Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

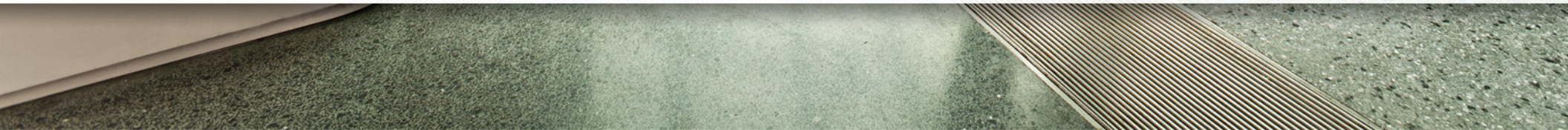
BORDERLESS NETWORKS

DEPLOYMENT GUIDE

GET VPN Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series



Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

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

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

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

Comments and Questions

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

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide

Cisco SBA Borderless Networks

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

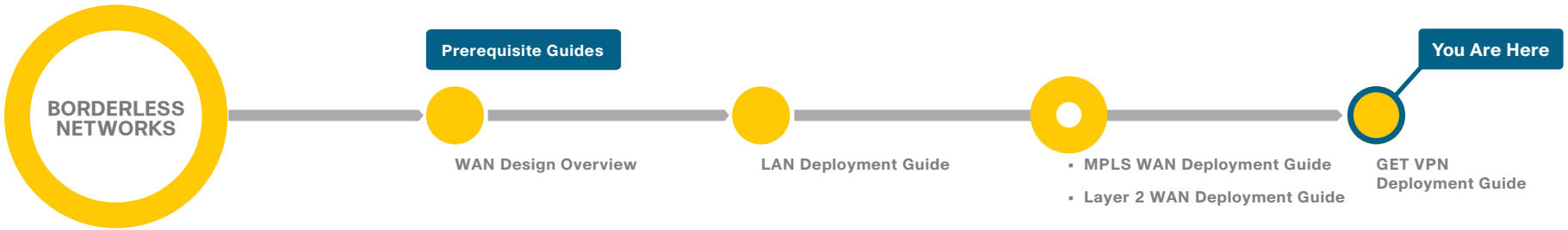
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



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.

Business Overview

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).

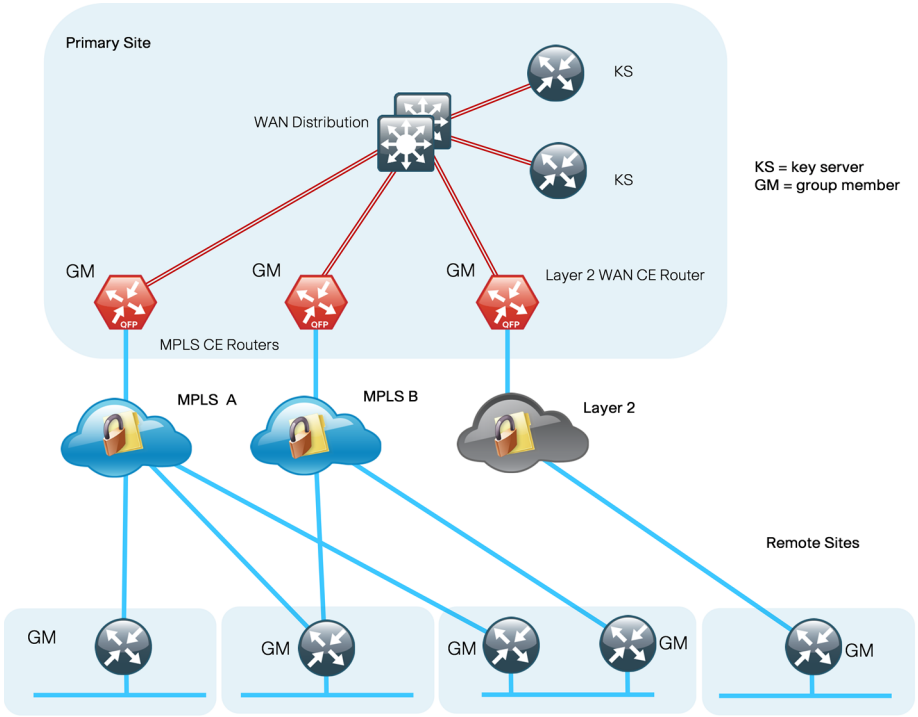
Technology Overview

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

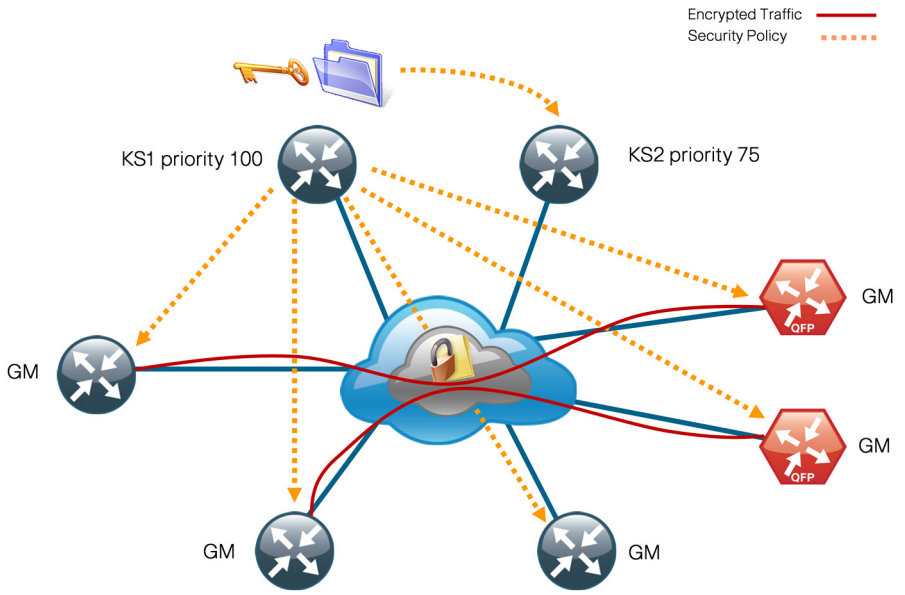


GET VPN Components

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

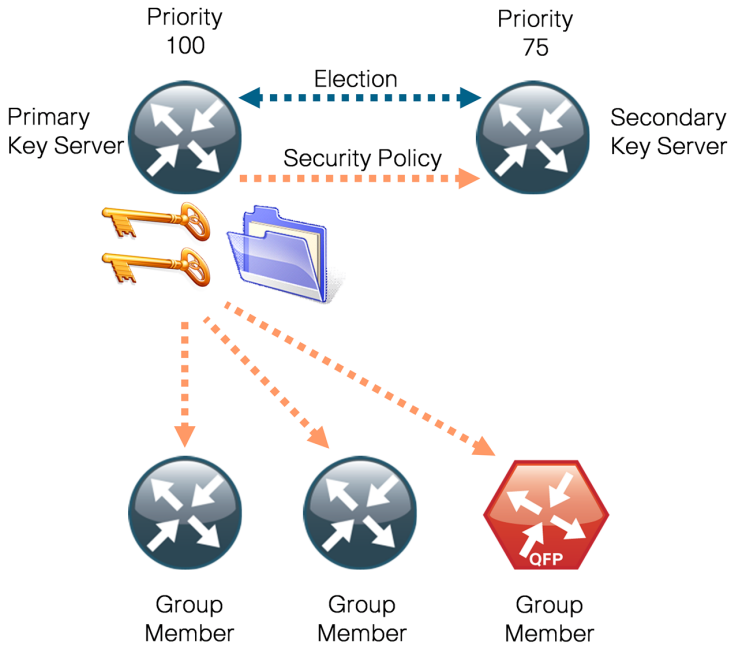


The KS sends out rekey messages as needed. The rekey message contains new encryption policy and encryption keys to use when the old IPSec Security Association (SA) expires. The rekey message is sent in advance of the SA expiration, which helps ensure that the new keys are available to all GMs.

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



Notes

Deployment Details

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 redundancy on primary KS
7. Configure secondary 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: Configure Layer 3 (if necessary).

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
```

Step 3: Configure EtherChannel member interfaces.

Tech Tip

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

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
 macro apply EgressQoS
 channel-group 21 mode on
 logging event link-status
 logging event bundle-status
```

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
 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.

Reader Tip

The AAA server used in this architecture is the Cisco Access Control System (ACS). For details about ACS configuration, see the *Cisco SBA—Borderless Networks Device Management Using ACS Deployment Guide*.

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 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 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
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 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.

Provide reachability information for the KS to reach GMs 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.

Before starting KS configuration, generate exportable RSA keys to be used during rekeys.

Step 1: Generate an RSA key to 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 will allow 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]
```

Step 2: Export RSA keys from the primary KS.

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

Tech Tip

In this example, you export the RSA key pair from the primary KS to a privacy-enhanced mail (PEM) format. We suggest that you use copy and paste from the KS console to a file, and store the file in a secure environment. You will use the key pair later to build secondary KSs or, if necessary, to rebuild the primary KS.

Repeat for both the public key and private key information.

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 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. The rekey algorithm is defined using AES-256 and using RSA signature for rekey authentication.

Step 8: 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 5
```

Step 9: 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 as shown in Step 8.

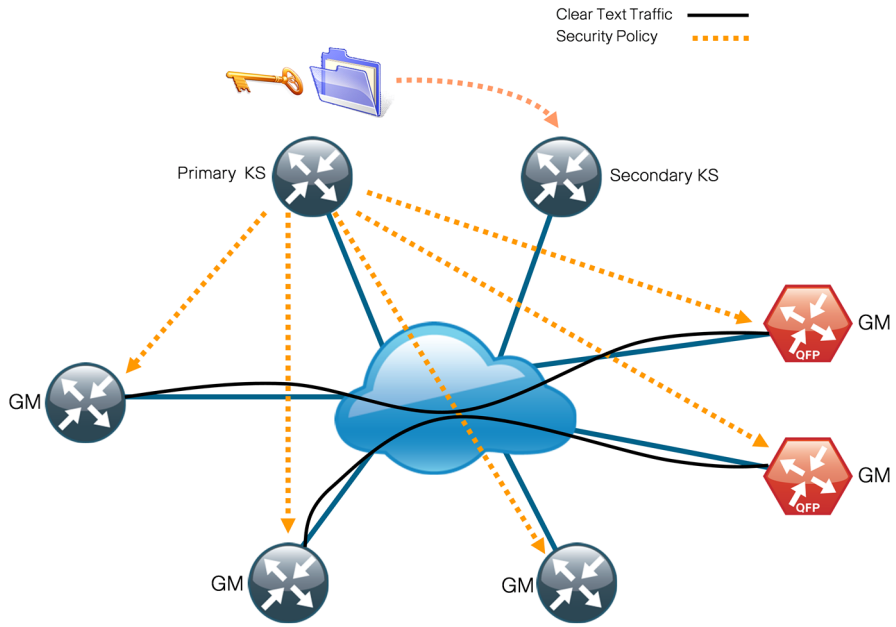
```
ip access-list extended GETVPN-POLICY-ACL
 remark >> exclude transient encrypted traffic (ESP, ISAKMP,
GDOI)
 deny   esp any any
 deny   udp any eq isakmp any eq isakmp
 deny   udp any eq 848 any eq 848
 remark >> exclude encrypted in-band management traffic (SSH,
TACACS+)
 deny   tcp any any eq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

Tech Tip

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. The following command enables the receive-only SA capability on the KS.

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

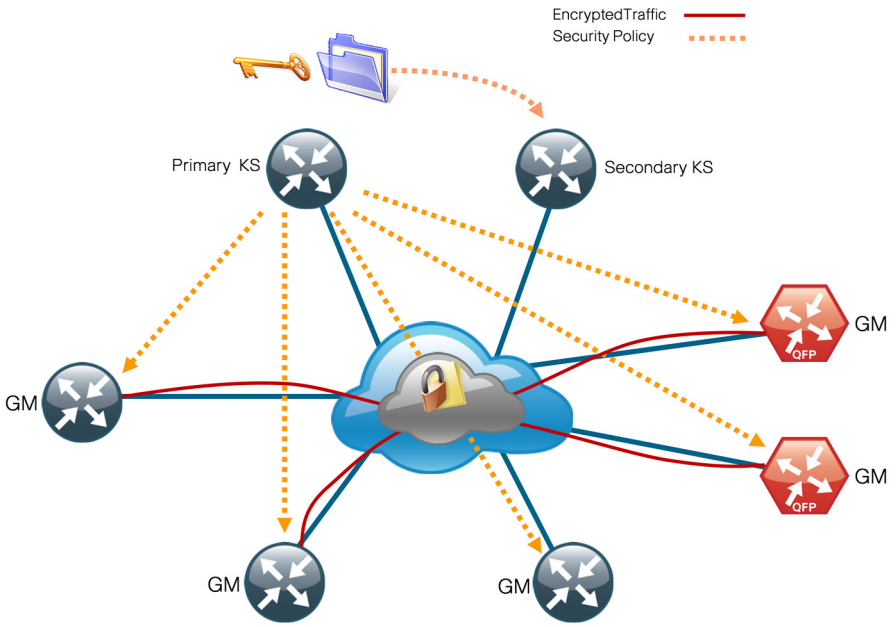
Figure 4 - Receive-only mode



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.

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

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 >> Require all other traffic to be encrypted
 permit ip any any
```

Procedure 6 Configure redundancy on primary KS

To achieve redundancy and high availability in a GET VPN network, Cisco recommends having at least two KSs running in COOP KS mode. 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.

Tech Tip

To minimize disruptions to the existing KS when adding a new KS into the COOP KS mode, we recommend that redundancy should be configured on the secondary KS in Procedure 7 Step 4 first, before redundancy is enabled on the primary KS.

```
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
```

Procedure 7 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 to configure the distribution switch. Follow this with Procedure 2, and Procedure 3. Then, complete the following steps. Identical policies must be configured between the primary and secondary KS. 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 from the primary KS that were created in Procedure 4. 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
ztRJIwLWJc682EIOK2IuhhNb05XAt3xXO241wNSvgE5zAtE9p2Z81GSevcWjfmoi
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 KS 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 results 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: Complete Procedure 5 (all steps) for the secondary KS

Tech Tip

Be sure to use the IP address of the secondary KS in Step 7

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

To minimize disruptions to the existing KS when adding a new KS into the COOP KS mode, we recommend that redundancy should be configured on the secondary KS first, before redundancy is enabled on the primary KS in Procedure 6 Step 1.

```
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
```

Process

Implementing Group Member

1. Configure a GM

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

Reader Tip

For complete MPLS CE router configuration, see *Cisco SBA—Borderless Networks MPLS WAN Deployment Guide*.

For complete Layer 2 WAN CE router configuration, see *Cisco SBA—Borderless Networks Layer 2 WAN Deployment Guide*.

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: 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 3: 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 4: 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 the 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 5: 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 6: 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 only affects 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
```

Notes

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	15.1(4)M2
WAN-aggregation Router	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	IOS-XE 15.2(2)S2 Advanced Enterprise
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	
WAN-aggregation Router	Cisco 3945 Security Bundle w/SEC license PAK	CISCO3945-SEC/K9	15.1(4)M4
	Cisco 3925 Security Bundle w/SEC license PAK	CISCO3925-SEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.1(4)M4
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
Modular WAN Remote-site Router	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	15.1(4)M4
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	
Modular WAN Remote-site Router	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	15.1(4)M4 securityk9, datak9
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	
Fixed WAN Remote-site Router	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.1(4)M4 securityk9, datak9

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) IP Base
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	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	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	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	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(1)SE2 LAN Base
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1 IP services
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP	
	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	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) Enterprise Services
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(1)SE2 IP Services
	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 Key Server

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname KS-2951-1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 **********************
!
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 authorization console
ip http authentication aaa
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
crypto pki token default removal timeout 0
!
no ipv6 cef
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
ip source-route
ip cef
!
!
!
!
!
ip domain name cisco.local
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
license udi pid CISCO2951/K9 sn ***********
license boot module c2951 technology-package securityk9
hw-module pvdm 0/0
!
!
!
username admin password 7 **************
!
```

```
redundancy
!
!
!
!
ip ssh version 2
!
!
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-ACL
   replay time window-size 5
  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 Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 channel-group 21
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 channel-group 21
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```
ip forward-protocol nd
!
no ip http server
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 >> Require all other traffic to be encrypted
 permit ip any any
!
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server community cisco RO
snmp-server community cisco123 RW
!
!
!
control-plane
!
!
!
!
mgcp profile default
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 113A1C0605171F270133
!
!
!
!
gatekeeper
 shutdown
!
!
!
line con 0
 logging synchronous
line aux 0
line 2
```

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

GET VPN Group Member

```
version 15.1
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-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 4 ******************
!
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 authorization console
ip http authentication aaa
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
!
!
ip domain name cisco.local
ip multicast-routing distributed
!
!
!
!
!
!
multilink bundle-name authenticated
!
!
!
```

```
!
!
!
!
!
!
username admin password 7 ***************
!
redundancy
 mode none
!
!
!
!
!
ip tftp source-interface Loopback0
ip ssh source-interface Loopback0
ip ssh version 2
!
!
!
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
 no ip address
 negotiation auto
 channel-group 1 mode active
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 channel-group 1 mode active
!
interface GigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/3
 description WAN Interface
 bandwidth 300000
 ip address 192.168.3.1 255.255.255.252
 ip tcp adjust-mss 1360
 negotiation auto
 crypto map GETVPN-MAP
!
interface GigabitEthernet0
```

```
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
!
router eigrp 100
 distribute-list route-map BLOCK-TAGGED-ROUTES in
 default-metric 100000 100 255 1 1500
 network 10.4.0.0 0.1.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface Port-channel1
 eigrp router-id 10.4.32.241
!
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 tacacs source-interface Loopback0
!
!
route-map BLOCK-TAGGED-ROUTES deny 10
 match tag 65401 65402 65512
!
route-map BLOCK-TAGGED-ROUTES permit 20
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 113A1C0605171F270133
!
!
control-plane
!
!
!
!
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 transport input ssh
line vty 5 15
 transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
end
```

Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- The software release for the Cisco ASR 1000 Series routers used as GET VPN GM was updated to IOS-XE 15.2(2)S2.
- The software release for the Cisco ISR-G2 Series routers used as GET VPN GM was updated to IOS 15.1(4)M4.

Notes

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

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-0000185-1 9/12