



Easy VPN Server

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.

Feature History for Easy VPN Server

Release	Modification
12.2(8)T	This feature was introduced.
12.3(2)T	New attributes were added to the server group, and the following commands, which correspond to the added attributes, were added: access-restrict, firewall are-u-there, group-lock, include-local-lan, and save-password.
12.3(4)T	RADIUS support for user profiles, user-based policy control, session monitoring for VPN group access, backup-gateway list, and PFS were added.
12.4(2)T	The following features were added in this release: <ul style="list-style-type: none">• Virtual IPsec Interface Support• Banner, Auto-Update, and Browser Proxy Enhancements
12.4(4)T	The following features were added in this release: <ul style="list-style-type: none">• Configuration Management Enhancements (Pushing a Configuration URL Through a Mode-Configuration Exchange)• Per User AAA Policy Download with PKI• Syslog Message Enhancements• Network Admission Control for Easy VPN



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

Copyright © 2003–2005 Cisco Systems, Inc. All rights reserved.

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 Easy VPN Server, page 2](#)
- [Information About Easy VPN Server, page 3](#)
- [How to Configure Easy VPN Server, page 15](#)
- [Configuration Examples for Easy VPN Server, page 35](#)
- [Additional References, page 46](#)
- [Command Reference, page 47](#)
- [Glossary, page 49](#)

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 Digital Signature Standard (DSS)
Diffie-Hellman (D-H) groups	1
IPsec Protocol Identifier	IPSEC_AH
IPsec Protocol Mode	Transport mode
Miscellaneous	Manual keys 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, Domain Name Service (DNS), and split tunnel access. Thus, customers must continue to use existing, globally defined parameters for IP address assignment, Windows Internet Naming Service (WINS) and DNS, and preshared keys.

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.

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.

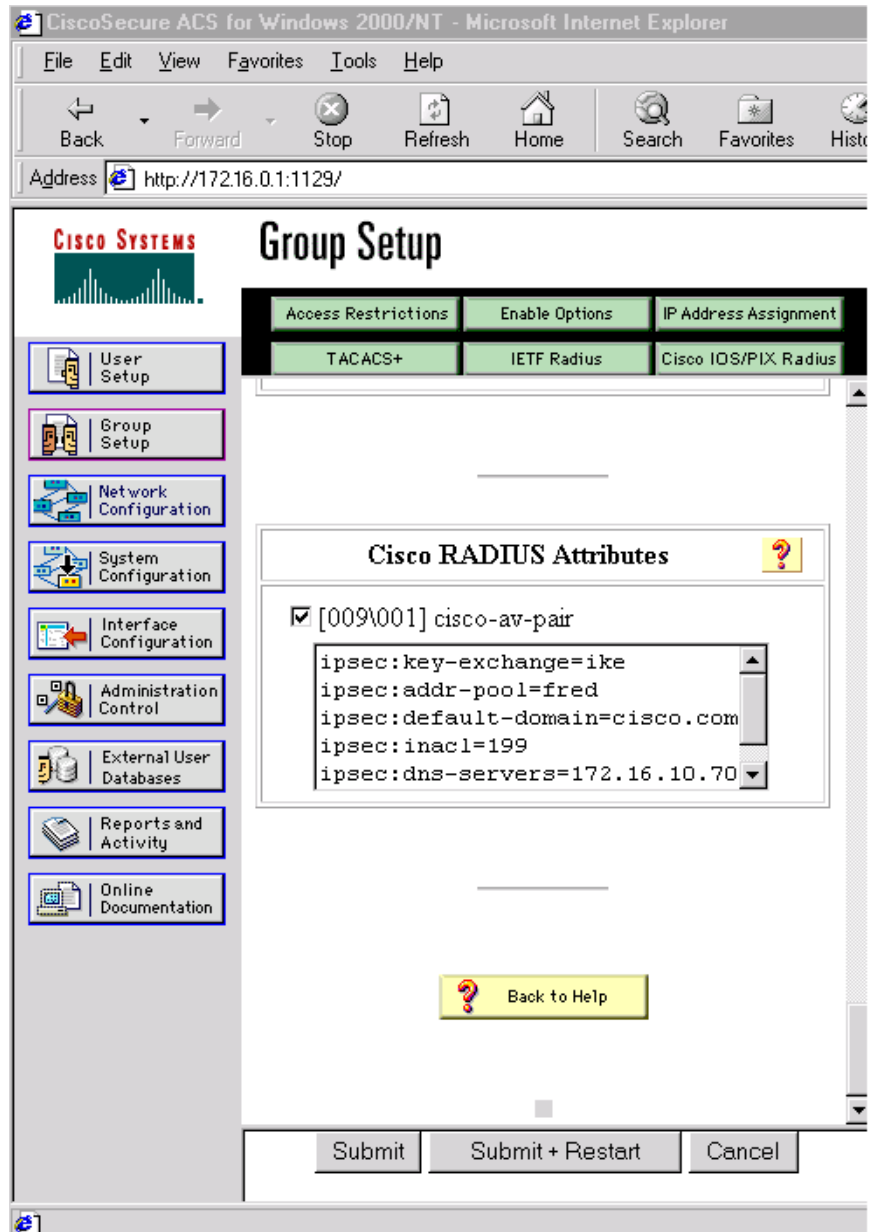
To define group policy attributes for RADIUS, you must do the following task on your RADIUS server:

- 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



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 attribute. 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

CISCO SYSTEMS

Group Setup

Access Restrictions	Enable Options	IP Address Assignment
TACACS+	IETF Radius	Cisco IOS/PIX Radius

IETF RADIUS Attributes

- [006] Service-Type: Outbound
- [027] Session-Timeout: 0
- [028] Idle-Timeout: 0
- [064] Tunnel-Type:
 - Tag 1: Value IP ESP
 - Tag 2: Value
- [065] Tunnel-Medium-Type:
 - Tag 1: Value
 - Tag 2: Value
- [069] Tunnel-Password:
 - Tag 1: Value cisco
 - Tag 2: Value

Submit Submit + Restart Cancel

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

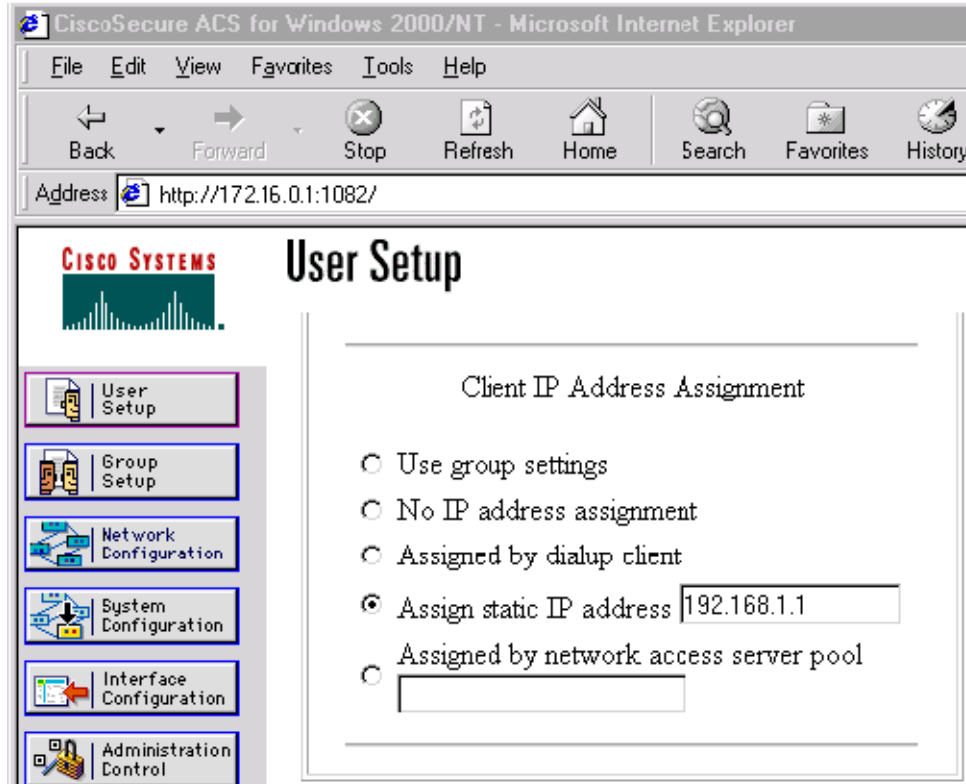
Attributes may also be applied on a per-user basis. If you apply attributes on a per-user basis, you can override a group attribute value with an individual user attribute. The attributes are retrieved at the time that user authentication via Xauth occurs. The attributes are then combined with group 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"> Hashed Message Authentication Codes with Message Digest 5 (HMAC-MD5) HMAC-Secure Hash Algorithm 1 (HMAC-SHA1)
Authentication Types	<ul style="list-style-type: none"> Preshared keys RSA digital signatures

Table 2 Supported IPsec Protocol Options and Attributes (continued)

Options	Attributes
D-H groups	<ul style="list-style-type: none"> • 2 • 5
Encryption Algorithms (IKE)	<ul style="list-style-type: none"> • Data Encryption Standard (DES) • Triple Data Encryption Standard (3DES)
Encryption Algorithms (IPsec)	<ul style="list-style-type: none"> • DES • 3DES • NULL
IPsec Protocol Identifiers	<ul style="list-style-type: none"> • Encapsulating Security Payload (ESP) • IP LZS compression (IPCOMP-LZS)
IPsec Protocol Mode	Tunnel mode

Functions Supported by Easy VPN Server

- [Mode Configuration Version 6 Support, page 9](#)
- [Xauth Version 6 Support, page 9](#)
- [IKE DPD, page 10](#)
- [Split Tunneling Control, page 10](#)
- [Initial Contact, page 10](#)
- [Group-Based Policy Control, page 10](#)
- [User-Based Policy Control, page 10](#)
- [Session Monitoring for VPN Group Access, page 12](#)
- [Easy VPN Virtual Interface Support on a Server, page 12](#)
- [Banner, Auto-Update, and Browser-Proxy, page 12](#)
- [Configuration Management Enhancements, page 13](#)
- [Per User AAA Policy Download with PKI, page 14](#)
- [Syslog Message Enhancements, page 14](#)
- [Network Admission Control Support for Easy VPN, page 15](#)

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.

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.

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 pre-shared 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 pre-shared 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 User-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
```

Easy VPN Virtual Interface Support on a Server

Easy VPN Virtual 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(2)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 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).

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.

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 43](#).

How to Configure Easy VPN Server

This section includes the following procedures:

- [Enabling Policy Lookup via AAA, page 16](#) (required)
- [Defining Group Policy Information for Mode Configuration Push, page 17](#) (required)
- [Enabling VPN Session Monitoring, page 20](#) (optional)
- [Verifying a VPN Session, page 21](#) (optional)
- [Applying Mode Configuration and Xauth, page 22](#) (required)
- [Enabling Reverse Route Injection for the Client, page 23](#) (optional)
- [Enabling IKE Dead Peer Detection, page 24](#) (optional)

- [Configuring RADIUS Server Support, page 25](#) (optional)
- [Verifying Easy VPN Server, page 26](#) (optional)
- [Configuring a Banner, page 26](#) (optional)
- [Configuring Auto Upgrade, page 27](#) (optional)
- [Configuring Browser Proxy, page 28](#) (optional)
- [Configuring the Pushing of a Configuration URL Through a Mode-Configuration Exchange, page 29](#)
- [Configuring Per User AAA Download with PKI, page 30](#) (optional)
- [Enabling Easy VPN Syslog Messages, page 34](#) (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	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 AAA.

	Command	Purpose
Step 4	aaa authentication password-prompt <i>text-string</i> Example: Router (config)# aaa authentication password-prompt "Enter your password now:"	(Optional) Changes the text displayed when users are prompted for a password.
Step 5	aaa authentication username-prompt <i>text-string</i> Example: 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	aaa authentication login [<i>list-name method1</i>] [<i>method2...</i>] Example: Router (config)# aaa authentication login userlist local group radius	Sets AAA authentication at login. <ul style="list-style-type: none"> A local and RADIUS server may be used together and will be tried in order. Note This command must be enabled to enforce Xauth.
Step 7	aaa authorization network <i>list-name</i> local group radius Example: Router (config)# aaa authorization network grouplist local group radius	Enables group policy lookup. <ul style="list-style-type: none"> A local and RADIUS server may be used together and will be tried in order.
Step 8	username <i>name</i> password <i>encryption-type encrypted-password</i> Example: Router (config)# username server_r password 7 121F0A18	(Optional) Defines local users for Xauth if RADIUS or TACACS+ is not used. Note 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. **acl** *number*
10. **split-dns** *domain-name*
11. **access-restrict** {*interface-name*}
12. **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	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> default } Example: 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. <ul style="list-style-type: none"> If no specific group matches and a default group is defined, users will automatically be given the policy of a default group.
Step 4	key <i>name</i> Example: Router (config-isakmp-group)# key group1	Specifies the IKE preshared key for group policy attribute definition. <p>Note This command <i>must</i> be enabled if the client identifies itself with a preshared key.</p>
Step 5	dns <i>primary-server secondary-server</i> Example: Router (config-isakmp-group)# dns 10.2.2.2 10.3.3.3	(Optional) Specifies the primary and secondary DNS servers for the group.
Step 6	wins <i>primary-server secondary-server</i> Example: Router (config-isakmp-group)# wins 10.10.10.10 10.12.12.12	(Optional) Specifies the primary and secondary WINS servers for the group.

	Command	Purpose
Step 7	domain <i>name</i> Example: Router (config-isakmp-group)# domain domain.com	(Optional) Specifies the DNS domain to which a group belongs.
Step 8	pool <i>name</i> Example: Router (config-isakmp-group)# pool green	Defines a local pool address. <ul style="list-style-type: none"> Although a user must define at least one pool name, a separate pool may be defined for each group policy. Note This command <i>must</i> be defined and refer to a valid IP local pool address or the client connection will fail.
Step 9	acl <i>number</i> Example: Router (config-isakmp-group)# acl 199	(Optional) Configures split tunneling. <ul style="list-style-type: none"> The <i>number</i> argument specifies a group of access control list (ACL) rules that represent protected subnets for split tunneling purposes.
Step 10	split-dns <i>domain-name</i> Example: Router (config-isakmp-group)# split-dns green.com	Specifies a domain name that must be tunneled or resolved to the private network.
Step 11	access-restrict { <i>interface-name</i> } Example: Router (config-isakmp-group)# access-restrict fastethernet0/0	Restricts clients in a group to an interface.
Step 12	firewall are-u-there Example: Router (config-isakmp-group)# firewall are-u-there	(Optional) Adds the firewall are-u-there attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls.
Step 13	group-lock Example: Router (config-isakmp-group)# group-lock	Enforces the group lock feature.
Step 14	include-local-lan Example: 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	save-password Example: Router (config-isakmp-group)# save-password	(Optional) Saves your Xauth password locally on your PC.

	Command	Purpose
Step 16	backup-gateway Example: 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"> • 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.
Step 17	pfs Example: 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"> • 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.

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. **max-logins** *number-of-logins*
5. **max-users** *number-of-users*

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.

	Command	Purpose
Step 3	crypto isakmp client configuration group <i>group-name</i> Example: 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"> <i>group-name</i>—Group definition that identifies which policy is enforced for users.
Step 4	max-logins <i>number-of-logins</i> Example: Router (config-isakmp-group)# max-logins 10	(Optional) Limits the number of simultaneous logins for users in a specific server group.
Step 5	exit Example: Router (config-isakmp-group)# exit	Exits ISAKMP group configuration mode.
Step 6	max-users <i>number-of-users</i> Example: 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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show crypto session group Example: Router# show crypto session group	Displays groups that are currently active on the VPN device.

	Command	Purpose
Step 3	<code>show crypto session summary</code>	Displays groups that are currently active on the VPN device and the users that are connected for each of those groups.
	Example: Router# show crypto session summary	

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	<code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
	Example: Router> enable	
Step 2	<code>configure terminal</code>	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	<code>crypto map tag client configuration address [initiate respond]</code>	Configures the router to initiate or reply to Mode Configuration requests. <p>Note Cisco clients require the respond keyword to be used; however, if the Cisco Secure VPN Client 1.x is used, the initiate keyword must be used; initiate and respond keywords may be used simultaneously.</p>
	Example: Router (config)# crypto map dyn client configuration address initiate	
Step 4	<code>crypto map map-name isakmp authorization list list-name</code>	Enables IKE querying for group policy when requested by the client. <ul style="list-style-type: none"> • 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 aaa authorization network command.
	Example: Router (config)# crypto map ikessaaamap isakmp authorization list ikessaaalist	

	Command	Purpose
Step 5	<pre>crypto map map-name client authentication list list-name</pre> <p>Example: Router (config)# crypto map xauthmap client authentication list xauthlist</p>	<p>Enforces Xauth.</p> <ul style="list-style-type: none"> The <i>list-name</i> argument is used to determine the appropriate username and password storage location (local or RADIUS) as defined in the aaa authentication login command.

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

	Command	Purpose
Step 3	<pre>crypto dynamic map-name seq-num</pre> <p>or</p> <pre>crypto map map-name seq-num ipsec-isakmp</pre> <p>Example: Router (config)# crypto dynamic mymap 10</p> <p>or</p> <pre>Router (config)# crypto map yourmap 15 ipsec-isakmp</pre>	<p>Creates a dynamic crypto map entry and enters crypto map configuration mode.</p> <p>or</p> <p>Adds a dynamic crypto map set to a static crypto map set and enters crypto map configuration mode.</p>
Step 4	<pre>set peer ip-address</pre> <p>Example: Router (config-crypto-map)# set peer 10.20.20.20 </p>	<p>Specifies an IPsec peer IP address in a crypto map entry.</p> <ul style="list-style-type: none"> This step is optional when configuring dynamic crypto map entries.
Step 5	<pre>set transform-set transform-set-name</pre> <p>Example: Router (config-crypto-map)# set transform-set dessha </p>	<p>Specifies which transform sets are allowed for the crypto map entry.</p> <ul style="list-style-type: none"> Lists multiple transform sets in order of priority (highest priority first). <p>Note This list is the only configuration statement required in dynamic crypto map entries.</p>
Step 6	<pre>reverse-route</pre> <p>Example: Router (config-crypto-map)# reverse-route </p>	<p>Creates source proxy information.</p>
Step 7	<pre>match address</pre> <p>Example: Router (config-crypto-map)# match address </p>	<p>Specifies an extended access list for a crypto map entry.</p> <ul style="list-style-type: none"> This step is optional when configuring dynamic crypto map entries.

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	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 secs retries Example: Router (config)# crypto isakmp keepalive 20 10	Allows the gateway to send DPD messages to the router. <ul style="list-style-type: none"> 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).

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

- enable**
- configure terminal**
- radius server host *ip-address* [*auth-port port-number*] [*acct-port port-number*] [*key string*]**

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.

	Command	Purpose
Step 2	<code>configure terminal</code>	Enters global configuration mode.
	Example: Router# <code>configure terminal</code>	
Step 3	<code>radius server host ip-address [auth-port port-number] [acct-port port-number] [key string]</code>	Specifies a RADIUS server host.
	Example: Router (config)# <code>radius server host 192.168.1.1. auth-port 1645 acct-port 1646 key XXXX</code>	Note 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	<code>enable</code>	Enables privileged EXEC mode.
	Example: Router> <code>enable</code>	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>show crypto map [interface interface tag map-name]</code>	Displays the crypto map configuration.
	Example: Router# <code>show crypto map interface ethernet 0</code>	

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	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 Group1	Specifies to which group a policy profile will be defined and enters crypto ISAKMP group configuration mode.
Step 4	banner c { <i>banner-text</i> } c Example: 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	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 {group-name} Example: 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	auto-update client {type-of-system} {url url} {rev review-version} Example: 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	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 browser-proxy { <i>browser-proxy-name</i> } Example: 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	proxy { <i>proxy-parameter</i> } Example: 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	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 Group1	Specifies to which group a policy profile will be defined and enters crypto ISAKMP group configuration mode.
Step 4	configuration url <i>{url}</i> Example: 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"> The URL must be a non-NULL terminated ASCII string that specifies the complete path of the configuration file.
Step 5	configuration version <i>{version-number}</i> Example: Router (config-isakmp-group)# configuration version 10	Specifies the version of the configuration. <ul style="list-style-type: none"> The version number will be an unsigned integer in the range 1 through 32767.

Configuring Per User AAA Download with PKI

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.

Configuring the Crypto PKI Trustpoint

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	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 ca-server	Declares the trustpoint that your router should use and enters ca-trustpoint configuration mode.
Step 4	enrollment url <i>url</i> Example: Router (config-ca-trustpoint)# enrollment url http://10.7.7.2:80	Specifies the URL of the certification authority (CA) server to which to send enrollment requests.
Step 5	revocation-check none Example: Router (config-ca-trustpoint)# revocation-check none	Checks the revocation status of a certificate.
Step 6	rsa-keypair <i>key-label</i> Example: Router (config-ca-trustpoint)# rsa-keypair rsa-pair	Specifies which key pair to associate with the certificate.
Step 7	authorization username { <i>subjectname subjectname</i> }	Specifies the parameters for the different certificate fields that are used to build the AAA username.
Step 8	exit Example: Router (config-ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.

Configuring Per User AAA Download with PKI

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	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 ISAKMP policy configuration mode.
Step 4	group { 1 2} Example: Router (config-isakmp-policy)# group 2	Specifies the Diffie-Hellman group identifier within an IKE policy.

	Command	Purpose
Step 5	exit Example: Router (config-isakmp-policy)# exit	Exits ISAKMP policy configuration mode.
Step 6	crypto isakmp profile <i>profile-name</i> Example: Router (config)# crypto isakmp profile ISA-PROF	Defines an ISAKMP profile and audits IPsec user sessions and enters crypto ISAKMP profile configuration mode.
Step 7	match certificate <i>certificate-map</i> Example: Router (config-isakmp-profile)# match certificate cert_map	Assigns an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate.
Step 8	client pki authorization list <i>listname</i> Example: Router (config-isakmp-profile)# client pki 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	client configuration address { initiate respond } Example: Router (config-isakmp-profile)# client configuration address respond	Configures IKE configuration mode in the ISAKMP profile.
Step 10	virtual-template <i>template-number</i> Example: Router(config-isakmp-profile)# virtual-template 2	Specifies which virtual template will be used to clone virtual access interfaces.
Step 11	exit Example: Router(config-isakmp-profile)# exit	Exits crypto ISAKMP profile configuration mode.
Step 12	crypto ipsec transform-set <i>transform-set-name transform1</i> [<i>transform2</i>] [<i>transform3</i>] [<i>transform4</i>] Example: Router (config)# crypto ipsec transform-set trans2 esp-3des esp-sha-hmac1	Defines a transform set—an acceptable combination of security protocols and algorithms.

	Command	Purpose
Step 13	<code>crypto ipsec profile name</code> Example: Router (config)# crypto ipsec profile IPSEC_PROF	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers.
Step 14	<code>set transform-set transform-set name</code> Example: Router (config)# set transform-set trans2	Specifies which transform sets can be used with the crypto map entry.

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	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>crypto logging ezvpn [group group-name]</code> Example: Router (config)# crypto logging ezvpn group group1	Enables Easy VPN syslog messages on a server. <ul style="list-style-type: none"> • The group 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.

Configuration Examples for Easy VPN Server

This section provides the following configuration examples:

- [Configuring Cisco IOS for Easy VPN Server: Example, page 35](#)
- [RADIUS Group Profile with IPsec AV Pairs: Example, page 36](#)
- [RADIUS User Profile with IPsec AV Pairs: Example, page 37](#)
- [Backup Gateway with Maximum Logins and Maximum Users: Example, page 37](#)
- [Easy VPN with an IPsec Virtual Tunnel Interface: Example, page 37](#)
- [Pushing a Configuration URL Through a Mode-Configuration Exchange: Examples, page 39](#)
- [Per User AAA Policy Download with PKI: Example, page 40](#)
- [Network Admission Control: Example, page 43](#)

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:inacl=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"
ciscoc-avpair = "ipsec:ipsec-backup-gateway=10.1.1.2"
ciscoc-avpair = "ipsec:pfs=1"

```

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 RMZPPMRQMSGiZNJg`EBbCWTKSTi\d[
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 usrgrpki
  server 10.76.248.201 auth-port 1645 acct-port 1646
!
aaa authentication login xauth group usrgrpki
aaa authentication login usrgrp group usrgrpki
aaa authorization network usrgrp group usrgrpki
!
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
9E715AAD 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 usrgrp
  client pki authorization list usrgrp
  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

```

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

```

Additional References

The following sections provide references related to Easy VPN Server.

Related Documents

Related Topic	Document Title
Configuring a router as a VPN client	Easy VPN Remote Enhancements , Cisco IOS Release 12.4(4)T feature module
General information on IPsec and VPN	Refer to the following information in the product literature and in IP technical tips sections on Cisco.com: <ul style="list-style-type: none"> • Cisco IOS Security Configuration Guide • Cisco IOS Security Command Reference, Release 12.4 • An Introduction to IP Security (IPSec) Encryption • Deploying IPSec • Certificate Authority Support for IPSec Overview • Cisco Secure VPN Client • IPSec VPN High Availability Enhancements, Cisco IOS Release 12.2(8)T feature module
IPsec Protocol options and attributes	“ Configuring Internet Key Exchange Security Protocol ” chapter in the Cisco IOS Security Configuration Guide
IPsec virtual tunnels	IPSec Virtual Tunnel Interface , Cisco IOS Release 12.3(14)T feature module
Network Admission Control	Network Admission Control , Cisco IOS Release 12.3(8)T
RRI	IPSec VPN High Availability Enhancements , Cisco IOS Release 12.2(8)T feature module

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 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 new and modified 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/124htix.htm>.

New Commands

- **access-restrict**
- **acl (ISAKMP)**
- **auto-update client**
- **backup-gateway**
- **banner**
- **browser-proxy**
- **client pki authorization list**
- **configuration url**
- **configuration version**
- **crypto ipsec server send-update**

- **crypto isakmp client configuration browser-proxy**
- **crypto isakmp client configuration group**
- **crypto logging ezvpn**
- **dns**
- **domain (isakmp-group)**
- **firewall are-u-there**
- **group-lock**
- **include-local-lan**
- **key (isakmp-group)**
- **max-logins**
- **max-users**
- **pfs**
- **pool (isakmp-group)**
- **proxy**
- **save-password**
- **show crypto session group**
- **show crypto session summary**
- **split-dns**
- **wins**

Modified Commands

- **show crypto isakmp peer**

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.

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.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

Copyright © 2003–2005 Cisco Systems, Inc. All rights reserved.