br><br><br><b>Example:</b><br>Router (config-isakmp-group)# dhcp server 10.10.1.2              | <b>dhcp server</b> { <i>ip-address</i>   <i>hostname</i> }        | Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular public data network (PDN) access point.                                                                                                 |

|               |                                                                                                              |                                                                                 |
|---------------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <b>Step 5</b> | <b>dhcp timeout</b> <i>time</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# dhcp timeout 6       | Sets the wait time in seconds before the next DHCP server on the list is tried. |
| <b>Step 6</b> | <b>dhcp giaddr</b> <i>scope</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# dhcp giaddr 10.1.1.4 | Specifies the giaddr for the DHCP scope.                                        |

## Verifying DHCP Client Proxy

To verify your DHCP client proxy configuration, perform the following steps (use the **show** commands one at a time or together).

### SUMMARY STEPS

1. **enable**
2. **show dhcp lease**
3. **show ip dhcp pool**
4. **show ip dhcp binding**

### DETAILED STEPS

|               |                                                                                    |                                                                                                                                                                                                                                               |
|---------------|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                            |
| <b>Step 1</b> | <b>show dhcp lease</b><br><br><b>Example:</b><br>Router# show dhcp lease           | Displays information about the DHCP address pools.<br><br><b>Note</b> Use this command when an external DHCP is used.                                                                                                                         |
| <b>Step 2</b> | <b>show ip dhcp pool</b><br><br><b>Example:</b><br>Router# show ip dhcp pool       | Displays information about the DHCP address pools.<br><br><b>Note</b> This command is applicable only when the Easy VPN server is also the DHCP server (generally not the case because in most cases, the DHCP server is an external server). |
| <b>Step 3</b> | <b>show ip dhcp binding</b><br><br><b>Example:</b><br>Router# show ip dhcp binding | Displays address bindings on the DHCP server.<br><br><b>Note</b> This command is applicable only when the Easy VPN server is also the DHCP server (generally not the case because in most cases, the DHCP server is an external server).      |

## Monitoring and Maintaining DHCP Client Proxy

To monitor and maintain your DHCP client proxy configuration, perform the following steps (use the **debug** commands one at a time or together).

### SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp**
3. **debug dhcp**
4. **debug dhcp detail**
5. **debug ip dhcp server events**

### DETAILED STEPS

|                                                                                 |                                                |                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b><br><br><br><b>Example:</b><br>Router> enable                      | <b>enable</b><br><br><br>                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                               |
| <b>Step 2</b><br><br><br><b>Example:</b><br>Router# debug crypto isakmp         | <b>debug crypto isakmp</b><br><br><br>         | Displays messages about Internet Key Exchange (IKE) event.                                                                                                                                                                                                       |
| <b>Step 3</b><br><br><br><b>Example:</b><br>Router# debug dhcp                  | <b>debug dhcp</b><br><br><br>                  | Reports server events, like address assignments and database updates.                                                                                                                                                                                            |
| <b>Step 4</b><br><br><br><b>Example:</b><br>Router# debug dhcp detail           | <b>debug dhcp detail</b><br><br><br>           | Displays detailed DHCP debugging information.                                                                                                                                                                                                                    |
| <b>Step 5</b><br><br><br><b>Example:</b><br>Router# debug ip dhcp server events | <b>debug ip dhcp server events</b><br><br><br> | Reports server events, like address assignments and database updates. <p><b>Note</b> This command is applicable only when the Easy VPN server is also the DHCP server (generally not the case because in most cases, the DHCP server is an external server).</p> |

## Configuring cTCP

To enable cTCP, perform the following steps on your Easy VPN server.

### Prerequisites

Before configuring cTCP, you should have configured crypto IPsec.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ctcp port** [*port-number*]

## DETAILED STEPS

|               |                                                                                                                |                                                                                                                                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                              |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                 | Enters global configuration mode.                                                                                                                                                                                                                |
| <b>Step 3</b> | <b>crypto ctcp port</b> [ <i>port-number</i> ]<br><br><b>Example:</b><br>Router (config)# crypto ctcp port 120 | Configures cTCP encapsulation for Easy VPN.<br><ul style="list-style-type: none"><li>• Up to 10 port numbers can be configured.</li><li>• If the <i>port-number</i> argument is not configured, cTCP is enabled on port 80 by default.</li></ul> |

## Verifying cTCP

To verify your cTCP configuration, perform the following steps (the **show** commands can be used one at a time or together).

## SUMMARY STEPS

1. **enable**
2. **show crypto ctcp** [*peer ip-address*]

## DETAILED STEPS

|               |                                                                                                                         |                                                                                                                     |
|---------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                  | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| <b>Step 2</b> | <b>show crypto ctcp</b> [ <i>peer ip-address</i> ]<br><br><b>Example:</b><br>Router# show crypto ctcp peer 10.76.235.21 | Displays information about a specific cTCP peer.                                                                    |

## Monitoring and Maintaining a cTCP Configuration

To monitor and maintain your cTCP configuration, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **debug crypto ctcp**

## DETAILED STEPS

|                                                                       |                          |                                                                                                                    |
|-----------------------------------------------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b><br><br><br><b>Example:</b><br>Router> enable            | <b>enable</b>            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b><br><br><br><b>Example:</b><br>Router# debug crypto ctcp | <b>debug crypto ctcp</b> | Displays information about a cTCP session.                                                                         |

## Clearing a cTCP Configuration

To clear a cTCP configuration, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **clear crypto ctcp [peer *ip-address*]**

## DETAILED STEPS

|                                                                                        |                                                   |                                                                                                                    |
|----------------------------------------------------------------------------------------|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b><br><br><br><b>Example:</b><br>Router> enable                             | <b>enable</b>                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b><br><br><br><b>Example:</b><br>Router# clear crypto ctcp peer 10.76.23.21 | <b>clear crypto ctcp [peer <i>ip-address</i>]</b> | Displays information about a cTCP session.                                                                         |



## Troubleshooting a cTCP Configuration

To troubleshoot a cTCP configuration, perform the following steps.

### SUMMARY STEPS

1. Ensure that the cTCP session is in the CTCP\_ACK\_RECEIVED state.
2. If the cTCP session is not in the CTCP\_ACK\_RECEIVED state, enable the **debug crypto ctcp** command.
3. If no cTCP bugs are seen, ensure that the firewall is allowing the cTCP packets to get to the server.
4. If the firewall configuration is correct, debugging is enabled, and you do not see any cTCP debugs on your console, you must find out why the cTCP port on the router is not receiving packets.

### DETAILED STEPS

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | To ensure that the cTCP session is in the CTCP_ACK_RECEIVED state, use the <b>show crypto ctcp</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 2</b> | If the cTCP session is not in the CTCP_ACK_RECEIVED state, enable the <b>debug crypto ctcp</b> command and then try using the <b>show crypto ctcp</b> command again.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 3</b> | If no cTCP bugs are seen, ensure that the firewall is allowing the cTCP packets to get to the server (check the firewall configuration).                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 4</b> | If the firewall configuration is correct, debugging is enabled, and you do not see any cTCP debugs on your console, you must find out why the cTCP port on the router is not receiving packets. If you do not see any cTCP debugs and a cTCP session has not been set up, there is a possibility that cTCP packets that are actually TCP packets could have been delivered to a TCP stack instead of to the cTCP port. By enabling the <b>debug ip packet</b> and <b>debug ip tcp packet</b> commands, you may be able to determine whether the packet is being given to the TCP stack. |
- 

## Configuration Examples for Easy VPN Server

This section provides the following configuration examples:

- [Configuring Cisco IOS for Easy VPN Server: Example, page 54](#)
- [RADIUS Group Profile with IPsec AV Pairs: Example, page 55](#)
- [RADIUS User Profile with IPsec AV Pairs: Example, page 56](#)
- [Backup Gateway with Maximum Logins and Maximum Users: Example, page 56](#)
- [Easy VPN with an IPsec Virtual Tunnel Interface: Example, page 56](#)
- [Pushing a Configuration URL Through a Mode-Configuration Exchange: Examples, page 58](#)
- [Per User AAA Policy Download with PKI: Example, page 58](#)
- [Per-User Attributes on an Easy VPN Server: Example, page 62](#)
- [Network Admission Control: Example, page 64](#)
- [Configuring Password Aging: Example, page 66](#)

- [Split DNS: Examples, page 68](#)
- [DHCP Client Proxy: Examples, page 69](#)
- [cTCP Session: Example, page 70](#)
- [VRF Assignment by a AAA Server: Example, page 71](#)

## Configuring Cisco IOS for Easy VPN Server: Example

The following example shows how to define group policy information locally for mode configuration. In this example, a group name is named “cisco” and another group name is named “default.” The policy is enforced for all users who do not offer a group name that matches “cisco.”

```
! Enable policy look-up via AAA. For authentication and authorization, send requests to
! RADIUS first, then try local policy.
aaa new-model
aaa authentication login userlist group radius local
aaa authorization network grouplist group radius local
enable password XXXX
!
username cisco password 0 cisco
clock timezone PST -8
ip subnet-zero
! Configure IKE policies, which are assessed in order so that the first policy that
matches the proposal of the client will be used.
crypto isakmp policy 1
 group 2
!
crypto isakmp policy 3
 hash md5
 authentication pre-share
 group 2
crypto isakmp identity hostname
!
! Define "cisco" group policy information for mode config push.
crypto isakmp client configuration group cisco
 key cisco
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.6
 domain cisco.com
 pool green
 acl 199
! Define default group policy for mode config push.
crypto isakmp client configuration group default
 key cisco
 dns 10.2.2.2 10.3.2.3
 pool green
 acl 199
!
!
crypto ipsec transform-set dessha esp-des esp-sha-hmac
!
crypto dynamic-map mode 1
 set transform-set dessha
!
! Apply mode config and xauth to crypto map "mode." The list names that are defined here
! must match the list names that are defined in the AAA section of the config.
crypto map mode client authentication list userlist
crypto map mode isakmp authorization list grouplist
crypto map mode client configuration address respond
crypto map mode 1 ipsec-isakmp dynamic mode
```

```

!
!
controller ISA 1/1
!
!
interface FastEthernet0/0
 ip address 10.6.1.8 255.255.0.0
 ip route-cache
 ip mroute-cache
 duplex auto
 speed auto
 crypto map mode
!
interface FastEthernet0/1
 ip address 192.168.1.28 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
! Specify IP address pools for internal IP address allocation to clients.
ip local pool green 192.168.2.1 192.168.2.10
ip classless
ip route 0.0.0.0 0.0.0.0 10.6.0.1
!
! Define access lists for each subnet that should be protected.
access-list 199 permit ip 192.168.1.0 0.0.0.255 any
access-list 199 permit ip 192.168.3.0 0.0.0.255 any
!
! Specify a RADIUS server host and configure access to the server.
radius-server host 192.168.1.1 auth-port 1645 acct-port 1646 key XXXXX
radius-server retransmit 3
!
!
line con 0
 exec-timeout 0 0
 length 25
 transport input none
line aux 0
line vty 5 15
!

```

## RADIUS Group Profile with IPsec AV Pairs: Example

The following is an example of a standard RADIUS group profile that includes RADIUS IPsec AV pairs. To get the group authorization attributes, “cisco” must be used as the password.

```

client_r Password = "cisco"
Service-Type = Outbound

cisco-avpair = "ipsec:tunnel-type=ESP"
cisco-avpair = "ipsec:key-exchange=ike"
cisco-avpair = "ipsec:tunnel-password=lab"
cisco-avpair = "ipsec:addr-pool=pool1"
cisco-avpair = "ipsec:default-domain=cisco"
cisco-avpair = "ipsec:inac1=101"
cisco-avpair = "ipsec:access-restrict=fastethernet 0/0"
cisco-avpair = "ipsec:group-lock=1"
cisco-avpair = "ipsec:dns-servers=10.1.1.1 10.2.2.2"
cisco-avpair = "ipsec:firewall=1"
cisco-avpair = "ipsec:include-local-lan=1"
cisco-avpair = "ipsec:save-password=1"
cisco-avpair = "ipsec:wins-servers=10.3.3.3 10.4.4.4"

```

```

cisco-avpair = "ipsec:split-dns=green.com"
ciscoc-avpair = "ipsec:ipsec-backup-gateway=10.1.1.1"
cisoc-avpair = "ipsec:ipsec-backup-gateway=10.1.1.2"
ciscoc-avpair = "ipsec:pfs=1"
cisco-avpair = "ipsec:cpp-policy="Enterprise Firewall"
cisco-avpair = "ipsec:auto-update="Win http://abc.com 4.0.1"
cisco-avpair = "ipsec:browser-proxy=bproxy_profile_A"
cisco-avpair = "ipsec:xauth-banner="Xauth banner text here"

```

## RADIUS User Profile with IPsec AV Pairs: Example

The following is an example of a standard RADIUS user profile that includes RADIUS IPsec AV pairs. These user attributes will be obtained during Xauth.

```

ualluall Password = "uall1234"
 cisco-avpair = "ipsec:user-vpn-group=unity"
 cisco-avpair = "ipsec:user-include-local-lan=1"
 cisco-avpair = "ipsec:user-save-password=1"
 Framed-IP-Address = 10.10.10.10

```

## Backup Gateway with Maximum Logins and Maximum Users: Example

The following example shows that five backup gateways have been configured, that the maximum users have been set to 250, and that maximum logins have been set to 2:

```

crypto isakmp client configuration group sdm
key 6 RMZPPMRQMSdiZNJg`EBbCWTkSTi\dl
pool POOL1
acl 150
backup-gateway 172.16.12.12
backup-gateway 172.16.12.13
backup-gateway 172.16.12.14
backup-gateway 172.16.12.130
backup-gateway 172.16.12.131
max-users 250
max-logins 2

```

## Easy VPN with an IPsec Virtual Tunnel Interface: Example

The following output shows that Easy VPN has been configured with an IPsec virtual tunnel interface.

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication login default local

```

```
aaa authorization network default local
!
aaa session-id common
!
resource policy
!
clock timezone IST 0
ip subnet-zero
ip cef
no ip domain lookup
no ip dhcp use vrf connected
!
username lab password 0 lab
!
crypto isakmp policy 3
 authentication pre-share
 group 2
crypto isakmp xauth timeout 90

!
crypto isakmp client configuration group easy
 key cisco
 domain foo.com
 pool dpool
 acl 101
crypto isakmp profile vi
 match identity group easy
 isakmp authorization list default
 client configuration address respond
 client configuration group easy
 virtual-template 1
!
!
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
!
interface Loopback0
 ip address 10.4.0.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.3.0.2 255.255.255.0
 no keepalive
 no cdp enable
interface Ethernet1/0
 no ip address
 no keepalive
 no cdp enable
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.5.0.1 10.5.0.10
!
ip classless
ip route 10.2.0.0 255.255.255.0 10.3.0.1
no ip http server
no ip http secure-server
!
```

```

!
access-list 101 permit ip 10.4.0.0 0.0.0.255 any
no cdp run
!
!
line con 0
line aux 0
line vty 0 4
!
end

```

## Pushing a Configuration URL Through a Mode-Configuration Exchange: Examples

The following **show crypto ipsec client ezvpn** command output displays the mode configuration URL location and version:

```

Router# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 5

Tunnel name : branch
Inside interface list: Vlan1
Outside interface: FastEthernet0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 172.16.1.209
Mask: 255.255.255.255
Default Domain: cisco.com
Save Password: Allowed
Configuration URL [version]: tftp://172.16.30.2/branch.cfg [11]
Config status: applied, Last successfully applied version: 11
Current EzVPN Peer: 192.168.10.1

```

The following **show crypto isakmp peers config** command output displays all manageability information that is sent by the remote device.

```

Router# show crypto isakmp peers config

Client-Public-Addr=192.168.10.2:500; Client-Assigned-Addr=172.16.1.209;
Client-Group=branch; Client-User=branch; Client-Hostname=branch.; Client-Platform=Cisco
1711; Client-Serial=FOC080210E2 (412454448); Client-Config-Version=11;
Client-Flash=33292284; Client-Available-Flash=10202680; Client-Memory=95969280;
Client-Free-Memory=14992140; Client-Image=flash:c1700-advipservicesk9-mz.ef90241;
Client-Public-Addr=192.168.10.3:500; Client-Assigned-Addr=172.16.1.121;
Client-Group=store; Client-User=store; Client-Hostname=831-storerouter.;
Client-Platform=Cisco C831; Client-Serial=FOC08472UXR (1908379618);
Client-Config-Version=2; Client-Flash=24903676; Client-Available-Flash=5875028;
Client-Memory=45298688; Client-Free-Memory=6295596;
Client-Image=flash:c831-k9o3y6-mz.ef90241

```

## Per User AAA Policy Download with PKI: Example

The following output shows that the Per User AAA Policy Download with PKI feature has been configured on the Easy VPN server.

```

Router# show running-config

Building configuration...

```

```

Current configuration : 7040 bytes
!
! Last configuration change at 21:06:51 UTC Tue Jun 28 2005
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname GEN
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa group server radius usrgppki
server 10.76.248.201 auth-port 1645 acct-port 1646
!
aaa authentication login xauth group usrgppki
aaa authentication login usrgpp group usrgppki
aaa authorization network usrgpp group usrgppki
!
aaa session-id common
!
resource policy
!
ip subnet-zero
!
!
ip cef
!
!
ip address-pool local
!
!
crypto pki trustpoint ca-server
enrollment url http://10.7.7.2:80
revocation-check none
rsa-keypair rsa-pair
! Specify the field within the certificate that will be used as a username to do a
per-user AAA lookup into the RADIUS database. In this example, the contents of the
commonname will be used to do a AAA lookup. In the absence of this statement, by default
the contents of the "unstructured name" field in the certificate is used for AAA lookup.
authorization username subjectname commonname
!
!
crypto pki certificate map CERT-MAP 1
subject-name co yourname
name co yourname
!
crypto pki certificate chain ca-server
certificate 02
308201EE 30820157 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 63612D73 65727665 72301E17 0D303530 36323832
30303731 345A170D 30363036 32383230 30373134 5A301531 13301106 092A8648
86F70D01 09021604 47454E2E 30819F30 0D06092A 864886F7 0D010101 05000381
8D003081 89028181 00ABF8F0 FDFDF8D F22098D6 A48EE0C3 F505DD96 C0022EA4
EAB95EE8 1F97F450 990BB0E6 F2B7151F C5C79391 93822FE4 DEE5B00C A03412BB
9B715AAD D6C31F93 D8802658 AF9A8866 63811942 913D0C02 C3E328CC 1C046E94

```

```

F73B7C1A 4497F86E 74A627BC B809A3ED 293C15F2 8DCFA217 5160F9A4 09D52044
350F85AF 08B357F5 D7020301 0001A34F 304D300B 0603551D 0F040403 0205A030
1F060355 1D230418 30168014 F9BC4498 3DA4D51D 451EFEFD 5B1F5F73 8D7B1C9B
301D0603 551D0E04 1604146B F6B2DFD1 1FE237FF 23294129 E55D9C48 CCB04630
0D06092A 864886F7 0D010104 05000381 81004AFF 2BE300C1 15D0B191 C20D06E0
260305A6 9DF610BB 24211516 5AE73B62 78E01FE4 0785776D 3ADFA3E2 CE064432
1C93E82D 93B5F2AB 9661EDD3 499C49A8 F87CA553 9132F239 1D50187D 21CC3148
681F5043 2F2685BC F544F4FF 8DF535CB E55B5F36 31FFF025 8969D9F8 418C8AB7
C569B022 46C3C63A 22DD6516 C503D6C8 3D81
quit
certificate ca 01
30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 63612D73 65727665 72301E17 0D303530 36323832
30303535 375A170D 30383036 32373230 30353537 5A301431 12301006 03550403
13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 BA1A4413 96339C6B D36BD720 D25C9A44 E0627A29 97E06F2A
69B268ED 08C7144E 7058948D BEA512D4 40588B87 322C5D79 689427CA 5C54B3BA
82FAEC53 F6AC0B5C 615D032C 910CA203 AC6AB681 290D9EED D31EB185 8D98E1E7
FF73613C 32290FD6 A0CBDC40 6E4D6B39 DE1D86BA DE77A55E F15299FF 97D7C185
919F81C1 30027E0F 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 168014F9
BC44983D A4D51D45 1EFEFD5B 1F5F738D 7B1C9B30 1D060355 1D0E0416 0414F9BC
44983DA4 D51D451E FEFD5B1F 5F738D7B 1C9B300D 06092A86 4886F70D 01010405
00038181 003EF397 F4D98BDE A4322FAF 4737800F 1671F77E BD6C45AE FB91B28C
F04C98F0 135A40C6 635FDC29 63C73373 5D5BBC9A F1BBD235 F66CE1AD 6B4BFC7A
AB18C8CC 1AB93AF3 7AC67436 930E9C81 F43F7570 A8FE09AE 3DEA01D1 DA6BD0CB
83F9A77F 1DFAFE5E 2F1F206B F1FDD8BE 6BB57A3C 8D03115D B1F64A3F 7A7557C1
09B0A34A DB
quit
!
!
crypto isakmp policy 10
group 2
crypto isakmp keepalive 10
crypto isakmp profile ISA-PROF
match certificate CERT-MAP
isakmp authorization list usrgp
client pki authorization list usrgp
client configuration address respond
client configuration group pkiuser
virtual-template 2
!
!
crypto ipsec transform-set trans2 esp-3des esp-sha-hmac
!
crypto ipsec profile IPSEC_PROF
set transform-set trans2
!
crypto ipsec profile ISC_IPSEC_PROFILE_1
set transform-set trans2
!
!
crypto call admission limit ike sa 40
!
!
interface Loopback0
ip address 10.3.0.1 255.255.255.255
no ip route-cache cef
no ip route-cache
!
interface Loopback1
ip address 10.76.0.1 255.255.255.255
no ip route-cache cef
no ip route-cache

```



```
!
interface Ethernet3/0
 ip address 10.76.248.209 255.255.255.255
 no ip route-cache cef
 no ip route-cache
 duplex half
!
!
interface Ethernet3/2
 ip address 10.2.0.1 255.255.255.0
 no ip route-cache cef
 no ip route-cache
 duplex half
!
!
interface Serial4/0
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 serial restart-delay 0
!
interface Serial4/1
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 serial restart-delay 0
!
interface Serial4/2
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 serial restart-delay 0
!
interface Serial4/3
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 serial restart-delay 0
!
interface FastEthernet5/0
 ip address 10.9.4.77 255.255.255.255
 no ip route-cache cef
 no ip route-cache
 duplex half
!
interface FastEthernet6/0
 ip address 10.7.7.1 255.255.255.0
 no ip route-cache cef
 no ip route-cache
 duplex full
!
interface Virtual-Template1
 no ip address
!
interface Virtual-Template2 type tunnel
 ip unnumbered Loopback0
 tunnel source Ethernet3/2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC_PROF
!
```

```

router eigrp 20
 network 172.16.0.0
 auto-summary
!
ip local pool ourpool 10.6.6.6
ip default-gateway 10.9.4.1
ip classless
ip route 10.1.0.1 255.255.255.255 10.0.0.2
ip route 10.2.3.0 255.255.0.0 10.2.4.4
ip route 10.9.1.0 255.255.0.0 10.4.0.1
ip route 10.76.0.0 255.255.0.0 10.76.248.129
ip route 10.11.1.1 255.255.255.0 10.7.7.2
!
no ip http server
no ip http secure-server
!
!
logging alarm informational
arp 10.9.4.1 0011.bcb4.d40a ARPA
!
!
radius-server host 10.76.248.201 auth-port 1645 acct-port 1646 key cisco
!
control-plane
!
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
!
!
end

```

## Per-User Attributes on an Easy VPN Server: Example

The following example shows that per-user attributes have been configured on an Easy VPN server.

```

!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login noAAA none
aaa authorization network default local
!
aaa attribute list per-group
 attribute type inacl "per-group-acl" service ike protocol ip mandatory
!
aaa session-id common
!
resource policy
!
ip subnet-zero
!
!

```

```
ip cef
!
!
username example password 0 example
!
!
crypto isakmp policy 3
 authentication pre-share
 group 2
crypto isakmp xauth timeout 90
!
crypto isakmp client configuration group PerUserAAA
 key cisco
 pool dpool
 crypto aaa attribute list per-group
!
crypto isakmp profile vi
 match identity group PerUserAAA
 isakmp authorization list default
 client configuration address respond
 client configuration group PerUserAAA
 virtual-template 1
!
!
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
!
interface GigabitEthernet0/0
 description 'EzVPN Peer'
 ip address 192.168.1.1 255.255.255.128
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto

interface Virtual-Templat1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.5.0.1 10.5.0.10
ip classless
!
no ip http server
no ip http secure-server
!
!
ip access-list extended per-group-acl
 permit tcp any any
 deny icmp any any
logging alarm informational
logging trap debugging
```

```

!
control-plane
!
gatekeeper
 shutdown
!
line con 0
line aux 0
 stopbits 1
line vty 0 4
!
!
end

```

## Network Admission Control: Example

The following is output for an Easy VPN server that has been enabled with Network Admission Control.



### Note

Network Admission Control is supported on an Easy VPN server only when the server uses IPsec virtual interfaces. Network Admission Control is enabled on the virtual template interface and applies to all PC clients that use this virtual template interface.

```

Router# show running-config

Building configuration...

Current configuration : 5091 bytes
!
version 12.4
!
hostname Router
!

aaa new-model
!
!
aaa authentication login userlist local
!
aaa authentication eou default group radius
aaa authorization network hw-client-groupname local
aaa accounting update newinfo
aaa accounting network acclist start-stop broadcast group radius
aaa session-id common
!
!
! Note 1: EAPoUDP packets will use the IP address of the loopback interface when sending
the EAPoUDP hello to the Easy VPN client. Using the IP address ensures that the returning
EAPoUDP packets come back encrypted and are associated with the correct virtual access
interface. The ip admission (ip admission source-interface Loopback10) command is
optional. Instead of using this command, you can specify the IP address of the virtual
template to be an address in the inside network space as shown in the configuration of the
virtual template below in Note 2.
ip admission source-interface Loopback10
ip admission name test eapoudp inactivity-time 60
!
!
eou clientless username cisco
eou clientless password cisco
eou allow ip-station-id

```

```
eou logging
!
username lab password 0 lab
username lab@easy password 0 lab
!
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
!
!
crypto isakmp key 0 cisco address 10.53.0.1
crypto isakmp client configuration group easy
 key cisco
 domain cisco.com
 pool dynpool
 acl split-acl
 group-lock
 configuration url tftp://10.13.0.9/Config-URL_TFTP.cfg
 configuration version 111
!
crypto isakmp profile vi
 match identity group easy
 client authentication list userlist
 isakmp authorization list hw-client-groupname
 client configuration address respond
 client configuration group easy
 accounting acclist
 virtual-template 2
!
crypto ipsec security-association lifetime seconds 120
crypto ipsec transform-set set esp-3des esp-sha-hmac
crypto ipsec transform-set aes-trans esp-aes esp-sha-hmac
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
crypto ipsec profile vi
 set security-association lifetime seconds 3600
 set transform-set set aes-trans transform-1
 set isakmp-profile vi
!
!
crypto dynamic-map dynmap 1
 set transform-set aes-trans transform-1
 reverse-route
!

interface Loopback10
 ip address 10.61.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.13.11.173 255.255.255.255
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.55.0.1 255.255.255.255
 duplex auto
 speed auto
!
!
interface Virtual-Template2 type tunnel
```

```

! Note2: Use the IP address of the loopback10. This ensures that the EAPoUDP packets that
are attached to virtual-access interfaces that are cloned from this virtual template carry
the source address of the loopback address and that response packets from the VPN client
come back encrypted.
!
ip unnumbered Loopback10
! Enable Network Admission Control for remote VPN clients.
ip admission test
tunnel mode ipsec ipv4
tunnel protection ipsec profile vi
!
!
ip local pool dynpool 172.16.2.65 172.16.2.70
ip classless
ip access-list extended ClientException
permit ip any host 10.61.0.1
ip access-list extended split-acl
permit ip host 10.13.11.185 any
permit ip 10.61.0.0 255.255.255.255 any
permit ip 10.71.0.0 255.255.255.255 any
permit ip 10.71.0.0 255.255.255.255 10.52.0.0 0.255.255.255
permit ip 10.55.0.0 255.255.255.255 any
!
ip radius source-interface FastEthernet0/0
access-list 102 permit esp any any
access-list 102 permit ahp any any
access-list 102 permit udp any any eq 21862
access-list 102 permit ospf any any
access-list 102 deny ip any any
access-list 195 deny ospf any any
access-list 195 permit ip 10.61.0.0 255.255.255.255 10.51.0.0 255.255.255.255
!
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server host 10.13.11.185 auth-port 1645 acct-port 1646 key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
end

```

## Configuring Password Aging: Example

The following example shows that password aging has been configured so that if the password expires, the Easy VPN client is notified.

```

Current configuration : 4455 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname xinl-gateway
!
boot-start-marker
boot system flash c2800nm-advsecurityk9-mz.124-7.9.T
boot-end-marker
!
!
aaa new-model
!

```

```
!
aaa authentication login USERAUTH passwd-expiry group radius aaa authorization network
branch local !
aaa session-id common
!

ip cef

username cisco privilege 15 secret 5 1A3HU$bCWj1krEztDJx6JJzSnMV1 !
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool !
crypto isakmp client configuration group branch
 key cisco
 domain cisco.com
 pool dynpool
!
!
crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac !
crypto isakmp profile profile2
 client authentication list USERAUTH
 match identity group branch
 isakmp authorization list branch
 client configuration address respond
 virtual-template 1

crypto ipsec profile vi
 set transform-set transform-1

interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
 ip address 192.168.1.100 255.255.255.0
 duplex auto
 speed auto
 crypto map dynmap
!
interface GigabitEthernet0/1
 description ES_LAN
 ip address 172.19.217.96 255.255.255.0
 duplex auto
 speed auto

!
!interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 no clns route-cache
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.0.0.1 10.0.0.3

!
radius-server host 172.19.220.149 auth-port 1645 acct-port 1646 key cisco radius-server
vsa send authentication !
control-plane
!
!
end
```

## Split DNS: Examples

In the following example, the split tunnel list named “101” contains the 10.168.0.0/16 network. It is necessary to include this network information so that the DNS requests to the internal DNS server of 10.168.1.1 are encrypted.

```
crypto isakmp client configuration group home
 key abcd
 acl 101
 dns 10.168.1.1. 10.168.1.2
```

### show Output

The following **show** command output example shows that `www.ciscoexample1.com` and `www.ciscoexample2.com` have been added to the policy group:

```
Router# show running-config | security group

crypto isakmp client configuration group 831server
key abcd
dns 10.104.128.248
split-dns www.ciscoexample1.com
split-dns www.ciscoexample2.com
group home2 key abcd
```

The following **show** command output example displays currently configured DNS views:

```
Router# show ip dns view

DNS View default parameters:
Logging is off
DNS Resolver settings:
 Domain lookup is enabled
 Default domain name: cisco.com
 Domain search list:
 Lookup timeout: 3 seconds
 Lookup retries: 2
 Domain name-servers:
 172.16.168.183
DNS Server settings:
 Forwarding of queries is enabled
 Forwarder addresses:

DNS View ezvpn-internal-view parameters:
Logging is off
DNS Resolver settings:
 Domain lookup is enabled
 Default domain name:
 Domain search list:
 Lookup timeout: 3 seconds
 Lookup retries: 2
 Domain name-servers:
 10.104.128.248
DNS Server settings:
 Forwarding of queries is enabled
 Forwarder addresses:
```

The following **show** command output example displays currently configured DNS view lists.

```
Router# show ip dns view-list

View-list ezvpn-internal-viewlist:
View ezvpn-internal-view:
 Evaluation order: 10
```



```

Restrict to ip dns name-list: 1
View default:
Evaluation order: 20

```

The following **show** command output displays DNS name lists.

```
Router# show ip dns name-list
```

```

ip dns name-list 1
 permit www.ciscoexample1.com
 permit www.ciscoexample2.com

```

## DHCP Client Proxy: Examples

The following examples display DHCP client proxy output information using **show** and **debug** commands.

### show Output



#### Note

To use the **show ip dhcp** command, the DHCP server must be a Cisco IOS server.

The following **show ip dhcp pool** command output provides information about the DHCP parameters:

```
Router# show ip dhcp pool
```

```

Pool dynpool :
 Utilization mark (high/low) : 100 / 0
 Subnet size (first/next) : 0 / 0
 Total addresses : 254
 Leased addresses : 1
 Pending event : none
 1 subnet is currently in the pool:
 Current index IP address range Leased addresses
 10.3.3.1 - 10.3.3.254 1
 No relay targets associated with class aclass

```

The following **show ip dhcp** command output provides information about the DHCP bindings:

```
Router# show ip dhcp binding
```

```

Bindings from all pools not associated with VRF:
IP address Client-ID/ Lease expiration Type
 Hardware address/User name
10.3.3.5 0065.7a76.706e.2d63. Apr 04 2006 06:01 AM Automatic
6c69.656e.74

```

### debug Output

The following example shows how the **debug crypto isakmp** and **debug ip dhcp server events** commands can be used to troubleshoot your DHCP client proxy support configuration:

```

*Apr 3 06:01:32.047: ISAKMP: Config payload REQUEST *Apr 3 06:01:32.047:
ISAKMP:(1002):checking request:
*Apr 3 06:01:32.047: ISAKMP: IP4_ADDRESS
*Apr 3 06:01:32.047: ISAKMP: IP4_NETMASK
*Apr 3 06:01:32.047: ISAKMP: MODECFG_CONFIG_URL
*Apr 3 06:01:32.047: ISAKMP: MODECFG_CONFIG_VERSION
*Apr 3 06:01:32.047: ISAKMP: IP4_DNS
*Apr 3 06:01:32.047: ISAKMP: IP4_DNS
*Apr 3 06:01:32.047: ISAKMP: IP4_NBNS

```

```

*Apr 3 06:01:32.047: ISAKMP: IP4_NBNS
*Apr 3 06:01:32.047: ISAKMP: SPLIT_INCLUDE
*Apr 3 06:01:32.047: ISAKMP: SPLIT_DNS
*Apr 3 06:01:32.047: ISAKMP: DEFAULT_DOMAIN
*Apr 3 06:01:32.047: ISAKMP: MODECFG_SAVEPWD
*Apr 3 06:01:32.047: ISAKMP: INCLUDE_LOCAL_LAN
*Apr 3 06:01:32.047: ISAKMP: PFS
*Apr 3 06:01:32.047: ISAKMP: BACKUP_SERVER
*Apr 3 06:01:32.047: ISAKMP: APPLICATION_VERSION
*Apr 3 06:01:32.047: ISAKMP: MODECFG_BANNER
*Apr 3 06:01:32.047: ISAKMP: MODECFG_IPSEC_INT_CONF
*Apr 3 06:01:32.047: ISAKMP: MODECFG_HOSTNAME
*Apr 3 06:01:32.047: ISAKMP/author: Author request for group homesuccessfully sent to AAA
*Apr 3 06:01:32.047: ISAKMP:(1002):Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST

*Apr 3 06:01:32.047: ISAKMP:(1002):Old State = IKE_P1_COMPLETE New State =
IKE_CONFIG_AUTHOR_AAA_AWAIT

*Apr 3 06:01:32.047: ISAKMP:(1002):attributes sent in message:
*Apr 3 06:01:32.047: Address: 10.2.0.0
*Apr 3 06:01:32.047: Requesting DHCP Server0 address 10.3.3.3 *Apr 3 06:01:32.047:
DHCPD: Sending notification of DISCOVER:
*Apr 3 06:01:32.047: DHCPD: htype 1 chaddr aabb.cc00.6600
*Apr 3 06:01:32.047: DHCPD: circuit id 00000000
*Apr 3 06:01:32.047: DHCPD: Seeing if there is an internally specified pool class:
*Apr 3 06:01:32.047: DHCPD: htype 1 chaddr aabb.cc00.6600
*Apr 3 06:01:32.047: DHCPD: circuit id 00000000

*Apr 3 06:01:34.063: DHCPD: Adding binding to radix tree (10.3.3.5) *Apr 3 06:01:34.063:
DHCPD: Adding binding to hash tree *Apr 3 06:01:34.063: DHCPD: assigned IP address
10.3.3.5 to client 0065.7a76.706e.2d63.6c69.656e.74.
*Apr 3 06:01:34.071: DHCPD: Sending notification of ASSIGNMENT:
*Apr 3 06:01:34.071: DHCPD: address 10.3.3.5 mask 255.255.255.0
*Apr 3 06:01:34.071: DHCPD: htype 1 chaddr aabb.cc00.6600
*Apr 3 06:01:34.071: DHCPD: lease time remaining (secs) = 86400
*Apr 3 06:01:34.183: Obtained DHCP address 10.3.3.5 *Apr 3 06:01:34.183:
ISAKMP:(1002):allocating address 10.3.3.5 *Apr 3 06:01:34.183: ISAKMP: Sending private
address: 10.3.3.5 *Apr 3 06:01:34.183: ISAKMP: Sending subnet mask: 255.255.255.0

```

## cTCP Session: Example

The following **debug crypto tcp** command output displays information about a cTCP session, and it includes comments about the output:

```
Router# debug crypto tcp
```

```

! In the following two lines, a cTCP SYN packet is received from the client, and the cTCP
connection is created.
*Sep 26 11:14:37.135: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
created
*Sep 26 11:14:37.135: cTCP: SYN from 10.76.235.21:3519
! In the following line, the SYN acknowledgement is sent to the client.
*Sep 26 11:14:37.135: cTCP: Sending SYN(680723B2)ACK(100C637) to 10.76.235.21:3519
! In the following two lines, an acknowledgement is received, and connection setup is
complete. IKE packets should now be received on this newly created cTCP session.
*Sep 26 11:14:37.135: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
found
*Sep 26 11:14:37.135: cTCP: ACK from 10.76.235.21:3519
*Sep 26 11:14:37.727: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
found

```

```

*Sep 26 11:14:37.731: cTCP: updating PEER Seq number to 168288031
*Sep 26 11:14:37.731: cTCP: Pak with contiguous buffer
*Sep 26 11:14:37.731: cTCP: mangling IKE packet from peer: 10.76.235.21:500->3519
 10.76.248.239:500->500
*Sep 26 11:14:37.731: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
found
*Sep 26 11:14:37.799: cTCP: demangling outbound IKE packet: 10.76.248.239:500->500
 10.76.235.21:3519->500
*Sep 26 11:14:37.799: cTCP: encapsulating IKE packet
*Sep 26 11:14:37.799: cTCP: updating LOCAL Seq number to 17452987271
! The above lines show that after the required number of IKE packets are exchanged, IKE
and IPsec SAs are created.
*Sep 26 11:14:40.335: cTCP: updating PEER Seq number to 168304311
*Sep 26 11:14:40.335: cTCP: Pak with particles
*Sep 26 11:14:40.335: cTCP: encapsulating pak
*Sep 26 11:14:40.339: cTCP: datagramstart 0xF2036D8, network_start 0xF2036D8, size 112
*Sep 26 11:14:40.339: cTCP: Pak with contiguous buffer
*Sep 26 11:14:40.339: cTCP: allocated new buffer
*Sep 26 11:14:40.339: cTCP: updating LOCAL Seq number to 17452995351
*Sep 26 11:14:40.339: IP: s=10.76.248.239 (local), d=10.76.235.21 (FastEthernet1/1), len
148, cTCP
! The above lines show that Encapsulating Security Payload (ESP) packets are now being
sent and received.

```

## VRF Assignment by a AAA Server: Example

The following output example shows that neither a VRF nor an IP address has been defined:

```

aaa new-model
aaa authentication login VPN group radius
aaa authorization network VPN group radius
!
ip vrf example1
rd 1:1
!
crypto isakmp profile example1
match identity group example1group
client authentication list VPN
isakmp authorization list VPN
client configuration address respond
virtual-template 10
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
crypto ipsec profile example1
set transform-set TS
set isakmp-profile example1
!
interface Virtual-Template10 type tunnel
! The next line shows that neither VRF nor an IP address has been defined.
no ip address
tunnel mode ipsec ipv4
tunnel protection ipsec profile example1

```

## Additional References

The following sections provide references related to Easy VPN Server.aaa new-model

## Related Documents

| Related Topic                        | Document Title                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring a router as a VPN client | <a href="#"><i>Cisco Easy VPN Remote</i></a>                                                                                                                                                                                                                                                                                          |
| General information on IPsec and VPN | <ul style="list-style-type: none"> <li>• <a href="#"><i>Cisco IOS Security Command Reference</i></a></li> <li>• <a href="#"><i>Configuring Internet Key Exchange for IPsec VPNs</i></a></li> <li>• <a href="#"><i>Cisco Easy VPN Remote</i></a></li> <li>• <a href="#"><i>IPsec VPN High Availability Enhancements</i></a></li> </ul> |
| IPsec virtual tunnels                | <a href="#"><i>IPsec Virtual Tunnel Interface</i></a>                                                                                                                                                                                                                                                                                 |
| Network Admission Control            | <a href="#"><i>Network Admission Control</i></a>                                                                                                                                                                                                                                                                                      |
| RRI                                  | <ul style="list-style-type: none"> <li>• <a href="#"><i>IPsec VPN High Availability Enhancements</i></a></li> <li>• <a href="#"><i>Reverse Route Injection</i></a></li> </ul>                                                                                                                                                         |
| Split DNS                            | <a href="#"><i>Configuring Split and Dynamic DNS on the Cisco VPN 3000</i></a>                                                                                                                                                                                                                                                        |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features.

- **aaa authentication login**
- **access-restrict**
- **acl (ISAKMP)**
- **auto-update client**
- **backup-gateway**
- **banner**
- **browser-proxy**
- **clear crypto ctp**
- **clear crypto session**
- **client authentication list**
- **client pki authorization list**
- **configuration url**
- **configuration version**
- **crypto aaa attribute list**
- **crypto ctp**
- **crypto ipsec server send-update**
- **crypto isakmp client configuration browser-proxy**
- **crypto isakmp client configuration group**
- **crypto isakmp client firewall**
- **crypto logging ezvpn**
- **debug crypto ctp**
- **debug crypto condition**

- **debug ip dns name-list**
- **debug ip dns view**
- **debug ip dns view-list**
- **dhcp server (isakmp)**
- **dhcp timeout**
- **domain (isakmp-group)**
- **firewall are-u-there**
- **firewall policy**
- **group-lock**
- **include-local-lan**
- **key (isakmp-group)**
- **max-logins**
- **max-users**
- **pfs**
- **policy**
- **pool (isakmp-group)**
- **proxy**
- **save-password**
- **show crypto ctp**
- **show crypto debug-condition**
- **show crypto isakmp peers**
- **show crypto isakmp profile**
- **show crypto isakmp sa**
- **show crypto session**
- **show crypto session group**
- **show crypto session summary**
- **show ip dns name-list**
- **show ip dns view**
- **show ip dns view-list**
- **split-dns**
- **wins**
- **Glossary**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

# Feature Information for Easy VPN Server

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for Easy VPN Server

| Feature Name    | Releases                | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Easy VPN Server | 12.2(8)T                | The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x and later software clients and Cisco VPN hardware clients (such as the Cisco 800, Cisco 900, Cisco 1700, VPN 3002, and PIX 501 devices). This feature allows a remote end user to communicate using IP Security (IPsec) with any Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPsec policies are “pushed” to the client device by the server, minimizing configuration by the end user. |
|                 | 12.3(2)T                | RADIUS support for user profiles, user-based policy control, session monitoring for VPN group access, backup-gateway list, and PFS were added.                                                                                                                                                                                                                                                                                                                                                           |
|                 | 12.3(7)T                | The <b>netmask</b> command was integrated for use on the Easy VPN server.<br><br>For information about configuring this command, see the following section: <ul style="list-style-type: none"> <li>Defining Group Policy Information for Mode Configuration Push, page 21</li> </ul>                                                                                                                                                                                                                     |
|                 | 12.4(2)T<br>12.2(33)SXH | The following feature was added in this release: <ul style="list-style-type: none"> <li>Banner, Auto-Update, and Browser Proxy Enhancements</li> </ul>                                                                                                                                                                                                                                                                                                                                                   |

**Table 3**      *Feature Information for Easy VPN Server (continued)*

| Feature Name | Releases                | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | 12.4(4)T<br>12.2(33)SXH | <p>The following features were added in this release:</p> <ul style="list-style-type: none"> <li>• Configuration Management Enhancements (Pushing a Configuration URL Through a Mode-Configuration Exchange)</li> <li>• Per User AAA Policy Download with PKI</li> <li>• Syslog Message Enhancements</li> <li>• Network Admission Control for Easy VPN</li> <li>• Password Aging</li> <li>• Virtual IPsec Interface Support</li> </ul> |
|              | 12.4(6)T                | The Central Policy Push Firewall Policy Push feature was added.                                                                                                                                                                                                                                                                                                                                                                        |
|              | 12.2(33)SRA             | This feature was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                                                                                                                                                                                                                                        |



**Table 3**      *Feature Information for Easy VPN Server (continued)*

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | 12.4(9)T | <p>The following features were added in this release:</p> <ul style="list-style-type: none"> <li>• DHCP Client Proxy<br/>The following section provides information about this feature:<br/>– <a href="#">DHCP Client Proxy, page 11</a></li> <li>• Virtual Tunnel Interface Per-User Attribute Support for Easy VPN Servers.<br/>– <a href="#">Virtual Tunnel Interface Per-User Attribute Support, page 13</a></li> <li>• Split DNS<br/>The following section provides information about this feature:<br/>– <a href="#">Split DNS, page 18</a></li> <li>• cTCP<br/>The following sections provide information about this feature:<br/>– <a href="#">cTCP, page 18</a><br/>– <a href="#">Configuring cTCP, page 50</a><br/>– <a href="#">cTCP Session: Example, page 70</a></li> <li>• Per-User Attribute Support for Easy VPN Servers<br/>The following sections provide information about this feature:<br/>– <a href="#">Per-User Attribute Support for Easy VPN Servers, page 15</a><br/>– <a href="#">Configuring Per-User Attributes on a Local Easy VPN AAA Server, page 38</a><br/>– <a href="#">Per-User Attributes on an Easy VPN Server: Example, page 62</a></li> <li>• VRF Assignment by a AAA Server<br/>The following sections provide information about this feature:<br/>– <a href="#">VRF Assignment by a AAA Server, page 19</a><br/>– <a href="#">VRF Assignment by a AAA Server: Example, page 71</a></li> </ul> <p>The following new commands were introduced: <b>crypto aaa attribute list</b>, <b>debug ip dns</b>, <b>dhcp-server (isakmp)</b>, <b>dhcp-timeout</b>, <b>show ip dns name-list</b>, <b>show ip dns view</b>, and <b>show ip dns view-list</b></p> <p>The following commands were modified: <b>crypto isakmp client configuration group</b></p> |

**Table 3**      **Feature Information for Easy VPN Server (continued)**

| Feature Name                | Releases                 | Feature Information                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | 12.4(11)T                | The DHCP Client Proxy feature was updated to include manageability enhancements for remote access VPNs.<br><br>The following commands were modified: <b>clear crypto session, crypto isakmp client configuration group, debug crypto condition, show crypto debug-condition, show crypto isakmp peers, show crypto isakmp profile, show crypto isakmp sa, show crypto session</b> |
| EasyVPN Server Enhancements | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                     |

# Glossary

**AAA**—authentication, authorization, and accounting. Framework of security services that provides the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

**aggressive mode (AM)**—Mode during Internet Key Exchange negotiation. Compared to main mode (MM), AM eliminates several steps, which makes it faster but less secure than MM. Cisco IOS software will respond in aggressive mode to an Internet Key Exchange (IKE) peer that initiates aggressive mode.

**AV pair**—attribute-value pair. Additional authentication and authorization information in the following format: Cisco:AVPair="protocol:attribute=value".

**IKE**—Internet Key Exchange. Hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. Although IKE can be used with other protocols, its initial implementation is with IPsec. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations.

**IPsec**—IP Security Protocol. Framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

**ISAKMP**—Internet Security Association Key Management Protocol. Protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.

**MM**—main mode. Mode that is slower than aggressive mode but more secure and more flexible than aggressive mode because it can offer an IKE peer more security proposals. The default action for IKE authentication (Rivest, Shamir, and Adelman signature (rsa-sig), RSA encryption (rsa-encr), or preshared) is to initiate main mode.

**policy push**—Allows administrators to push policies that enforce security to the Cisco Easy VPN (software) Client and related firewall software.

**reverse route injection (RRI)**—Simplified network design for VPNs on which there is a requirement for redundancy or load balancing. RRI works with both dynamic and static crypto maps.

In the dynamic case, as remote peers establish IPsec security associations with an RRI enabled router, a static route is created for each subnet or host protected by that remote peer. For static crypto maps, a static route is created for each destination of an extended access-list rule.

**SA**—security association. Description of how two or more entities will utilize security services to communicate securely. For example, an IPsec SA defines the encryption algorithm (if used), the authentication algorithm, and the shared session key to be used during the IPsec connection.

Both IPsec and IKE require and use SAs to identify the parameters of their connections. IKE can negotiate and establish its own SA. The IPsec SA is established either by IKE or by manual user configuration.

**VPN**—Virtual Private Network. Framework that consists of multiple peers transmitting private data securely to one another over an otherwise public infrastructure. In this framework, inbound and outbound network traffic is protected using protocols that tunnel and encrypt all data. This framework permits networks to extend beyond their local topology, while remote users are provided with the appearance and functionality of a direct network connection.

**Note**

---

Refer to *[Internetworking Terms and Acronyms](#)* for terms not included in this glossary.

---

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

---

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.