GET VPN

Technology Design Guide

August 2014 Series

CISCO VALIDATED DESIGN

Table of Contents

Preface 1

CVD Navigator 2

- Use Cases 2
- Scope 2
- Proficiency 2

Introduction 3

- Technology Use Case 3
  - Use Case: Site-to-Site WAN Encryption using MPLS Services 3
- Design Overview 4
  - GET VPN Components 5

Deployment Details 7

- Implementing Key Servers 8
- Implementing Group Member 23

Appendix A: Product List 26

Appendix B: Device Configuration Files 28

- GET VPN Primary Key Server 28
- GET VPN Secondary Key Server 32
- GET VPN Group Member 36

Appendix C: Changes 43

Preface

Cisco Validated Designs (CVDs) present systems that are based on common use cases or engineering priorities. CVDs incorporate a broad set of technologies, features, and applications that address customer needs. Cisco engineers have comprehensively tested and documented each design in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested design details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate existing CVDs but also include product features and functionality across Cisco products and sometimes include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems.

CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit the CVD Foundation web site.

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **Site-to-Site WAN Encryption using MPLS Services**—Many organizations require encryption in order to secure communications between sites over private-cloud services such as provider-managed Multiprotocol Label Switching (MPLS).
- For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Design and configuration of Group Encrypted Transport Virtual Private Network (GET VPN)

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Routing and Switching**—1 to 3 years installing, configuring, and maintaining routed and switched networks
- **CCNP Security**—3 to 5 years testing, deploying, configuring, maintaining security appliances and other devices that establish the security posture of the network

Related CVD Guides

MPLS WAN Technology Design Guide

Layer 2 WAN Technology Design Guide

To view the related CVD guides, click the titles or visit the CVD Foundation web site.

Introduction

This guide describes how to deploy Cisco Group Encrypted Transport VPN (GET VPN) technology to secure WAN and metropolitan-area network (MAN) connectivity between a primary site and up to 500 remote sites.

Technology Use Case

Organizations pay a great deal of attention to protecting their electronic assets from outside threats. This includes an important development: IT services are increasingly migrating toward cloud-based services.

With organizations moving toward cloud-based IT services and cloud computing, they have an increasing need to secure data in transit and ensure data confidentiality, integrity, and availability. This is further driven by government regulatory requirements and industry security standards such as the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), the Sarbanes-Oxley Act, and the Payment Card Industry Data Security Standard (PCI DSS) that spell out the need and set standards for encrypting data transported over networks.

Furthermore, voice and video are becoming a prominent piece of the overall network traffic. Organizations are looking to leverage technologies (for example, rich media collaboration tools and interactive video solutions) to lower operating cost and reduce their carbon footprint by cutting down on travel. As a result, the distributed nature of voice and interactive video applications has accelerated the need for instantaneous, remote site–to–remote site communications. At the same time, current WAN technologies force organizations to make tradeoffs between enabling quality of service (QoS) to support these real-time applications and network transport security.

To address these challenges, Cisco introduced the next generation of WAN encryption technology, Cisco GET VPN, which addresses the security requirement while maintaining the instantaneous remote site-to-remote site communication needed for real-time applications. Cisco GET VPN eliminates the need for compromise between network intelligence and data privacy in private WAN environments. The technology introduces a new category of VPN that eliminates the need for tunnels, while providing strong encryption that meets the 140 series of the Federal Information Processing Standards (FIPS).

Use Case: Site-to-Site WAN Encryption using MPLS Services

This guide helps organizations that require encryption in order to secure communications between sites over private cloud services such as provider-managed Multiprotocol Label Switching (MPLS).

This design guide enables the following network capabilities:

- Any-to-any secure encrypted communications well suited for MPLS-based WAN services, for up to 500 locations.
- Encrypted traffic that follows the native routing path directly between remote sites, rather than following a tunnel overlay model.
- Encryption services—with single or dual MPLS service providers—that support resilient designs using single or dual routers in remote-site locations.
- Support for IP Multicast, allowing multicast replication after encryption within the service provider network.
- Compatibility with WAN transport solutions that *do not* perform Network Address Translations (NAT) after encryption.
- QoS for WAN traffic such as Voice over IP (VoIP) and business critical applications.

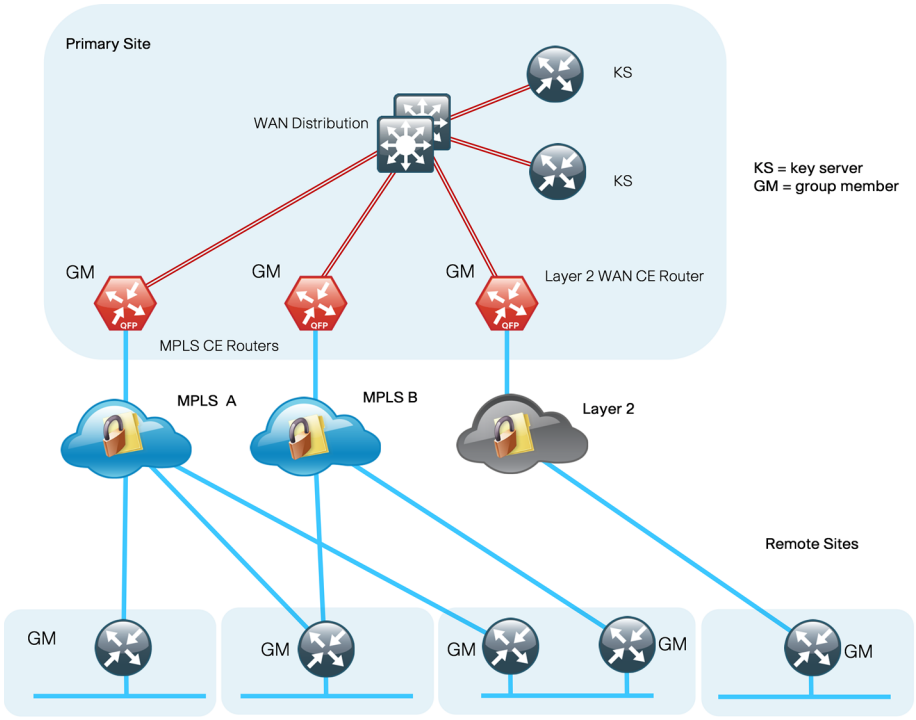
Design Overview

GET VPN is a tunnel-less VPN technology based on the IETF standard (RFC 3547). The technology provides end-to-end data encryption for network infrastructure while maintaining any-to-any communication between sites. You can deploy it across various WAN core transports, such as IP or Multiprotocol Label Switching (MPLS) networks. GET VPN leverages the Group Domain of Interpretation (GDOI) protocol to create a secure communication domain among network devices.

The benefits of GET VPN include the following:

- Highly scalable VPN technology that provides an any-to-any meshed topology without the need for complex peer-to-peer security associations
- Low latency and jitter communication with direct traffic between sites
- Centralized encryption policy and membership management with the key servers (KSs)
- Simplified network design due to leveraging of native routing infrastructure (no overlay routing protocol needed)
- Efficient bandwidth utilization by supporting multicast-enabled network core
- Network intelligence such as native routing path, network topology, and QoS

Figure 1 - Secure WAN using GET VPN

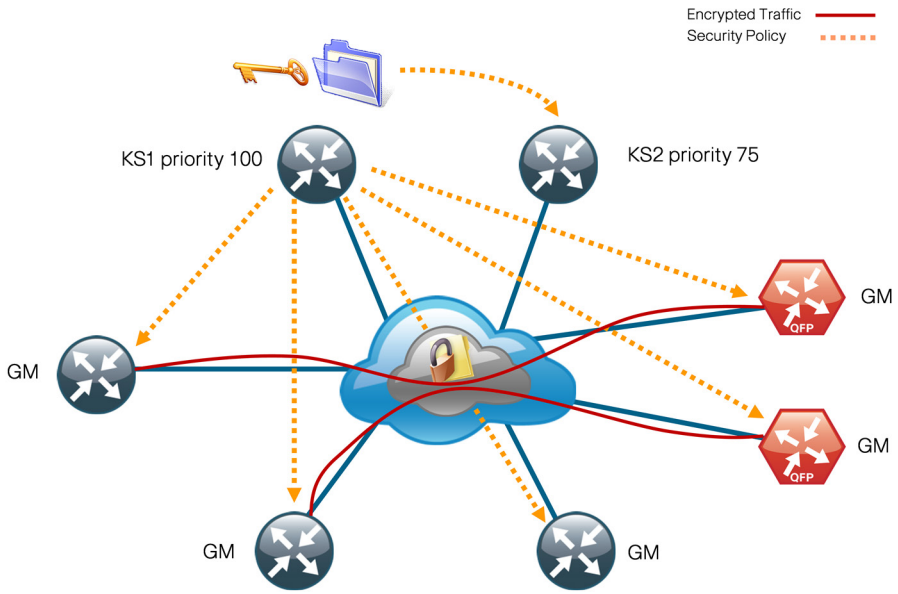


GET VPN Components

A *group member* (GM) is a router running Cisco IOS that encrypts and decrypts the data traffic. A GM registers with a key server to obtain the encryption keys necessary for encrypting and decrypting traffic streams traversing through the device. The GM also performs routing between secure and unsecure domains. Lastly, the GM participates in multicast communications that have been established in the network.

A *key server (KS)* is the brain of the GET VPN operation. It is responsible for authenticating GMs. The KS manages security policies that determine which traffic should be encrypted. The KS distributes session keys for traffic encryption and the security policies through GDOI protocol to GMs. There are two types of keys that the KS sends out to GMs: the key encryption key (KEK) and the traffic encryption key (TEK). The KS uses the KEK to secure communication between the KS and GMs. GMs use the TEK for bulk data encryption of traffic traversing between GMs.

Figure 2 - GET VPN components

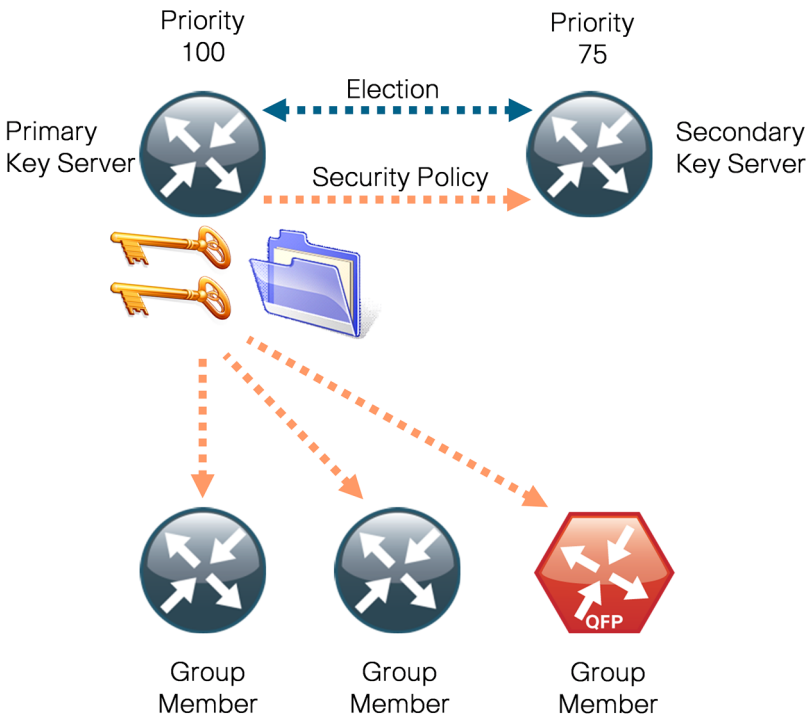


The KS sends out rekey messages as needed. The rekey message contains new encryption policy and encryption keys to use when the old IPSec Security Association (SA) expires. The rekey message is sent in advance of the SA expiration, which helps ensure that the new keys are available to all GMs.

The KS is an essential component in the GET VPN deployment. If the KS becomes unavailable, new GMs will not be able to register and participate in the secure communication, and the existing GMs will not receive new rekeys and updated security policies when the existing ones expire.

To help ensure a highly available and resilient GET VPN network, redundant KSs operate in cooperative mode. Cooperative key servers (COOP KSs) share the GM registration load by jointly managing the GDOI registration of the group. When COOP KSs start up, they go through an election process and the KS with the highest priority assumes the primary role, while the other KSs remain in secondary roles. The primary KS is responsible for creating and redistributing the security policies and keys to GMs, as well as synchronizing the secondary KSs.

Figure 3 - COOP KS synchronization flow



Deployment Details

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

This section covers the following:

- Deployment details for key servers
- Deployment details for group members

Caution

If you are using a Cisco ASR 1000 Series router as a GET VPN GM, the required software release is version 15.2(2)S2. Additional details are included in Appendix A: Product List.

PROCESS

Implementing Key Servers

1. Configure the distribution switch
2. Configure the KS
3. Configure connectivity to the LAN
4. Generate and export an RSA key
5. Configure KS policies
6. Configure secondary KS
7. Configure redundancy on primary KS

This section describes configuring the GET VPN KSs. Only the core relevant features are described.

Table 1 - Parameters used in the deployment examples

Host name	Port-channel number	IP address	Netmask	Default gateway	KS role	KS priority
KS-2951-1	21	10.4.32.151	255.255.255.192	10.4.32.129	Primary	100
KS-2951-2	22	10.4.32.152	255.255.255.192	10.4.32.129	Secondary	75

Procedure 1 Configure the distribution switch

Step 1: If a VLAN does not already exist on the distribution layer switch, configure it now.

```
vlan 350
 name WAN_Service_Net
```

Step 2: If the Layer 3 SVI has not yet been configured, configure it now.

Be sure to configure a VLAN interface (SVI) for every new VLAN you add, so devices in the VLAN can communicate with the rest of the network.

```
interface Vlan350
 ip address 10.4.32.129 255.255.255.192
 no shutdown
```

Next, configure EtherChannel member interfaces.

Tech Tip

EtherChannel is a logical interface that bundles multiple physical LAN links into a single logical link.

Step 3: Connect the KS EtherChannel uplinks in order to separate switches in the distribution layer switches or stack (for the Cisco Catalyst 4507R+E distribution layer, this separates redundant modules for additional resiliency), and then configure two physical interfaces to be members of the EtherChannel. Also, apply the egress QoS macro that was defined in the platform configuration procedure. This ensures traffic is prioritized appropriately.

Tech Tip

Configure the physical interfaces that are members of a Layer 2 EtherChannel prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration and reduces errors because most of the commands entered to a port-channel interface are copied to its members interfaces and do not require manual replication.

```
interface GigabitEthernet 1/0/9
 description Link to KS-2951-1 Gig0/0
interface GigabitEthernet 2/0/9
 description Link to KS-2951-1 Gig0/1
!
interface range GigabitEthernet 1/0/9, GigabitEthernet 2/0/9
 switchport
 channel-group 21 mode on
 logging event link-status
 logging event bundle-status
 load-interval 30
 macro apply EgressQoS
```

Next, configure the EtherChannel. Access mode interfaces are used for the connection to the KSs.

Step 4: Assign the VLAN created at the beginning of the procedure to the interface. When using EtherChannel, the port-channel number must match the channel group configured in Step 3.

```
interface Port-channel 21
 description EtherChannel link to KS-2951-1
 switchport access vlan 350
 logging event link-status
 load-interval 30
 no shutdown
```

Procedure 2 Configure the KS

Within this design, there are features and services that are common across all KS routers. In this procedure, you configure system settings that simplify and secure the management of the solution.

Step 1: Configure the device host name to make it easy to identify the device.

```
Hostname KS-2951-1
```

Step 2: Configure the local login and password.

The local login account and password provide basic access authentication to a router, which provides only limited operational privileges. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the disclosure of plaintext passwords when viewing configuration files.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

By default, HTTPS access to the router will use the enable password for authentication.

Step 3: If you want to configure centralized user authentication, perform this step.

As networks scale in the number of devices to maintain, the operational burden to maintain local user accounts on every device also scales. A centralized authentication, authorization, and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root-cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (Secure Shell [SSH] Protocol and Secure HTTP [HTTPS]) is controlled by AAA.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined in Step 2 on each network infrastructure device in order to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

Step 4: Configure device management protocols.

HTTPS and SSH are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

The use of the SSH and HTTPS protocols enables secure management of the network device. Both protocols are encrypted for privacy, and the unsecure protocols—Telnet and HTTP—are turned off.

Specify the **transport preferred none** command on vty lines in order to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
ip scp server enable
line vty 0 15
 transport input ssh
 transport preferred none
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0
 logging synchronous
```

Enable Simple Network Management Protocol (SNMP) to allow the network infrastructure devices to be managed by a network management system (NMS). SNMPv2c is configured both for a read-only and a read/write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Step 5: If operational support is centralized in your network, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
 access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```

Tech Tip

If you configure an access list on the vty interface, you may lose the ability to use SSH to log in from one router to the next for hop-by-hop troubleshooting.

Step 6: Configure a synchronized clock.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

You should program network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. By configuring console messages, logs, and debug output to provide time stamps on output, you can cross-reference events in a network.

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Procedure 3 Configure connectivity to the LAN

Any links to adjacent distribution layers should be Layer 3 links or Layer 3 EtherChannels.

Step 1: Configure a Layer 3 interface.

```
interface Port-channel21
  ip address 10.4.32.151 255.255.255.192
  no shutdown
```

Step 2: Configure EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port-channel by using the **channel-group** command. The number for the port-channel and channel-group must match. Not all router platforms can support Link Aggregation Control Protocol (LACP) to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet0/0
 description WAN-D3750X Gig1/0/9
!
interface GigabitEthernet0/1
 description WAN-D3750X Gig2/0/9
!
interface range GigabitEthernet0/0, GigabitEthernet0/1
  no ip address
  channel-group 21
  no shutdown
```

Step 3: Configure a default route. This provides reachability information for the KS to reach GMs by using a default route.

```
ip route 0.0.0.0 0.0.0.0 10.4.32.129
```

Procedure 4 Generate and export an RSA key

This procedure is for the primary KS only. Perform this procedure before starting KS configuration.

Step 1: Generate an RSA key for use during rekeys.

```
crypto key generate rsa label GETVPN-REKEY-RSA modulus 2048 exportable
```

Tech Tip

Generate the RSA key pair on the primary KS. Make sure that the “exportable” option is used in generating the RSA keys. This allows you to export the key pair and install it into other KSs that will be running in COOP KS mode in the network.

Example

```
KS-2951-1(config)# crypto key generate rsa label GETVPN-REKEY-RSA modulus 2048
exportable
The name for the keys will be: GETVPN-REKEY-RSA
% The key modulus size is 2048 bits
      % Generating 2048 bit RSA keys, keys will be exportable...
      [OK] (elapsed time was 2 seconds)
```

Step 2: Export RSA keys from the primary KS.

```
crypto key export rsa GETVPN-REKEY-RSA pem terminal 3des c1sco123
```

Step 3: Copy and paste the output from Step 2 into a text file. Make sure that you capture both the public key and private key.

> **Tech Tip**
>
> It is recommended that you store the key file in a secure environment. You will use the key pair later to build secondary KSs or, in the case of hardware failure, to rebuild the primary KS.

Example

```
KS-2951-1(config)#crypto key export rsa GETVPN-REKEY-RSA pem terminal 3des c1sco123
% Key name: GETVPN-REKEY-RSA
   Usage: General Purpose Key
   Key data:
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtX3Cr8QUpSmgTpmLkyYG
CySAYlPTnoy06umGRMmxXu/XB4ls64BpfHnrmuCqhtNajrlOxKO9TYh6r7kUSSKO
EpFqmtk3bEJq/MF+hUvCXxz6Qe8S+YC0dHUem1039/mZJdK9RBwjC7KlFbP4io6D
h9WmlL9R8mvTmslCEfdu4ameRaR+8dt6Tbm9SGwamKA8U2I8q5BPXDXfJMHCe/4y
Kijo+5gSy1hy+1SEXW9MiNtV4Htckb5KlH+vhtkxDIzhXT2m8/wUQz3t+9LXfRgU
OWFSo9XjTqbMDcMpAGSNnhFsqHW6+DYqup1wJGypfRKlTFr5cQ8nCQx0q6pwzA+5
fwIDAQAB
-----END PUBLIC KEY-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,B0EA38C0B90569C9
2BADU1kcBZQo3aY/C+lgT3jVQxbawIoidGi5OZtqpczzHX5KwkgjN/o36t1Wa7ka
TtPh3XZ6UZJ1YCiAW/fzyuKD3ITx6eS/npaHQu2pKl0ToDUEman0ptdKklRv5ODV7
AQEMYwI27Uy16cbbOdTkX4y1y5VmzCz3oLWqcygEiYWe2pHaB1dP7TEHnKmnrp3H
ztRJIwLWJc682EIOK2IuhhNb05XAt3xXO241wNSvgE5zAtE9p2Z8lGSevcWjfmoi
Pp58T7EWL9hWoCmpUA6+S60b/OVTV+MG7tGENGiL0alquMKQnGRf/eK28KaLwg7x
<key data deleted>
-----END RSA PRIVATE KEY-----
```

Procedure 5 Configure KS policies

The Internet Security Association and Key Management Protocol (ISAKMP) policy for GET VPN uses the following:

- Advanced Encryption Standard (AES) with 256-bit key
- Secure Hash Standard (SHA)
- Diffie-Hellman Group: 5 (used for KS)
- Diffie-Hellman Group: 2 (used for GM)
- Internet Key Exchange (IKE) lifetime: 86,400 (default, used for KS)
- IKE lifetime: 1200 (used for GM)

Step 1: Define ISAKMP policy for COOP KS.

```
crypto isakmp policy 10
 encr aes 256
 group 5
```

Step 2: Define ISAKMP policy for GMs.

```
crypto isakmp policy 15
 encr aes 256
 group 2
 lifetime 1200
```

Although most ISAKMP policy parameters must be identically configured between KS and GM, IKE lifetime is negotiated between KS and GM to the lowest value configured. On the KS, change the IKE lifetime to 1200 seconds from the default 86400 seconds to centrally set the IKE lifetime for GM.

Step 3: Configure the IKE authentication method by using pre-shared key (PSK).

```
crypto isakmp policy 10
 authentication pre-share
!
crypto isakmp policy 15
 authentication pre-share
```

The default authentication method uses public key infrastructure (PKI) (authentication rsa-sig). For ease of deployment, this example uses PSK as the authentication method.

Step 4: Configure the PSK. For IKE authentication to be successful, the remote peer's PSK must match the local peer's PSK. You can uniquely configure the PSK on a per-peer basis, or you can use a wildcard PSK to allow a group of remote devices with the same level of authentication to share an IKE PSK.

```
crypto isakmp key c1sco123 address 0.0.0.0 0.0.0.0
```

Step 5: Configure the IPsec encryption profile.

```
crypto ipsec transform-set AES256/SHA esp-aes 256 esp-sha-hmac
!
crypto ipsec profile GETVPN-PROFILE
 set security-association lifetime seconds 7200
 set transform-set AES256/SHA
```

This example defines the algorithm used for data encryption, as well as the traffic encryption key (TEK) lifetime. Using the AES-256 encryption algorithm provides more robust security. The TEK lifetime is set for 2 hours (7200 seconds).

> **Tech Tip**
>
> The TEK lifetime should not be less than the default 3600 seconds. A short TEK lifetime creates more encryption policy rollovers that must be synchronized from the KS to all GMs. Setting the TEK lifetime too low may cause the GET VPN network to operate in an unstable state.

Step 6: Configure GET VPN GDOI group parameters. Each GDOI group configured on the KS requires a unique group ID.

```
crypto gdoi group GETVPN-GROUP
 identity number 65511
```

Step 7: Designate the device as a GDOI KS and define the parameters that will be used during the rekey process.

```
server local
 rekey algorithm aes 256
 rekey retransmit 40 number 3
 rekey authentication mypubkey rsa GETVPN-REKEY-RSA
 rekey transport unicast
 address ipv4 [KS address]
```

The default rekey transport is multicast, but in this example you use the unicast rekey transport mechanism, with two more retransmits at 40-second intervals. You configure the AES-256 cipher to encrypt rekey messages, and you configure authentication to use the RSA key pair generated earlier.

Configure the IPsec profile and security policies, which define the traffic to be encrypted, and then configure the time-based anti-replay (TBAR) window size.

```
sa ipsec 10
 profile GETVPN-PROFILE
 match address ipv4 GETVPN-POLICY-ACL
 replay time window-size 20
```

Step 8: Configure the security policy access control list (ACL).

Define the security policy on the KS by using an extended IP ACL. You should only use the 5-tuple in the ACL (that is, source_ip_address, destination_ip_address, protocol, source_port, destination_port) to determine what to encrypt. The **permit** entries in the ACL define the traffic that should be encrypted, and the **deny** entries define the traffic that should be excluded from the GET VPN encryption. The **deny** entries in the ACL should be configured to exclude routing protocols and the traffic that is encrypted already, such as SSH, TACACS+, GDOI, ISAKMP, etc. The ACL is applied to the GET VPN configuration.

```
ip access-list extended GETVPN-POLICY-ACL
 remark >> exclude transient encrypted traffic (ESP, ISAKMP, GDOI)
 deny   esp any any
 deny   udp any eq isakmp any eq isakmp
 deny   udp any eq 848 any eq 848
```

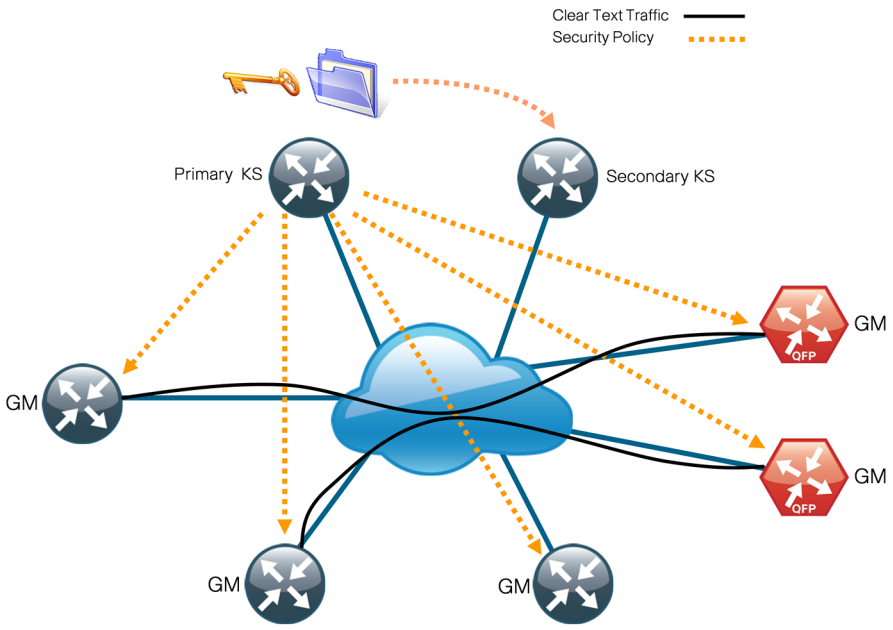
```
remark >> exclude encrypted in-band management traffic (SSH, TACACS+)
deny   tcp any any eq 22
deny   tcp any eq 22 any
deny   tcp any any eq 49
deny   tcp any eq 49 any
remark >> exclude routing protocol with MPLS provider
deny   tcp any any eq bgp
deny   tcp any eq bgp any
remark >> exclude routing protocol used for Layer 2 WAN
deny   eigrp any any
remark >> exclude other protocols as necessary (multiple lines)
deny   [protocol] [source] [destination]
remark >> Require all other traffic to be encrypted
permit ip any any
```

By migrating from an unencrypted network to GET VPN, you can use receive-only SAs while WAN edge routers are in the process of converting to GET VPN GMs. The receive-only SA allows a GM to register to a KS and start receiving security policies and keys used for encryption; however, the GM continues to forward traffic in clear. The receive-only SA option establishes the control plane for the GET VPN network without engaging the data plan. This serves to provide interoperability between the sites that have been migrated to the GET VPN network and the sites waiting to be migrated.

Step 9: If you want to use receive-only SAs while WAN edge routers are in the process of converting to GET VPN GMs, enable receive-only SA capability on the KS.

```
crypto gdoi group GETVPN-GROUP
 server local
  sa receive-only
```

Figure 4 - Receive-only mode



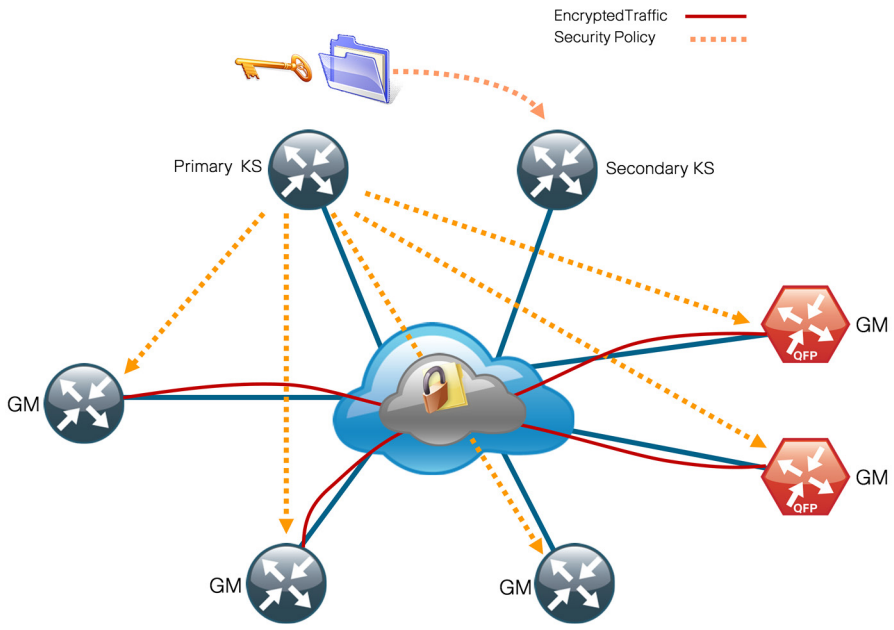
After your network is fully migrated to GET VPN and you have verified that the control plane is completely operational, you can enable the encryption for all GMs in a group by disabling the receive-only SA mode on the KS.

Step 10: Disable the receive-only SA mode on the KS.

```
crypto gdoi group GETVPN-GROUP
 server local
  no sa receive-only
```

> **Tech Tip**
>
> To force an immediate rekey to be sent from the key servers to the group members, enter the command **crypto gdoi ks rekey** on the primary key server.

Figure 5 - Steady-state operation



Example: Primary KS

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp policy 15
 encr aes 256
 authentication pre-share
 group 2
 lifetime 1200
crypto isakmp key c1sco123 address 0.0.0.0 0.0.0.0
!
```

```
!
crypto ipsec transform-set AES256/SHA esp-aes 256 esp-sha-hmac
!
crypto ipsec profile GETVPN-PROFILE
 set security-association lifetime seconds 7200
 set transform-set AES256/SHA
!
crypto gdoi group GETVPN-GROUP identity number 65511
 server local
  rekey algorithm aes 256
  rekey retransmit 40 number 3
  rekey authentication mypubkey rsa GETVPN-REKEY-RSA
  rekey transport unicast
  sa ipsec 10
   profile GETVPN-PROFILE
   match address ipv4 GETVPN-POLICY-ACL
   replay time window-size 5
  address ipv4 10.4.32.151
!
ip access-list extended GETVPN-POLICY-ACL
 remark >> exclude transient encrypted traffic (ESP, ISAKMP, GDOI)
 deny   esp any any
 deny   udp any eq isakmp any eq isakmp
 deny   udp any eq 848 any eq 848
 remark >> exclude encrypted in-band management traffic (SSH, TACACS+)
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any any eq 49
 deny   tcp any eq 49 any
 remark >> exclude routing protocol with MPLS provider
 deny   tcp any any eq bgp
 deny   tcp any eq bgp any
 remark >> exclude routing protocol used for Layer 2 WAN
 deny   eigrp any any
 remark >> exclude PIM protocol
 deny   pim any host 224.0.0.13
 remark >> exclude IGMP with MPLS provider
 deny   igmp any host 224.0.0.1
 deny   igmp host 224.0.0.1 any
 deny   igmp any host 224.0.1.40
 deny   igmp host 224.0.1.40 any
 remark >> exclude icmp traffic destined to SP address
 deny   icmp any 192.168.3.0 0.0.0.255
 deny   icmp 192.168.3.0 0.0.0.255 any
 deny   icmp any 192.168.4.0 0.0.0.255
 deny   icmp 192.168.4.0 0.0.0.255 any
 remark >> exclude icmp traffic destined to KS from Loopback address
```

```
deny   icmp host 10.4.32.151 10.255.0.0 0.0.255.255
deny   icmp 10.255.0.0 0.0.255.255 host 10.4.32.151
deny   icmp host 10.4.32.152 10.255.0.0 0.0.255.255
deny   icmp 10.255.0.0 0.0.255.255 host 10.4.32.152
remark >> Require all other traffic to be encrypted
permit ip any any
```

Procedure 6 Configure secondary KS

This procedure is for the secondary KS only.

The secondary KSs are configured similarly to the primary KS. Begin by repeating Procedure 1, "Configure the distribution switch." Follow this with Procedure 2, "Configure the KS," and Procedure 3, "Configure connectivity to the LAN." Then complete the following steps. You must configure identical policies between the primary and secondary KSs. This helps ensure that the same rules are redistributed to the GM if the secondary KS assumes the primary role.

Step 1: Import the RSA keys that you created in Procedure 4, "Generate and export an RSA key," from the primary KS. This step requires PEM-formatted keys. Cut and paste from the terminal to a new KS router. You need to paste the public and private keys separately.

```
crypto key import rsa GETVPN-REKEY-RSA exportable terminal c1sco123
```

Example

```
KS-2951-2(config)# crypto key import rsa GETVPN-REKEY-RSA exportable terminal c1sco123
% Enter PEM-formatted public General Purpose key or certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtX3Cr8QUpSmgTpmLkyYG
CySAYlPTnoy06umGRMmxXu/XB4ls64BpfHnrmuCqhtNajrlOxKO9TYh6r7kUSSKO
EpFqmtk3bEJq/MF+hUvCXxz6Qe8S+YC0dHUem1039/mZJdK9RBwjC7KlFbP4io6D
h9WmlL9R8mvTmslCEfdu4ameRaR+8dt6Tbm9SGwamKA8U2I8q5BPXDXfJMHCe/4y
Kijo+5gSy1hy+1SEXW9MiNtV4Htckb5KlH+vhtkxDIzhXT2m8/wUQz3t+9LXfRgU
OWFSo9XjTqbMDcMpAGSNnhFsqHW6+DYqup1wJGypfRKlTFr5cQ8nCQx0q6pwzA+5
fwIDAQAB
-----END PUBLIC KEY-----
quit
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,B0EA38C0B90569C9
2BADU1kcBZQo3aY/C+lgT3jVQxbawIoidGi5OZtqpczzHX5KwkgjN/o36t1Wa7ka
TtPh3XZ6UZJ1YCiAW/fzyuKD3ITx6eS/npaHQu2pKl0ToDUEman0ptdKklRv5ODV
AQEMYwI27Uy16cbbOdTkX4y1y5VmzCz3oLWqcygEiYWe2pHaB1dP7TEHnKmnrp3H
ztRJIwLWJc682EIOK2IuhhNb05XAt3xXO241wNSvgE5zAtE9p2Z8lGSevcWjfmoi
Pp58T7EWL9hWoCmpUA6+S60b/OVTV+MG7tGENGiL0alquMKQnGRf/eK28KaLwg7x
<key data deleted>
-----END RSA PRIVATE KEY-----
quit
% Key pair import succeeded.
```

Tech Tip

The RSA key pair must be identical on all KSs running in COOP KS mode. If a KS is added to a group without the RSA key, it will not be able to generate policies. This will result in the GM registered to this KS to stay in a fail-closed state and be unable to pass traffic with the rest of the GM in the group.

Step 2: Repeat Procedure 5, "Configure KS policies" for the secondary KS.

Caution

Be sure to use the IP address of the secondary KS in Step 7 of Procedure 5, "Configure KS policies."

Step 3: Configure periodic dead-peer protection on all secondary KSs running in COOP KS mode so that the primary KS can track state for the secondary KS.

```
crypto isakmp keepalive 15 periodic
```

Step 4: Configure KS redundancy by enabling the cooperative KS function on the secondary KS and setting the KS priority to 75, which is less than that of the primary KS (which is set to 100).

Tech Tip

It is recommended that redundancy be configured on the secondary KS first, before redundancy is enabled on the primary KS in Procedure 7, "Configure redundancy on primary KS." This minimizes disruptions to the existing KS when adding a new KS into the COOP KS mode.

```
crypto gdoi group GETVPN-GROUP
 server local
  redundancy
   local priority 75
   peer address ipv4 10.4.32.151
```

Example: Secondary KS

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp policy 15
 encr aes 256
 authentication pre-share
 group 2
 lifetime 1200
crypto isakmp key c1sco123 address 0.0.0.0 0.0.0.0
```

```
crypto isakmp keepalive 15 periodic
!
!
crypto ipsec transform-set AES256/SHA esp-aes 256 esp-sha-hmac
!
crypto ipsec profile GETVPN-PROFILE
 set security-association lifetime seconds 7200
 set transform-set AES256/SHA
!
crypto gdoi group GETVPN-GROUP
 identity number 65511
 server local
  rekey algorithm aes 256
  rekey retransmit 40 number 3
  rekey authentication mypubkey rsa GETVPN-REKEY-RSA
  rekey transport unicast
  sa ipsec 10
   profile GETVPN-PROFILE
   match address ipv4 GETVPN-POLICY
   replay time window-size 5
  address ipv4 10.4.32.152
  redundancy
   local priority 75
   peer address ipv4 10.4.32.151
!
ip access-list extended GETVPN-POLICY-ACL
 remark >> exclude transient encrypted traffic (ESP, ISAKMP, GDOI)
 deny   esp any any
 deny   udp any eq isakmp any eq isakmp
 deny   udp any eq 848 any eq 848
 remark >> exclude encrypted in-band management traffic (SSH, TACACS+)
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any any eq 49
 deny   tcp any eq 49 any
 remark >> exclude routing protocol with MPLS provider
 deny   tcp any any eq bgp
 deny   tcp any eq bgp any
 remark >> exclude routing protocol used for Layer 2 WAN
 deny   eigrp any any
 remark >> exclude PIM protocol
 deny   pim any host 224.0.0.13
 remark >> exclude IGMP with MPLS provider
 deny   igmp any host 224.0.0.1
 deny   igmp host 224.0.0.1 any
 deny   igmp any host 224.0.1.40
 deny   igmp host 224.0.1.40 any
```

```
remark >> exclude icmp traffic destined to SP address
deny   icmp any 192.168.3.0 0.0.0.255
deny   icmp 192.168.3.0 0.0.0.255 any
deny   icmp any 192.168.4.0 0.0.0.255
deny   icmp 192.168.4.0 0.0.0.255 any
remark >> Permit all other traffic to be encrypted
permit ip any any
```

Procedure 7 Configure redundancy on primary KS

It is recommended that you have at least two KSs running in COOP KS mode in order to achieve redundancy and high availability in a GET VPN network. COOP KSs ensure that the group security policies, encryption keys, and registered GM information are shared and synchronized between KSs. From among the available KSs running in COOP mode, a primary KS is determined based first on highest priority, and then on the highest IP address used for rekey.

The primary KS is responsible for creating and redistributing group policies, and it also sends out updates on group information to other KSs to keep the secondary KSs in sync. If the primary KS is unavailable, a secondary KS can declare itself primary KS for the group and transition to the primary KS role if it does not detect other KS with higher priority.

Step 1: Configure KS redundancy on the primary KS and set the KS priority to 100.

```
crypto gdoi group GETVPN-GROUP
 server local
  redundancy
   local priority 100
   peer address ipv4 10.4.32.152
```

Step 2: Configure periodic dead peer protection on the primary KS running in COOP KS mode so that the secondary KS can track the state for the primary KS.

```
crypto isakmp keepalive 15 periodic
```

Example: Primary KS with redundancy

```
crypto isakmp keepalive 15 periodic
crypto gdoi group GETVPN-GROUP
 identity number 65511
 server local
  redundancy
   local priority 100
   peer address ipv4 10.4.32.152
```

PROCESS

Implementing Group Member

1. Configure a GM

This process adds GM functionality to an already configured WAN router. It includes only the additional steps required to enable the GM capabilities.

Procedure 1 Configure a GM

The GM registers with the KS in order to obtain the IPSec SA and the encryption keys that are necessary to encrypt traffic. During registration, the GM presents a group ID to the KS to get the respective policies and keys for the group. Because most of the intelligence resides on the KS, the configuration on a GM is relatively simple and is identical across all GMs.

This procedure assumes that all of the basic connectivity configurations (such as default route, routing protocols, etc.) are already set up. This procedure needs to be repeated for every GM that runs GET VPN.

Step 1: Configure ISAKMP policy.

The ISAKMP policy for GET VPN uses the following:

- AES with 256-bit key
- SHA
- Diffie-Hellman Group 2
- PSK authentication

```
crypto isakmp policy 15
 encr aes 256
 authentication pre-share
 group 2
```

Step 2: Define and add the pre-shared keys for GET VPN key servers to the GLOBAL-KEYRING.

```
crypto keyring GLOBAL-KEYRING
  pre-shared-key address 10.4.32.151 key c1sco123
  pre-shared-key address 10.4.32.152 key c1sco123
```

Tech Tip

If you require concurrent GET VPN and DMVPN in a non-VRF aware configuration, all crypto keys must be included in a global keyring. This applies to single-router MPLS and L2WAN primary with DMVPN backup configurations that do not include front-door VRF. This is the case with local Internet access and DMVPN shared hub configurations. In this scenario, you must also ensure that the more specific pre-shared-key entries for the key server are at the top of the list and the default pre-shared-key is the last entry in the keyring, as shown.

```
crypto keyring GLOBAL-KEYRING
  pre-shared-key address 10.4.32.151 key c1sco123
  pre-shared-key address 10.4.32.152 key c1sco123
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

Step 3: Configure the PSK for the KSs.

```
crypto isakmp key c1sco123 address 10.4.32.151
crypto isakmp key c1sco123 address 10.4.32.152
```

For IKE authentication to be successful, the remote peer's PSK must match the local peer's PSK. You only need to specify the PSKs with the KSs.

Step 4: Configure the GDOI group information.

```
crypto gdoi group GETVPN-GROUP
 identity number 65511
 server address ipv4 10.4.32.151
 server address ipv4 10.4.32.152
```

You do not need to configure IPsec transform-set and profile on a GM. When the GM successfully registers with the KS, it downloads these parameters. A GM needs to define only the GDOI group identity and the address of the KSs.

Step 5: Define the crypto map with the GDOI option and associate it to the GDOI group created in the previous step. Although the sequence number is arbitrary, it is a best practice to use the same value on all GMs.

```
crypto map GETVPN-MAP local-address Loopback0
crypto map GETVPN-MAP [Sequence number] gdoi
 set group GETVPN-GROUP
```

Step 6: Activate GET VPN configuration on the GM.

Tech Tip

A router that is connected to multiple WAN transports, such as dual MPLS, must have the crypto map applied to each of its WAN-facing interfaces. When you use trunked demarcation in Layer 2 WAN deployments, you must apply the crypto map to all WAN-facing subinterfaces.

```
interface [type] [number]
 crypto map GETVPN-MAP
```

Step 7: Apply the **ip tcp adjust-mss 1360** command on the WAN interface to account for the IPsec overhead. This command results in lowering the maximum segment size (MSS) for TCP traffic traverse through the interface to avoid the overhead caused by the IPsec header. This command affects only TCP traffic and is not applicable to UDP traffic.

```
interface [type] [number]
 ip tcp adjust-mss 1360
```

Example: MPLS and Layer 2 WAN

```
crypto isakmp policy 15
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key c1sco123 address 10.4.32.151
crypto isakmp key c1sco123 address 10.4.32.152
!
crypto gdoi group GETVPN-GROUP
 identity number 65511
 server address ipv4 10.4.32.151
 server address ipv4 10.4.32.152
!
!
crypto map GETVPN-MAP local-address Loopback0
crypto map GETVPN-MAP 10 gdoi
 set group GETVPN-GROUP
```

Example: MPLS CE router

```
interface GigabitEthernet0/0/3
 description Connection to MPLS PE router
 ip tcp adjust-mss 1360
 crypto map GETVPN-MAP
```

Example: Layer 2 WAN CE router (with trunked demarcation)

```
interface GigabitEthernet0/0/3.38
 encapsulation dot1Q 38
 description Connection to Layer 2 WAN
 ip tcp adjust-mss 1360
 crypto map GETVPN-MAP
```

Appendix A: Product List

WAN Aggregation

Functional Area	Product Description	Part Numbers	Software
GET VPN Key Server	Cisco 2951 Security Bundle with Security License	CISCO2951-SEC/K9	15.3(3)M3 securityk9 feature set
WAN-aggregation Router	Aggregation Services 1002X Router	ASR1002X-5G-VPNK9	IOS-XE 15.4(2)S Advanced Enterprise feature set
	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	
	Cisco ISR 4451-X Security Bundle w/SEC license PAK	ISR4451-X-SEC/K9	IOS-XE 15.4(2)S securityk9 feature set

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco ISR 4451 w/ 4GE,3NIM,2SM,8G FLASH, 4G DRAM, IP Base, SEC, AX license with: DATA, AVC, ISR-WAAS with 2500 connection RTU	ISR4451-X-AX/K9	IOS-XE 15.4(2)S securityk9 feature set appxk9 feature set
	Cisco ISR 3945 w/ SPE150, 3GE, 4EHWIC, 4DSP, 4SM, 256MBCF, 1GBDRAM, IP Base, SEC, AX licenses with; DATA, AVC, and WAAS/vWAAS with 2500 connection RTU	C3945-AX/K9	15.3(3)M3 securityk9 feature set datak9 feature set uck9 feature set
	Cisco ISR 3925 w/ SPE100 (3GE, 4EHWIC, 4DSP, 2SM, 256MBCF, 1GBDRAM, IP Base, SEC, AX licenses with; DATA, AVC, WAAS/vWAAS with 2500 connection RTU	C3925-AX/K9	
	Unified Communications Paper PAK for Cisco 3900 Series	SL-39-UC-K9	
	Cisco ISR 2951 w/ 3 GE, 4 EHWIC, 3 DSP, 2 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC, and WAAS/vWAAS with 1300 connection RTU	C2951-AX/K9	15.3(3)M3 securityk9 feature set datak9 feature set uck9 feature set
	Cisco ISR 2921 w/ 3 GE, 4 EHWIC, 3 DSP, 1 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC, and WAAS/vWAAS with 1300 connection RTU	C2921-AX/K9	
	Cisco ISR 2911 w/ 3 GE,4 EHWIC, 2 DSP, 1 SM, 256MB CF, 1GB DRAM, IP Base, SEC, AX license with; DATA, AVC and WAAS/vWAAS with 1300 connection RTU	C2911-AX/K9	
	Unified Communications Paper PAK for Cisco 2900 Series	SL-29-UC-K9	
	Cisco ISR 1941 Router w/ 2 GE, 2 EHWIC slots, 256MB CF, 2.5GB DRAM, IP Base, DATA, SEC, AX license with; AVC and WAAS-Express	C1941-AX/K9	15.3(3)M3 securityk9 feature set datak9 feature set
Fixed WAN Remote-site Router	Cisco 891 Router	CISCO891W-AGN-A-K9	15.3(3)M3 securityk9 feature set datak9 feature set
	WAAS-Express/AVC/Advanced IP with upgrade up to 1GB DRAM for Cisco 800 Series Routers	FL-C800-APP	

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis	C6807-XL	15.1(2)SY3 IP Services feature set
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
	Cisco Catalyst 6500 CEF720 48 port 10/100/1000mb Ethernet	WS-X6748-GE-TX	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
	Cisco Catalyst 6500 Series 6506-E 6-Slot Chassis	WS-C6506-E	
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
	Cisco Catalyst 6500 48-port GigE Mod (SFP)	WS-X6748-SFP	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
	Cisco Catalyst 6500 24-port GigE Mod (SFP)	WS-X6724-SFP	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.5.3E(15.2.1E3) Enterprise Services feature set
	Cisco Catalyst 4500E Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
	Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45)	WS-X4748-RJ45V+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3850 Series Stackable Switch with 12 SFP Ethernet	WS-C3850-12S	3.3.3SE(15.0.1EZ3) IP Services feature set
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.2(1)E3 IP Services feature set
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Appendix B: Device Configuration Files

GET VPN Primary Key Server

```
version 15.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname KS-2951-1
!
!
!
enable secret 5 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
!
ip cef
!
!
ip domain name cisco.local
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
no ipv6 cef
!
multilink bundle-name authenticated
!
```

```
!
voice-card 0
!
!
license udi pid CISCO2951/K9 sn FHK1436F09P
license boot module c2951 technology-package securityk9
!
username admin password 7 08221D5D0A16544541
!
redundancy
!
!
ip ssh version 2
ip scp server enable
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp policy 15
 encr aes 256
 authentication pre-share
 group 2
 lifetime 1200
crypto isakmp key c1sco123 address 0.0.0.0
crypto isakmp keepalive 15 periodic
!
!
crypto ipsec transform-set AES256/SHA esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile GETVPN-PROFILE
 set security-association lifetime seconds 7200
 set transform-set AES256/SHA
!
!
crypto gdoi group GETVPN-GROUP
 identity number 65511
 server local
  rekey algorithm aes 256
  rekey retransmit 40 number 3
  rekey authentication mypubkey rsa GETVPN-REKEY-RSA
  rekey transport unicast
  sa ipsec 10
   profile GETVPN-PROFILE
```

```
   match address ipv4 GETVPN-POLICY-ACL
   replay time window-size 20
  address ipv4 10.4.32.151
  redundancy
   local priority 100
   peer address ipv4 10.4.32.152
!
!
interface Port-channel21
 ip address 10.4.32.151 255.255.255.192
 hold-queue 150 in
!
!
interface GigabitEthernet0/0
 description WAN-D3750X Gig1/0/9
 no ip address
 duplex auto
 speed auto
 channel-group 21
!
interface GigabitEthernet0/1
 description WAN-D3750X Gig2/0/9
 no ip address
 duplex auto
 speed auto
 channel-group 21
!
!
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.4.32.129
!
ip access-list extended GETVPN-POLICY-ACL
 remark >> exclude transient encrypted traffic (ESP, ISAKMP, GDOI)
 deny   esp any any
 deny   udp any eq isakmp any eq isakmp
 deny   udp any eq 848 any eq 848
 remark >> exclude encrypted in-band management traffic (SSH, TACACS+)
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any any eq tacacs
 deny   tcp any eq tacacs any
 remark >> exclude routing protocol with MPLS provider
```

```
 deny   tcp any any eq bgp
 deny   tcp any eq bgp any
 remark >> exclude routing protocol used for Layer 2 WAN
 deny   eigrp any any
 remark >> exclude PIM protocol
 deny   pim any host 224.0.0.13
 remark >> exclude IGMP with MPLS provider
 deny   igmp any host 224.0.0.1
 deny   igmp host 224.0.0.1 any
 deny   igmp any host 224.0.1.40
 deny   igmp host 224.0.1.40 any
 remark >> exclude icmp traffic destined to SP address
 deny   icmp any 192.168.3.0 0.0.0.255
 deny   icmp 192.168.3.0 0.0.0.255 any
 deny   icmp any 192.168.4.0 0.0.0.255
 deny   icmp 192.168.4.0 0.0.0.255 any
 remark >> exclude icmp traffic destined to KS from Loopback address
 deny   icmp host 10.4.32.151 10.255.0.0 0.0.255.255
 deny   icmp 10.255.0.0 0.0.255.255 host 10.4.32.151
 deny   icmp host 10.4.32.152 10.255.0.0 0.0.255.255
 deny   icmp 10.255.0.0 0.0.255.255 host 10.4.32.152
 remark >> Require all other traffic to be encrypted
 permit ip any any
!
access-list 55 permit 10.4.48.0 0.0.0.255
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server enable traps entity-sensor threshold
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 097F4B0A0B0003390E15
!
control-plane
!
!
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
```

```
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 access-class 55 in
 transport preferred none
 transport input ssh
line vty 5 15
 access-class 55 in
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp update-calendar
ntp server 10.4.48.17
!
end
```

GET VPN Secondary Key Server

```
version 15.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname KS-2951-2
!
!
aaa new-model
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
ip cef
!
!
ip domain name cisco.local
ipv6 spd queue min-threshold 62
```

```
ipv6 spd queue max-threshold 63
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
license udi pid CISCO2951/K9 sn FTX1446AKD8
hw-module pvdm 0/0
!
!
username admin password 7 13061E010803557878
!
redundancy
!
!
ip ssh version 2
ip scp server enable
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp policy 15
 encr aes 256
 authentication pre-share
 group 2
 lifetime 1200
crypto isakmp key c1sco123 address 0.0.0.0
crypto isakmp keepalive 15 periodic
!
!
crypto ipsec transform-set AES256/SHA esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile GETVPN-PROFILE
 set security-association lifetime seconds 7200
 set transform-set AES256/SHA
!
!
crypto gdoi group GETVPN-GROUP
 identity number 65511
 server local
  rekey algorithm aes 256
  rekey retransmit 40 number 3
  rekey authentication mypubkey rsa GETVPN-REKEY-RSA
```

```
  rekey transport unicast
  sa ipsec 10
   profile GETVPN-PROFILE
   match address ipv4 GETVPN-POLICY-ACL
   replay time window-size 20
  address ipv4 10.4.32.152
  redundancy
   local priority 75
   peer address ipv4 10.4.32.151
!
!
interface Port-channel22
 ip address 10.4.32.152 255.255.255.192
 hold-queue 150 in
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description WAN-D3750X Gig1/0/10
 no ip address
 duplex auto
 speed auto
 channel-group 22
!
interface GigabitEthernet0/1
 description WAN-3750X Gig2/0/10
 no ip address
 duplex auto
 speed auto
 channel-group 22
!
!
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.4.32.129
!
ip access-list extended GETVPN-POLICY-ACL
 remark >> exclude transient encrypted traffic (ESP, ISAKMP, GDOI)
 deny   esp any any
 deny   udp any eq isakmp any eq isakmp
 deny   udp any eq 848 any eq 848
```

```
 remark >> exclude encrypted in-band management traffic (SSH, TACACS+)
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any any eq tacacs
 deny   tcp any eq tacacs any
 remark >> exclude routing protocol with MPLS provider
 deny   tcp any any eq bgp
 deny   tcp any eq bgp any
 remark >> exclude routing protocol used for Layer 2 WAN
 deny   eigrp any any
 remark >> exclude PIM protocol
 deny   pim any host 224.0.0.13
 remark >> exclude IGMP with MPLS provider
 deny   igmp any host 224.0.0.1
 deny   igmp host 224.0.0.1 any
 deny   igmp any host 224.0.1.40
 deny   igmp host 224.0.1.40 any
 remark >> exclude icmp traffic destined to SP address
 deny   icmp any 192.168.3.0 0.0.0.255
 deny   icmp 192.168.3.0 0.0.0.255 any
 deny   icmp any 192.168.4.0 0.0.0.255
 deny   icmp 192.168.4.0 0.0.0.255 any
 remark >> exclude icmp traffic destined to KS from Loopback address
 deny   icmp host 10.4.32.151 10.255.0.0 0.0.255.255
 deny   icmp 10.255.0.0 0.0.255.255 host 10.4.32.151
 deny   icmp host 10.4.32.152 10.255.0.0 0.0.255.255
 deny   icmp 10.255.0.0 0.0.255.255 host 10.4.32.152
 remark >> Require all other traffic to be encrypted
 permit ip any any
!
logging host 10.4.48.48
access-list 55 permit 10.4.48.0 0.0.0.255
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server enable traps entity-sensor threshold
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 13361211190910012E3D
!
!
line con 0
 logging synchronous
```

```
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 access-class 55 in
 transport preferred none
 transport input ssh
line vty 5 15
 access-class 55 in
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp update-calendar
ntp server 10.4.48.17
!
end
```

GET VPN Group Member

```
version 15.4
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no platform punt-keepalive disable-kernel-core
!
hostname CE-ASR1002-1
!
boot-start-marker
boot system bootflash:asr1000rp1-adventerprisek9.03.12.00.S.154-2.S-std.bin
boot-end-marker
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 5 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
```

```
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
ip nbar protocol-pack flash:pp-adv-asr1k-154-2.S-18-10.0.0.pack
!
!
ip domain name cisco.local
ip multicast-routing distributed
!
!
subscriber templating
!
!
!
multilink bundle-name authenticated
!
key chain CAMPUS-KEY
 key 1
   key-string 7 130646010803557878
key chain LAN-KEY
 key 1
   key-string 7 070C285F4D06
!
!
spanning-tree extend system-id
!
username admin password 7 03070A180500701E1D
!
redundancy
 mode none
!
!
cdp run
!
ip tftp source-interface Loopback0
ip ssh source-interface Loopback0
ip ssh version 2
```

```
ip scp server enable
!
class-map match-any DATA
 match dscp af21
class-map match-any BGP-ROUTING
 match protocol bgp
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4  af41
class-map match-any CRITICAL-DATA
 match dscp cs3  af31
class-map match-any VOICE
 match dscp ef
class-map match-any SCAVENGER
 match dscp cs1  af11
class-map match-any TP-MEDIA
 match protocol telepresence-media
class-map match-any NETWORK-CRITICAL
 match dscp cs2  cs6
!
policy-map MARK-BGP
 class BGP-ROUTING
  set dscp cs6
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
   service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0/3
 class class-default
  shape average 300000000
   service-policy WAN
policy-map type performance-monitor PerfMon-Baseline
 description PerfMon Baseline
```

```
 class INTERACTIVE-VIDEO
  flow monitor PerfMon-All-RTP
  react 10 transport-packets-lost-rate
   description Check for > 1% loss
   threshold value gt 1.00
   alarm severity critical
   action syslog
   action snmp
  react 20 rtp-jitter-average
   description Check for > 25 ms average jitter
   threshold value gt 25000
   alarm severity critical
   action syslog
   action snmp
 class TP-MEDIA
  flow monitor PerfMon-All-RTP
  monitor metric rtp
   clock-rate 96 48000
   clock-rate 101 8000
 class DATA
  flow monitor PerfMon-All-TCP
 class CRITICAL-DATA
  flow monitor PerfMon-All-TCP
 class VOICE
  flow monitor PerfMon-All-RTP
!
!
crypto isakmp policy 15
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key c1sco123 address 10.4.32.151
crypto isakmp key c1sco123 address 10.4.32.152
!
!
crypto gdoi group GETVPN-GROUP
 identity number 65511
 server address ipv4 10.4.32.151
 server address ipv4 10.4.32.152
!
!
crypto map GETVPN-MAP local-address Loopback0
crypto map GETVPN-MAP 10 gdoi
 set group GETVPN-GROUP
!
!
interface Loopback0
```

```
 ip address 10.4.32.241 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel1
 ip address 10.4.32.2 255.255.255.252
 ip pim sparse-mode
 no negotiation auto
!
interface GigabitEthernet0/0/0
 description WAN-D3750X Gig1/0/1
 no ip address
 negotiation auto
 channel-group 1
!
interface GigabitEthernet0/0/1
 description WAN-D3750X Gig2/0/1
 no ip address
 negotiation auto
 channel-group 1
!
interface GigabitEthernet0/0/3
 description MPLS WAN Uplink
 bandwidth 300000
 ip address 192.168.3.1 255.255.255.252
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 negotiation auto
 crypto map GETVPN-MAP
 service-policy output WAN-INTERFACE-G0/0/3
!
!
router eigrp CAMPUS
 !
 address-family ipv4 unicast autonomous-system 100
  !
  af-interface default
   passive-interface
  exit-af-interface
  !
  af-interface Port-channel1
   authentication mode md5
   authentication key-chain CAMPUS-KEY
   no passive-interface
  exit-af-interface
  !
  topology base
   default-metric 300000 100 255 1 1500
```

```
   distribute-list route-map BLOCK-TAGGED-ROUTES in
   redistribute bgp 65511
  exit-af-topology
  network 10.4.0.0 0.1.255.255
  eigrp router-id 10.4.32.241
  nsf
 exit-address-family
!
router bgp 65511
 bgp router-id 10.4.32.241
 bgp log-neighbor-changes
 network 0.0.0.0
 network 192.168.3.0 mask 255.255.255.252
 redistribute eigrp 100
 neighbor 10.4.32.242 remote-as 65511
 neighbor 10.4.32.242 update-source Loopback0
 neighbor 10.4.32.242 next-hop-self
 neighbor 192.168.3.2 remote-as 65401
!
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
ip pim autorp listener
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
!
access-list 55 permit 10.4.48.0 0.0.0.255
!
route-map BLOCK-TAGGED-ROUTES deny 10
 match tag 65401 65402 65512
!
route-map BLOCK-TAGGED-ROUTES permit 20
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server trap-source Loopback0
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 00371605165E1F2D0A38
!
control-plane
!
line con 0
 logging synchronous
```

```
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 55 in
 exec-timeout 0 0
 transport preferred none
 transport input ssh
line vty 5 15
 access-class 55 in
 transport preferred none
 transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
!
end
```

Appendix C: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We updated EIGRP for named mode configuration.
- We added the **ip scp server enable** command to the router configuration.
- We added the use of a global crypto keyring for consistency across other CVDs.
- We increased the replay time window-size to 20 in order to reduce the likelihood of false replay messages.

Feedback

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

B-0000285-1 08/14