Cisco IOS GETVPN Solution Deployment Guide

Purpose and Scope

This document provides basic deployment guidelines to enable Cisco IOS Group Encrypted Transport VPN (GETVPN) in an enterprise network. This document does not cover in-depth technical details about various features comprising Cisco IOS GETVPN. Please refer to the References section for additional documents.

Introduction to GETVPN

The Cisco IOS GETVPN is a tunnel-less VPN technology that provides end-to-end security for network traffic in a native mode and maintaining the fully meshed topology. It uses the core network's ability to route and replicate the packets between various sites within the enterprise. Cisco IOS GETVPN preserves the original source and destination IP addresses information in the header of the encrypted packet for optimal routing. Hence, it is largely suited for an enterprise running over a private Multiprotocol Label Switching (MPLS)/IP-based core network. It is also better suited to encrypt multicast traffic.

Cisco IOS GET VPN uses Group Domain of Interpretation (GDOI) as the keying protocol and IPSec for encryption.

Cisco IOS GET VPN Benefits

Following are some of the advantages of GETVPN over other VPN technologies.

- Provides highly scalable any to any mesh topology natively and eliminates the need for complex peer-to-peer security associations.
- For Multiprotocol Label Switching (MPLS) networks, maintains network intelligence (such as full-mesh connectivity, natural routing path, and QoS).Grants easy membership control with centralized key servers.
- Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub.
- GETVPN allows replication of the packets after encryption. This allows the multicast traffic to be replicated at the core, thereby reducing the load and band width requirement on the Customer Premises Equipment (CPE).
- IP Address Preservation enables encrypted packets carry the original source and destination IP addresses in the outer IP header rather than replacing them with tunnel endpoint addresses. This technique is known as IPSec Tunnel Mode with Address Preservation. Some of the IP header parameters are also preserved. Many network features like routing, basic firewall, QoS, traffic management etc. work based on the information contained in the IP header. Since the IP header is persevered, all the network features will work as before. This eliminates lot of issues associated with deploying point to point encryption in a core network.

Hardware Platforms and Software Images

This document is written based on the following software versions and hardware. The following list is not the complete list of platforms supported.

Key Servers: Cisco 3845, Cisco 7200

Group Members: Cisco 881, Cisco 1811, Cisco1841, Cisco 3845, Cisco 7200, Cisco ASR1004

IOS image version: 12.4(15)T8 and 12.4(22)T2

IOS-XE image version: 12.2(33)XNC

GETVPN Technology Overview

A GETVPN deployment has primarily three components, Key Server (KS), Group Member (GM), and Group Domain of Interpretation (GDOI) protocol. GMs do encrypt/decrypt the traffic and KS distribute the encryption key to all the group members. The KS decides on one single data encryption key for a given life time. Since all GMs use the same key, any GM can decrypt the traffic encrypted by any other GM. GDOI protocol is used between the GM and KS for group key and group SA management. Minimum one KS is required for a GETVPN deployment.

Unlike traditional IPSec encryption solutions, GET VPN uses the concept of group SA. All members in the GETVPN group can communicate with each other using a common encryption policy and a shared SA and therefore no need to negotiate IPSec between GMs on a peer to peer basis; thereby reducing the resource load on the GM routers.

Group Member

The group member registers with the key server to get the IPSec SA that is necessary to encrypt data traffic within the group. The group member provides the group ID to the key server to get the respective policy and keys for this group. These keys are refreshed periodically by KS, and before the current IPSec SAs expire, so that there is no loss of traffic.

Key Server

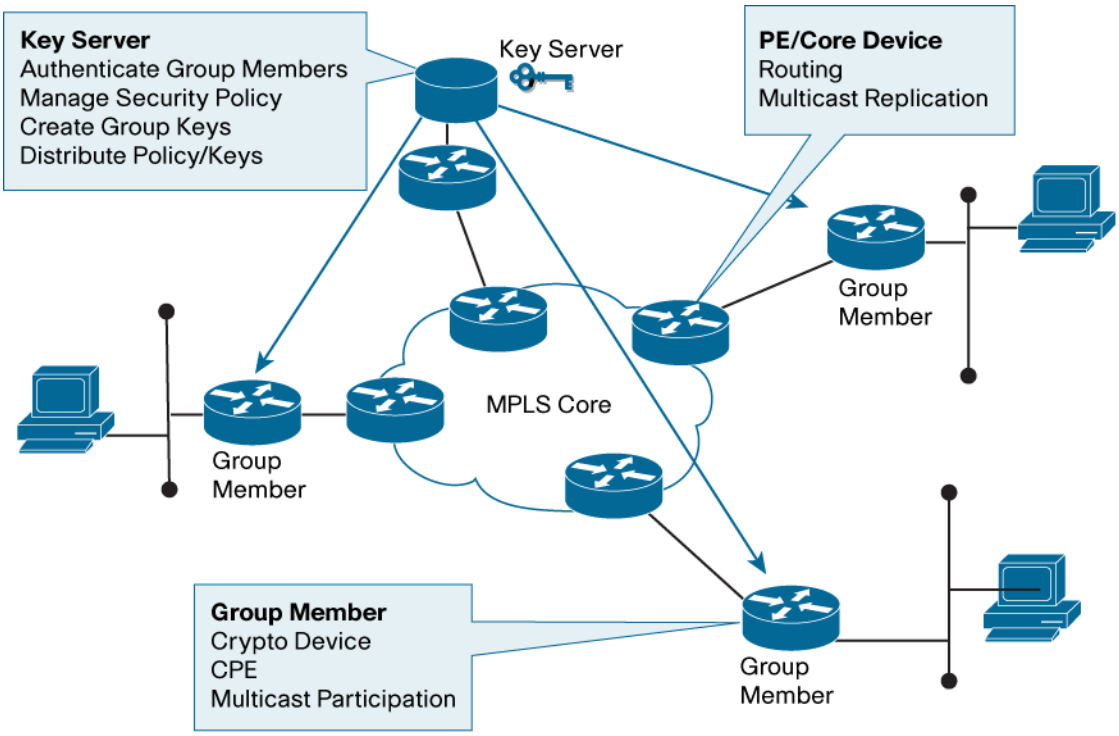
Key server is responsible for maintaining security policies, authenticating the GMs and providing the session key for encrypting traffic. KS authenticates the individual GMs at the time of registration. Only after successful registration the GMs can participate in group SA.

A group member can register at any time and receive the most current policy and keys. When a GM registers with the key server, the key server verifies the group id number of the GM. If this id number is a valid and the GM has provided valid Internet Key Exchange (IKE) credentials, the key server sends the SA policy and the Keys to the group member.

There are two types of keys that the GM will receive from the KS: the Key Encryption Key (KEK) and the Traffic Encryption Key (TEK). The TEK becomes part of the IPSec SA with which the group members within the same group encrypt the data. KEK is used to secure rekey messages between the key server and the group members.

The Key Server sends out rekey messages either because of an impending IPSec SA expiration or because the security policy has changed on the key server. Keys can be distributed during re-key using either multicast or unicast transport. Multicast method is more scalable as keys need not be transmitted to each group member individually. Unlike in unicast, KS will not receive acknowledgement from GM about the success of the rekey reception in multicast rekey method. In unicast rekey method, KS will delete a GM from its database if three consecutive rekeys are not acknowledged by that particular GM.

Figure 1. GETVPN Components



GDOI Protocol

GDOI protocol is used for Group key and group SA management. GDOI uses Internet Security Association Key Management Protocol (ISAKMP) for authenticating the GMs and KSs. All the standard ISAKMP authentication schemes like RSA Signature (certificates) and Pre-shared key can be used for GETVPN.

All the necessary crypto policies are configured only on the KS. This includes the crypto access list, crypto policies, life times etc.

Typically the KS is installed in the data center of the customer network. The CPE routers connecting to the MPLS core is configured as GMs. The KS should be reachable from all GMs through the core or the enterprise network.

The steps below explain protocol flows that are necessary for Group Members to participate in a GETVPN group:

1. Once the GM boots up, it attempts to register with the KS using the GDOI protocol.
2. Registration goes through after successful mutual authentication.
3. After successful registration GM receives KEK and TEK keys.
4. GMs can now encrypt and decrypt the packets as specified by the SA.
5. KS keeps track of the SA life time. It sends rekey information when the current SA is about to expire. Rekey information includes the new SA and session key details. Rekey messages are sent in advance of the SA expiration time to ensure that valid group keys are always available.

GETVPN supports only time based SA expiry. Volume based expiry is not practical when many devices use the same SA as in the case of GETVPN.

Advanced GETVPN Features

These are some of the GETVPN features which make its deployment easier, more scalable and resilient.

- Cooperative Key Server
- Receive-only SA
- Passive SA Mode
- Fail Close mode
- Local Exception ACL
- Time-based Anti Replay
- VRF-lite support on Group Member

Next section explains each of this feature and its configurations.

Configuring and Deploying GETVPN

Basic GETVPN

This section provides the basic configuration for a sample GETVPN setup with one KS and a sample GM. The following sections will provide the configurations for more advanced features. At least two GMs and a KS are needed to establish a basic GETVPN deployment.

Configuring Key Server

This sample configuration uses pre-shared key authentication for simplicity and also assumes single Key Server. In production deployments it is recommended to have at least two key Servers in co-operative mode to ensure redundancy. The IKE configuration for GETVPN is same as the standard IPSec.

A basic KS configuration should include at least the following.

- **IKE Policy:** IKE used as the authentication mechanism when GMs register with KS. Sample configuration used pre-shared key. Using digital certificates is preferred and more secure.
- **RSA Key for re-keying:** This is used to secure the re-key messages.
- **IPSec polices:** This defines the policies used to secure the data traffic (like encryption algorithm, per packet authentication, life times, etc.)
- **Traffic classification ACL:** This determines which traffic should be encrypted. “permit any any” is allowed in GETVPN. But care should be taken to exclude critical traffic which should be allowed to pass always.

Basic Key Server Configuration:

```
!
! ISAKMP Policy
crypto isakmp policy 1
 encr aes
 ! Pre-shared key autentication
 authentication pre-shared
 group 2
 lifetime 86400
!
! Define pre-shared keys for each GM and other KS if any.
```

```
crypto isakmp key tempkey1 address 10.0.1.1
! IPSec policy
!
crypto IPSec transform-set aes128 esp-aes esp-sha-hmac
crypto IPSec profile profile1
 ! IPSec SA life time
 set security-association lifetime seconds 7200
 ! Transfrom set to be used
 set transform-set aes128
!
Interface Loopback 0
 Ip address 10.0.0.1 255.255.255.255
!
interface GigabitEthernet0/1
 ! Interface connecting to the WAN network
 ip address 10.0.0.2 255.255.255.255
!
crypto gdoi group GDOI-GROUP1
 ! "GDOI-GROUP1" is the GETVPN group name
 ! Identity number for the Group
 identity number 12345
 server local
 rekey algorithm aes 128
 ! How often to rekey (KEY life time). It is good to
 ! rekey life time about three times of SA lifetime.
 rekey lifetime seconds 86400
 rekey authentication mypubkey rsa REKEYRSA
 rekey transport unicast
 ! Configure Security policies
 sa IPSec 1
  ! Policies
  profile profile1
  ! Traffic ACL
  match address ipv4 getvpn-acl
  ! Enable time base anti-replay with 5 second window
  replay time window-size 5
 address ipv4 10.0.0.1
```

```
! The following access list defines the traffic to
! be encrypted. Only those traffic which matches the
! "permit" lines will be encrypted. Care should be
! taken not to encrypt certain traffic which
! which should be permited always even if crypto sessions
! are not up.
!
ip access-list extended getvpn-acl
 deny udp any eq 848 any eq 848
 deny tcp any any eq ssh
 deny tcp any eq ssh any
 deny tcp any any eq tacacs
 deny tcp any eq tacacs any
 deny tcp any any eq bgp
 deny tcp any eq bgp any
 deny ospf any any
 deny eigrp any any
 deny udp any any eq ntp
 deny udp any eq ntp any
 deny udp any any eq snmp
 deny udp any eq snmp any
 deny udp any any eq snmp-trap
 deny udp any eq snmp-trap any
 deny udp any any eq syslog
 deny udp any eq syslog any
 ! Encrypt all the rest of the traffic
 permit ip any any
!
```

Installing RSA key for REKEY:

RSA key is used to secure the re-key transmission. So for the above sample configuration to work, an RSA key with label "REKEYRSA" needs to be created. To generate RSA key go to the configuration mode on the router and execute the following command.

```
"crypto key generate rsa modulus 1024 label REKEYRSA"
```

To verify if the keys exist on the router execute the below command at the enable prompt.

```
"show crypto key mypubkey rsa"
```

If more than one Key Server needs to be configured in co-op mode, the RSA key should made exportable at the time of key generation.

```
"crypto key generate rsa modulus 1024 label REKEYRSA exportable"
```

Basic Group Member Configuration

This section provides a sample configuration for the Group Member using pre-shared key based authentication and unicast re-keying. The configuration on the GM is relatively simple and almost same across all the GMs. This makes the deployment much easier.

The basic configuration should include at least the following sections.

- IKE Policy: This should match the policy on the GM. This sample configuration used pre-shared key. Using digital certificates is preferred and more secure. IKE SA is used only during registration. It is not needed after wards. Therefore low life time can be used and the faster expiry of the SAs may free up some resources on the KS.
- GDOI Crypto map: The GDOI policies
- Interface configuration: Crypto map applied on the interface

```
!
! ISAKMP Policy
crypto isakmp policy 1
 ! Small lifetime
 lifetime 300
 encr aes
 ! Pre-shared key autentication
 authentication pre-shared
 group 2
!
crypto isakmp key tempkey1 address 10.0.0.1
!
! GETVPN Group configuration
crypto gdoi group GDOI-GROUP1
 identity number 12345
 server address ipv4 10.0.0.1
!
! Crypto Map
crypto map gdoimap 1 gdoi
 set group GDOI-GROUP1
!
! Aply the crypto map on the interface
interface FastEthernet4
 ip address 10.0.1.1 255.255.255.0
 crypto map gdoimap
!
```

Multicast Rekeying

The KS will distribute the keys during re-key process using unicast or multicast. In unicast mode each GM is individually contacted and the key is provided. In multicast mode, the KS just announces the key information to a multicast address. All GMs join to that address group and get the key information. In case one of the GM does not receive the rekey, it will re-register with the KS again. Current SA and key will be downloaded as part of the registration. Using multicast rekey is more scalable compared to the unicast method but it needs a robust multicast infrastructure deployed on the core.

Apart from this multicast routing should be enabled on the core network between the KS and GMs and a multicast address should be reserved for sending rekey messages. The following configuration example uses Source-Specific Multicast (SSM) based multicast routing.

The following sections cover the configuration needs to be incorporated into the basic configuration for enabling multicast rekeying.

Key Server Configuration for Multicast Rekey

This is a sample incremental configuration needed to convert the GEVPN deployment from unicast to multicast rekey.

```
!
! Enable multi-cast routing
ip multi-cast routing
! Enable SSM mode
ip pim ssm range 1
!
! ACL list used in SSM range command
access-list 1 permit 239.192.1.190 0.0.0.0
!
interface GigabitEthernet0/1
 ! Interface connecting to the WAN network
 ip address 10.0.0.2 255.255.255.0
 ip pim sparse-mode
!
crypto gdoi group GDOI-GROUP1
 server local
 ! Default rekey method is multicast
 no rekey transport unicast
 ! Multicat group for re-keying. This is specified as a ACL
 rekey address ipv4 getvpn-rekey-multicast-group
 rekey retransmit 10 number 3
!
 ! Add these ACEs in getvpn-acl
ip access-list extended getvpn-acl
 deny ip any 224.0.0.0 0.255.255.255
```

```
 deny pim any host 224.0.0.13
!
ip access-list extended getvpn-rekey-multicast-group
 permit ip any host 239.192.1.190

!
```

Group Member Configuration for Multicast Rekey

Following configuration need to be added to the GMs to receive multicast rekey. This can be used only if multicast routing is enabled on rest of the network. Below configuration uses SSM for multicast. The configuration may need to be changed according to the existing multicast mechanism deployed in the network.

```
ip multicast-routing
! Enable SSM
ip igmp ssm-map enable
ip pim ssm range 1
! ACL used in ssm range command
access-list 1 permit 239.192.1.190 0.0.0.0
interface FastEthernet4
 ! Interface where crypto map is applied
 ip pim sparse-mode
! Join for each KS serving the group
 ip igmp join-group 239.192.1.190 source <IP-Addr-of-KS-1>
 ip igmp join-group 239.192.1.190 source <IP-Addr-of-KS-2>
 ...
```

Co-operative Key Server

Key Server is an essential component in a GETVPN deployment. If the KS becomes unavailable, the GMs will not be able to register or get new rekeys when the existing SA expires. Also in large deployments one KS will not be sufficient to handle the registration load of all the GMs.

Co-operative key server (COOP KS) solves the above two issues. Multiple Key Servers can be deployed to ensure redundancy, high availability, and fast recovery if one key server fails. Cooperative Key Servers jointly manage the GDOI registrations for the group. That way each Key Server shares the registration load. The GMs can be configured to register with any one of the Key Servers. If more than one KS is configured on a GM, it will register with the first KS. If this KS is unreachable, it will try the following ones.

Although all Key Servers accept registration from GMs, only one KS will be responsible for the rekey operation. This KS is called the Primary KS. The Primary KS is decided through an election process among all the co-operative Key Servers. In order to aid this process a priority number should be configured in each KS. If more than one Key Servers have the same highest priority, then the one with highest IP address will be selected.

Election process will be repeated whenever the existing primary KS goes down. It should be noted that when a new KS joins the group, election process will not be triggered even if the new KS has a higher priority than the existing primary.

Network partition and rejoin: There is a possibility that few Key Servers may lose contact with the remaining key Servers because of network issues. This creates more than one group of Key Servers. When this happens, the separated group which lost the primary KS will initiate re-election process and find a new primary among them. Once the network connectivity is restored, re-election is done again to eliminate the additional primary KS of the separated group. After a rejoin the current SA and key of each primary KS will be distributed to all the GMs so that each GM can decrypt the traffic encrypted by the separated GMs. They keep all the SAs until they expire.

KS Redundancy on GM: More than one KS can be configured on a GM. From the group member perspective, the group member tries to register with the first key server listed in the configuration. If the first key server listed is not reachable, the group member then tries to reach the next key server listed in its configuration. The group member keeps trying this way until it can successfully register with one of the key servers. However, only the primary key server will send further rekeys to the entire network.

COOP Key Server Configuration

Before deploying the COOP configurations, following needs to be considered.

- Generate a named RSA key in one of the Key Server (as required for rekeys) and export it to all the COOP Key Servers.
- Election between the key servers is based on the highest-priority value configured. If they are same, it is based on highest IP address. It is suggested to configure different priorities on all Key Servers.
- Periodic ISAKMP keepalive (Dead Peer Detection (DPD)) needs to be enabled on all the Key Servers so that key Servers can keep track of the state of other Key Servers effectively.
- The GETVPN related configuration should be same on all Key Servers. The KS does not have the capability to verify that the configuration is in sync with other Key Servers.

Below is the additional configuration for enabling co-op KS functionality on a KS.

```
! Enable DPD
crypto isakmp keepalive 15 periodic
!
crypto gdoi group GDOI-GROUP1
server local
 address ipv4 10.0.0.1
 redundancy
  ! The KS with higher priority number is elected as primary
  local priority 250
  peer address ipv4 10.0.6.1
!
```

Generating RSA key for Rekey on COOP Key Servers

This key is used during rekey process. It should be a named RSA key so that it will not take the default Fully Qualified Domain Name (FQDN) of the router. “REKEYRSA” is the name of the RSA key used in the sample configuration and it is generated as exportable. The key is generated on one KS and the same key is imported into other Key Serves.

Execute the below command at the configuration mode on the router console.

```
“crypto key generate rsa modulus 1024 label REKEYRSA exportable”
```

Once the key is generated, it needs to be exported.

Export the RSA key to the router console:

It is a good practice not to save the exported keys anywhere, instead import it to the other routers directly by copy pasting from the console of the first KS. It should be done through a secure computer. If the keys are compromised, the security of the network would be undermined.

Execute the below command at the configuration prompt of the router.

```
crypto key export rsa REKEYRSA pem terminal 3des <pass code>
% Key name: REKEYRSA
  Usage: General Purpose Key
  Key data:
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCuKbSROW7eSqxC+IjB0ipplVkT
...
...
...
NtSRSR51ooWQW5CXRwIDAQAB
-----END PUBLIC KEY-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,B2CE8D823EE52FDC

Zi82W/lX3u0WiHN0ezi6qH5Jeo1baptdqzLlVk2jioAyZabWJqc7+svFY+DJ8rT+
...
...
...
p3dHnQSBaLu1pH3YI9gebQhMgqH6Ie00ucEYVl4/jArzUjifjdCvkQ==
-----END RSA PRIVATE KEY-----
```

Importing RSA key to other Key Servers

Execute the below command on the configuration prompt of the router. “Pass code” is same as the one used to export the key.

```
crypto key import rsa REKEYRSA pem terminal <pass code>
% Enter PEM-formatted public General Purpose key or certificate.
% End with a blank line or "quit" on a line by itself.
<Paste the public key from the output of the key export. Paste
 the hexadecimel information the linesmarkedBEGIN and END.>
quit

% Enter PEM-formatted encrypted private General Purpose key.
```

```
% End with "quit" on a line by itself.
<Paste the private key from the output of the key export. Paste
 the hexadecimel information the linesmarkedBEGIN and END.>
quit
!
```

Repeat the process for all other Key Servers. In the above example export and import are done on route console. Instead of console the key can be exported and imported to a TFTP location also.

Group Member Configuration for Co-op KS
The GM can be configured to register with more than one KS. It will try to register with one of the configured Key Servers. All the Key Servers will be tried in the order of configuration until it successfully registers with one of the Key Servers. The GM will be registered with only one KS at a time. In order to help with registration load balancing, some GMs can be configured to register with one set of Key Servers and some other GMs can be configured with a different set of Key Servers.

```
crypto gdoi group GDOI-GROUP1
 identity number 12345
 server address ipv4 10.0.0.1
 server address ipv4 10.0.6.1
!
```

Key Server Role Change
Availability: 12.4(22)T

There may be a need to change the role of the key server from Primary to Secondary. The Key Server election process can be kicked off by executing ‘clear crypto gdoi ks coop role’ on the current primary KS. If the priority values of the Key Servers have been changed prior to this, a new Primary KS will be selected as per the new priorities. This command will not clear any policy or GDOI sessions. It is purely for the sake of having the current Primary Key Server relinquish its role.

It should be noted that this command will have effect only when executed on the primary key server. Executing it on any other Key Server will not change the role of KS irrespective of the priority value.

Receive only SA Feature
Receive only SA feature is enabled on the Key Server configuration. This enables the SAs to be installed in the inbound direction on all the Group Members. Therefore traffic leaving the GMs will not be encrypted. The GM will decrypt the traffic if it comes encrypted. The incoming traffic will be accepted even if it is not encrypted.

This can be useful when the GETVPN is being enabled on an existing production network. By configuring receive only mode, the deployment can be validated without encrypting traffic. It also helps to deploy the GETVPN on all the potential locations before the encryption is tuned on. Once all the control plane of GETVPN is working satisfactorily and all the GMs are configured with GETVPN, encryption can be enabled by disabling this feature on the Key Server side.

It is also possible to enable encryption selectively on few GMs by executing the exec command *“crypto gdoi gm IPSec direction inbound optional”*. This will force the GM to encrypt the outbound traffic while receiving both encrypted and clear traffic. If all the other GMs are able to decrypt the traffic send by this GM, will serve as an additional proof of configuration working fine.

“crypto gdoi gm IPSec direction …” command overrides the policy temporarily until the next rekey or reboot.

Encryption can be turned on all the devices at the same time by removing the “sa receive-only” command from the KS. This causes an immediate rekey to be sent from the KS changing the direction of the SA on all the GMs.

Receive only SA Configuration
Add the following configuration on Key Server.

```
crypto gdoi group GDOI-GROUP1
 server local
 sa receive-only
!
```

The SA direction can be verified by executing “show crypto gdoi” command on the GM.

```
GM#sh crypto gdoi


GROUP INFORMATION
  Group Name        : GDOI-GROUP1
  Group Identity      : 12345
  Rekeys received     : 4
  IPSec SA Direction    : Inbound Only
```

Passive SA Feature
Availability: 12.4(22)T

This is a Group Member feature which enables the GM to override the receive-only function. Once enabled, the outbound traffic will be encrypted even when receive-only SA is active. The un-encrypted traffic will continue to be accepted as before.

This is feature mainly useful for initial deployment and testing the control plane. This helps to test if the other GMs are able to decrypt encrypted traffic sent by one of the GMs.

Passive SA Configuration
Add the following configuration on GM.

```
crypto gdoi group GDOI-GROUP1
 identity number 12345
 passive
!
```

Fail Close mode
In the basic GETVPN configuration, the traffic passing through group members will be sent in clear until it registers with the KS. This is because the crypto ACL is configured on the KS and GM will get that information only after the registration is successful. This means for a short period of time the traffic can go out unencrypted after a GM is booted up or the existing GETVPN session is cleared manually. This mode is called “fail open” and it is the default behavior. This behavior can be turned off by configuring “Fail Close” mode on the GMs.

If Fail Close feature is configured, all the traffic passing through the GM will be dropped until GM is registered successfully. Once GM registers successfully and SAs are downloaded, this feature turns off by itself. The encryption

will then follow the downloaded ACL. In the case of a re-registration failure the GM will use the last downloaded ACL to handle the traffic. In that case traffic matching the expired IPSec SA is dropped and rest is passed.

If there are critical traffic which needs to be passed in clear (e.g. control/routing traffic), it can be done on the ACL configuration. Typically the ACL used for fail-close is similar to the one configured on the Key Server for the crypto map.

Note

The Fail Close function can also be achieved by configuring an interface ACL. However, the Fail-Close feature is more manageable and is easier to implement.

Fail Close Configuration

```
! Access list for fail-close
ip access-list extended bypass_acl
 ! Traffic which should not be dropped if registration failed
 deny udp any any eq bootps
 deny udp any any eq domain
 ...
!
!Crypto Map
crypto map gdoimap gdoi fail-close
 match address bypass_acl
 ! Configuring "no activate" will disable this feature.
 activate
!
```

To verify whether fail-close mode is activated, use the show crypto map gdoi fail-close command.

Local Exception Policy on GM

In addition to the traffic ACL configured on the KS, a local exception ACL can be configured on the GM. This can be helpful if additional traffic must be excluded from the encryption policy at that specific GM. This method is preferred when the excluded traffic is specific to that GM. By defining local policy on the GM; the size of the policy pushed from the KS is reduced as the ACL can be smaller now.

This configuration is preferred when certain traffic needs to be excluded which is specific to few GMs only. E.g. traffic from a specific subnet to another specific subnet needs to be excluded from encryption.

The crypto ACL applied at the GM represents a concatenation of the downloaded ACL and local ACL. The order of operations is such that the locally defined ACL is checked first, followed by the one downloaded from the KS.

Note: Only deny statements can be added locally at the GM. Permit statements are not supported in the locally configured policies. In case of a conflict, local policy overrides the policy downloaded from the KS.

Local Exception Configuration

Configure an ACL with desired "deny" statements. "permit" statements do not have any effect. Then configure this ACL in the GDOI crypto map.

```
!
```

```
! Exception Access Control List
ip access-list extended exception-acl
 deny  ip 10.32.176.0 0.0.0.255 host 10.32.178.23
 deny  ip 10.32.176.0 0.0.0.255 host 10.32.178.56
!
! Crypto Map
crypto map gdoimap 1 gdoi
 set group GDOI-GROUP1
 match address exception-acl
!
```

VRF–lite Support in Group Member

It is possible to have more than one virtual routing domains in the CE router which is configured as the GM. This is done using the Virtual Routing and Forwarding (VRF) feature. Traffic from each VRF is then routed to service network via separate interfaces or sub-interface. This type of VRF configuration is called VRF-lite.

This type of configuration is required if the CE router needs to be shared by many customers or to separate departments in the same company. Unless configured, the traffic will not be routed between two VRFs. Each VRF maintains its own routing table.

GET VPN can use VRF-lite to connect each VPN segment on the CE to a distinct MPLS VPN or to a shared MPLS VPN on the provider network. Each interface on the group member will need a unique crypto map with a unique GETVPN group identifier. The key server must be accessible through the interface where the crypto map is applied. If the shared MPLS VPN is used, then the IP addresses behind each VRF-lite segment cannot overlap. If a distinct MPLS VPN is used for each VRF, then overlapping IP addresses may be used. A separate key server pair/set is recommended for each of the VRF-lite VPN segments; however, a shared key server may be used as long as each GM identity is uniquely represented in the KS.

Note: Key Server is not VRF aware.

For more information and how to configure VRF-lite based GETVPN, visit the following site.

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/prod_white_paper0900aecd80617171_ps7180_Products_White_Paper.html

GETVPN Status and Diagnostics Commands

This section explains some of the “show” commands and troubleshooting mechanisms of GETVPN solution. Outputs of some of these commands are shown in Appendix B.

Key Server Show Commands

Table 1. Key Server Show Commands

Command	Description
show crypto gdoi	Displays the GETVPN group information
show crypto gdoi ks	Displays basic Key Server status and parameters
show crypto gdoi ks acl	Displays the encryption ACL
show crypto gdoi ks coop	Coop key server status
show crypto gdoi ks members	Displays the group member list

Command	Description
show crypto gdoi ks policy	Displays KEK and TEK policies
show crypto gdoi ks rekey	Displays the rekey status like how many rekeys so far and when the net rekey will happen etc.
show crypto gdoi ks replay	Shows the Time Based Anti-Replay (TBAR) is enabled or not.
show crypto gdoi group <group name> <params>	This command is similar to the ones listed in previous columns but does it based on a specific group. This is particularly useful if there are multiple GETVPN groups configured on the KS.
show crypto isakmp sa	Displays the IKE Security Associations active on the KS. Successful GETVPN IKE sessions will have either GDOI_IDLE or GDOI_REKEY as the status. One GDOI_IDLE session is created between each Coop KS for inter KS communication. There will also be a GDOI_IDLE session between KS and each GM immediately after the GM is registered. It may disappear once the IKE SA life time expires GDOI_REKEY is the rekey SA. Usually there is only one SA exist. If multicast rekey is used, this SA will be between the KS and the multicast address used for rekey. If unicast rekey is used this SA will be between the KS and the last GM which received the rekey SA.

Group Member Show Commands

Table 2. Group Member Show Commands

Command	Description
show crypto gdoi	Basic detail of all the GETVPN groups on GM. This includes the registration status, encryption ACL, KEK policy, TEK policy etc.
show crypto gdoi IPSec sa	Displays an overview of IPSec SAs belonging to all the groups on the GM.
show crypto gdoi gm <options>	Displays brief status of all the configured groups.
show crypto gdoi gm acl	Display the IPSec ACL and local deny ACL. Optional keyword “download” or “local” can be used if only one of the ACL needs to be displayed.
show crypto gdoi gm rekey	Display the rekey details
show crypto gdoi gm replay	Time based Anti Replay information
show crypto gdoi group <group name> <options>	This version of the commands can be used if only the information pertaining one single group needs to be displayed. This is particularly useful if multiple groups are configured on the same GM. The command syntax is same as all the above commands except that “group <group name>” is inserted after “gdoi” keyword.
show crypto IPSec sa	This is a standard IPSec show command. It displays all the IPSec SAs installed on the router including the ones installed by GETVPN.
show crypto isakmp sa	Displays the IKE Security Associations active on the GM. Successful GETVPN IKE sessions will have either GDOI_IDLE or GDOI_REKEY as the status. One GDOI_IDLE session is created between the GM and KS as a result of successful registration. It may disappear once the IKE SA life time expires. This SA is not needed for further operation of the GETVPN. GDOI_REKEY is the rekey SA. Usually there is only one SA active. But the show command may display the old and current SAs. If multicast rekey is used, this SA will be between the KS and the multicast address used for rekey. If unicast rekey is used this SA will be between the KS and the last GM which received the rekey SA.

GETVPN Clear Commands

The “clear” commands are used mainly for diagnostics purpose and also for clearing and kick starting certain events. Below table explains some of the clear commands used in GETVPN.

Table 3. GETVPN Clear commands

Command	Description
clear crypto gdoi	Executing this on KS clears all the existing registrations and causes the GMs to re-register. If executed on GM, the existing SAs are destroyed and the GM re-registers.
clear crypto gdoi group <group name>	Same as above but operates only on the specified group.
clear crypto gdoi ks coop counter	Resets the coop counters on KS if coop feature is enabled. No effect on GM.
clear crypto gdoi ks coop role	If coop feature is enabled on KS, executing this command will trigger a re-election. If a new primary is elected after this forced re-election, it will not take effect unless the command was executed on the existing primary KS. This feature is not available before IOS version 22T
clear crypto gdoi replay	Anti-replay counters are reset.

Command	Description
clear crypto sa	This is a standard IPSec command. This is will clear the IPSec SAs downloaded GETVPN SAs. This will force a re-registration immediately so that existing SAs are downloaded again.
clear crypto isakmp	All IKE SAs including GDOI_REKEY and GDOI_IDLE (registration SA) are deleted. This will not trigger immediate IKE SA negotiation. It will be renegotiated only when needed.

GETVPN Debug Commands

Debug commands are used for advanced trouble shooting. This should be used only when absolutely necessary and by experienced professional. Enabling debugs can adversely affect the performance of a router and not advisable to be enabled on a live router.

Following table lists some of the debug commands related GETVPN.

Table 4. GETVPN Debug Commands

Command	Description
debug crypto gdoi	Basic GDOI debugging.
debug crypto gdoi gm	Basic debugging on a group member
debug crypto gdoi ks	Basic debugging on a Key Server
debug crypto gdoi <options>	Detailed debugging specified by each options like detail, event, rekey etc.
debug crypto gdoi ks <options>	Detailed Ker Server debugging.
debug crypto gdoi gm <options>	Detailed Group Member debugging.
Standard IKE and IPSec debug commands	Since GEVPN leverages standard IPSec code, enabling the standard IKE and IPSec debugging also will provide valuable debug details.

GETVPN Syslog Messages

The router generates various syslog messages to display the status and error states of the GETVPN. This is useful for monitoring the health of GETVPN deployment. Below table lists most of the common syslogs associated with GETVPN. For more updated list refer to Appendix I of the following URL.

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_encrypt_trns_vpn.html

Table 5. GETVPN Syslog

Error Messages	Explanation
COOP_CONFIG_MISMATCH	The configuration between the primary key server and secondary key server are mismatched.
COOP_KS_ADD	A key server has been added to the list of cooperative key servers in a group.
COOP_KS_ELECTION	The local key server has entered the election process in a group.
COOP_KS_REACH	The reachability between the configured cooperative key servers is restored.
COOP_KS_REMOVE	A key server has been removed from the list of cooperative key servers in a group.
COOP_KS_TRANS_TO_PRI	The local key server transitioned to a primary role from being a secondary server in a group.
COOP_KS_UNAUTH	An authorized remote server tried to contact the local key server in a group. Could be considered a hostile event.
COOP_KS_UNREACH	The reachability between the configured cooperative key servers is lost. Could be considered a hostile event.
COOP_KS_VER_MISMATCH	Key servers are running different versions of the IOS code.
COOP_PACKET_DROPPED	Hard limit set on the driver buffer size prevents the sending of packets this size or bigger.
GDOI-3-GM_NO_CRYPTO_ENGINE	No crypto engine is found due to lack of resource or unsupported feature requested.
GDOI_ACL_NUM	The ACL has too many entries. GDOI will honor only the first 100 ACL entries specified.
GDOI_REKEY_FAILURE	During GDOI rekey the payload parsing failed on this group member from the key server.
GM_ACL_MERGE	The ACL differences between a group member and key server are resolved and a merge took place.
GM_ACL_PERMIT	The group member can support only an ACL for "deny." Any traffic matching the "permit" entry will be dropped.

Error Messages	Explanation
GM_CLEAR_REGISTER	The clear crypto gdoi command has been executed by the local group member.
GM_CM_ATTACH	A crypto map has been attached for the local group member.
GM_CM_DETACH	A crypto map has been detached for the local group member.
GM_CONV_SA_DUPLEX	IPSec SAs have been converted to bidirectional mode in a group on a group member.
GM_CONV_SA_DUPLEX_LOCAL	IPSec SAs have been converted to bidirectional mode in a group on a group member by a CLI command.
GM_ENABLE_GDOI_CM	Group member has enabled ACL on a GDOI crypto map in a group with a key server.
GM_HASH_FAIL	During GDOI registration protocol, a message sent by the key server has bad or no hash.
GM_INCOMPLETE_CFG	Registration cannot be completed because the GDOI group configuration may be missing the group ID, server ID, or both.
GM_NO_ IPSEC_FLOWS	Hardware limitation for IPSec flow limit reached. Cannot create any more IPSec SAs.
GM_RE_REGISTER	IPSec SA created for one group may have been expired or cleared. Need to reregister to the key server.
GM_RECV_DELETE	A message sent by the key server to delete the group member has been received.
GM_RECV_REKEY	Rekey received.
GM_REGS_COMPL	Registration complete.
GM_REJECTING_SA_PAYLOAD	During GDOI registration protocol, a proposal sent by the key server was refused by the local group member.
GM_REKEY_NOT_RECD	Group member has not received a rekey message from a key server in a group. Currently unimplemented.
GM_REKEY_TRANS_2_MULTI	Group member has transitioned from using a unicast rekey mechanism to using a multicast mechanism.
GM_REKEY_TRANS_2_UNI	Group member has transitioned from using a multicast rekey mechanism to using a unicast mechanism.
GM_SA_INGRESS	Received-only ACL has been received by a group member from a key server in a group.
GM_UNREGISTER	A group member has left the group.
KS_BAD_ID	Configuration mismatch between a local key server and a group member during GDOI registration protocol.
KS_BLACKHOLE_ACK	Key server has reached a condition of blackholing messages from a group member. Could be considered a hostile event.
KS_CLEAR_REGISTER	The clear crypto gdoi command has been executed by the local key server.
KS_CONV_SAS_DUPLEX	IPSec SAs have been converted to bidirectional mode in a group.
KS_CONV_SAS_INGRESS	IPSec SAs have been converted to receive-only mode in a group.
KS_FIRST_GM, GDOI, LOG_INFO	Local key server has received the first group member joining the group.
KS_GM_REJECTS_SA_PAYLOAD	During GDOI registration protocol, a proposal sent by the key server was refused by the group member.
KS_GM_REVOKED	During rekey protocol, an unauthorized member tried to join a group. Could be considered a hostile event.
KS_GROUP_ADD	A configuration command has been executed to add a key server in a group.
KS_GROUP_DELETE	A configuration command has been executed to remove a key server from a group.
KS_HASH_FAIL	During GDOI registration protocol, a message sent by the group member has bad or no hash.
KS_LAST_GM	Last group member has left the group on the local key server.
KS_NACK_GM_EJECT	Key server has reached a condition of not receiving an ACK message from group member and has been ejected.
KS_NO_RSA_KEYS	RSA keys were not created or they are missing.
KS_REGS_COMPL	Key server has successfully completed a registration in a group.
KS_REKEY_TRANS_2_MULTI	Group has transitioned from using a unicast rekey mechanism to a multicast mechanism.
KS_REKEY_TRANS_2_UNI	Group has transitioned from using a multicast rekey mechanism to using a unicast mechanism.
KS_SEND_MCAST_REKEY	Sending multicast rekey.
KS_SEND_UNICAST_REKEY	Sending unicast rekey.
KS_UNAUTHORIZED	During GDOI registration protocol, an unauthorized member tried to join a group. Could be considered a hostile event.
KS_UNSOL_ACK	Key server has received an unsolicited ACK message from a past group member or is under a DOS attack. Could be considered a hostile event.
PSEUDO_TIME_LARGE	A group member has received a pseudo time with a value that is largely different from its own pseudo time.
REPLAY_FAILED	A group member or key server has failed an anti-replay check.

Error Messages	Explanation
UNAUTHORIZED_IDENTITY	The registration request was dropped because the requesting device was not authorized to join the group.
UNAUTHORIZED_IPADDR	The registration request was dropped because the requesting device was not authorized to join the group.
UNEXPECTED_SIGKEY	Unexpected signature key found: freeing the signature key.
UNREGISTERED_INTERFACE	Receiving registration from unregistered interface. Stop processing it.
UNSUPPORTED_TEK_PROTO	Unexpected TEK protocol.

Migrating to GETVPN

This section provides some insight into how easily an existing network can migrate to a GETVPN enabled network with minimal or no network outage.

GETVPN has different mode of operation to facilitate smooth migration. These modes can be used to test the GETVPN control plane and then smoothly move from a partially encrypted network to a full GETVPN network.

The below table explains the different operational modes of GETVPN.

Table 6. GETVPN Mode of operations

Conformant (Normal) mode	Receiving	Encrypted traffic matching ACL is decrypted.
		Encrypted traffic not matching ACL is dropped if SPI matches else forwarded.
		Clear traffic matching ACL is dropped.
		Clear traffic not matching ACL is forwarded.
	Sending	Traffic matching ACL is encrypted.
		Traffic not matching ACL is forwarded as is.
Receive Only SA mode - Configured on KS and applicable to all GMs registering to this Group	Receiving	Encrypted traffic matching ACL is decrypted.
		Encrypted traffic not matching ACL is dropped if SPI matches else forwarded.
		All Clear traffic is forwarded.
	Sending	All traffic is forwarded as is without encryption.
Passive SA Mode - Configured on individual GM and will override the receive-only option pushed by KS	Receiving	Encrypted traffic matching ACL is decrypted.
		Encrypted traffic not matching ACL is dropped if SPI matches else forwarded.
		All Clear traffic is forwarded.
	Sending	Traffic matching ACL is encrypted.
		Traffic not matching ACL is forwarded as is.

Migration from Clear Text to GETVPN

If carefully planned GETVPN can be deployed in a non-encrypted network with low downtime. This section explains a strategy by which this can be achieved.

Configure the KS: Configure the Key Server with appropriate security policies. Configure ‘receive-only’ mode on the KS so that the GMs will not encrypt the traffic.

Test the control plane: Configure few GMs initially to test the registration and rekey process. Because of receive-only mode the GMs will not encrypt any traffic. Verify if the registration is happening fine and also wait for some rekeys to happen. Validate using show commands, that rekey is happening fine and the GMs are not trying to re-register. Re-registration should happen only if the rekey fails.

Verify the ACL: Make sure important control traffic (routing, TACACS, SSH etc.) is exempted from encryption by adding deny ACEs as the first lines in the ACL.

Test the encryption: Use the Passive SA Mode feature (available 12.4(22)T or later) to enable encryption temporary on a pair of GMs. This will override the Receive-Only mode. But it will continue to accept unencrypted traffic. Now do

a traffic test to make sure that traffic is indeed getting encrypted and decrypted. Same can achieve by using 'gdoi gm ipsec direction inbound optional' cli but this configuration will be override by next 'rekey' or when GM reloads.

Application Testing: GETVPN technology enables network administrators to introduce encryption into the network in a non-intrusive manner. Still it is possible that some applications may be sensitive to the changes encryption is introducing (like Maximum Transfer Unit (MTU) change and fragmentation etc.). So it is a good idea to test the important applications (email, web applications etc.) before enabling GETVPN on the entire network. If there are issues introduce workarounds.

Final deployment: Once all the above steps are completed without problems, then plan for the full deployment.

- Configure COOP KS if redundancy is planned. Test the redundancy by making the primary KS offline. The GMs should get rekey from the new primary KS when the current SA is about to expire. Clear the GDOI session on one GM to see if it gets successfully re-registered with the second KS.
- Configure GETVPN on all the GMs and apply the crypto map. Make sure all the GMs are registered successfully.
- Change the existing ACL on the KS to the desired one to cover the entire traffic to be encrypted. Rekey should immediately go out to all the GMs.
- Remove the receive-only configuration from all the Key Servers, secondary Key Servers first and the primary KS should be the last one.
- Look at the encryption counters and make sure the traffic is encrypted and decrypted as expected. Make sure re-key happens without glitches on all the GMs.

Modifying crypto ACL from Detailed to "permit any any"

It is possible that a GEVPN deployment started with detailed ACL with individual ACE for each subnet to be encrypted. When more sites are added number of ACEs may hit the maximum allowed number. In this case the deployment needs to move to "permit any any" ACL. When such ACL is configured, management traffic and control traffic should be excluded by configuring corresponding denies. If certain branch is not yet GEVPN enabled, traffic to and from that site also should be excluded. The traffic exclusion can also be done using local deny ACL on the GM or even a combination of both local deny and deny ACEs on the crypto ACL on the KS.

In this case it is better to configure a new ACL on the KS instead of modifying the existing one. Once it is time to migrate the ACL name can be just changed on the GETVPN configuration. If the ACL is carefully designed, there is no risk in quickly migrating in this manner.

GETVPN Recommendations and Best Practices

Pre-requisites

- The enterprise network must have full network reachability between the routers configured as key servers and group members.
- Customer Edge (CE) routers are typically configured as GM. So the CE router should have the appropriate crypto hardware installed depending on the platform and the expected amount of traffic.
- If there is a firewall between the GM and the rest of the core network, the firewall policies should be modified appropriately to make sure that GETVPN traffic is passed. They are primarily GDOI (UDP 848) and ESP (IP 50). If it is for the KS, then only GDOI needs to be opened.
- If multicast rekey is to be used, the core network should have multicast routing enabled.
- Necessary network services like PKI Certificate server, NTP and other management servers must be reachable by all the GMs and KS. Preferably host them on a separate subnet so that it can be easily excluded from encryption ACL.

Authentication Policy for GM Registration

GMs can authenticate to the KS at the time of registration using pre-shared keys or PKI. Pre-shared keys are easy to configure but must be managed proactively. It is recommended to deploy a pre-shared key per peer instead of defining a common key shared by all the devices in the network. The pre-shared keys should be regularly updated (every few months) for added security.

PKI based authentication uses RSA key pair and digital certificates. This eliminates the regular key management difficulty. RSA keys need not to be reconfigured often and digital certificates are unique to each device. Therefore PKI is considered more secure compared to pre-shared key based authentication.

Unicast Rekey vs. Multicast Rekey

GETVPN supports both unicast and multicast based rekey. Unicast method uses one-to-one communication between primary KS and the GMs. GM acknowledges the rekey receipt. So the status of each GM is known at the KS. In multicast method the primary KS multicasts the rekey information to the multicast address configured and GMs listen to that group address and accept the rekey. KS will retransmit the 'rekey' the number of times its configured for. KS does not keep track of GMs on individual basis. Unicast method is easier to configure and trouble shoot but when number of GMs increase the rekey load on KS also increases. In the case of multicast the rekey load does not increase proportional to the number of GMs.

Multicast Configuration Guidelines

It is recommended to configure all multicast participating interfaces on the GMs, including Loopback and private VLAN interfaces in sparse mode. Sparse mode avoids flooding multicast traffic to all parts of the network and allows only multicast control and data traffic to parts of the network with registered groups.

Life time Considerations

Different components of GETVPN use different life times. It is important to configure appropriate life time in relation to each other.

IKE Lifetime: IKE is used for both KS to KS (coop KS) communication and GM to KS registration. KS to KS IKE session needs to be up always so a larger life time is preferred for this on KS as it will reduce frequent IKE renegotiations. GM to KS IKE session is used only for the registration. Rekeys do not use it. So after a successful registration, the IKE session does not have any use. A small IKE lifetime on GM will cause the IKE session to expire faster and free up some resources on GM and KS.

Note: Changing IKE credentials such as revoking a certificate or changing pre-shared key after the GM registered will be effective only during the next re-registration which will happen in the event of a missed Rekey or executing 'clear crypto gdoi'.

The recommended values for IKE on GM and KS are 300 seconds and 24 hours respectively.

```
! GM Configuration
crypto isakmp policy 1
 lifetime 300
!
! On KS
crypto isakmp policy 1
 lifetime 86400
!
```

TEK Lifetime: The recommended value of TEK lifetime is two hours. Shorter life times will cause frequent rekeys. Larger life time can be used if the overall traffic rate on the network is less.

```
crypto IPSec profile profile1
 set security-association lifetime seconds 7200
!
```

KEK Lifetime: It is recommended to have the KEK lifetime at least three times of the TEK lifetime. So if TEK lifetime is two hours, a KEK lifetime of six hours or higher can be used.

```
crypto gdoi group GDOI-GROUP1
 server local
 rekey lifetime seconds 86400
!
```

Fragmentation Considerations

Pre-fragmentation: Encryption typically increases the IP packet size. If the original packet is large enough, it may need to be fragmented as a result of that. The default behavior of Cisco IOS router is fragment the large packets before encryption instead of doing it afterwards. This method is called pre-fragmentation. The fragments will be re-assembled by end host instead of the decrypting router. This improves the decryption performance on the router.

TCP MSS value: It is also recommended to configure a reduced Maximum Segment Size (MSS) value for TCP traffic. This way TCP flows will not generate larger IP packets which can get fragmented during encryption. This can be achieved by configuring “ip tcp adjust-mss 1360” on the interface connecting to the corporate network. The value 1360 assumes the MTU of the core network is 1500. An MSS value of 1360 will ensure that the resulting IP packet on the LAN segment is less than 1400 bytes thereby providing 100 bytes for any overhead. Modify the MSS value appropriately for other MTU sizes.

It is a good practice to ensure that all the routers on the core network support the same MTU.

DF bit processing: Some applications may set the Do not Fragment (DF) bit so that the packets don’t get fragmented by intermediate routers. When the router encounters a packet which needs to be fragmented before forwarding, it will just drop the packet if DF bit is set on that packet. Router will also send an ICMP notification back to the source address of that packet. By default GM copies the DF bit from the original packet to the new encrypted packet. If there is an intermediate router which has a smaller MTU than the GM, it may drop the packet if the DF bit is set. To avoid this GM can be configured to clear the DF bit after encryption, so that the intermediate router can fragment the encrypted packet if needed. The destination GM will take care of assembling the packet before decryption. Configure *“crypto ipsec df-bit clear”* to achieve this.

Note: In pre-fragmentation, the GM may fragment the packet with DF bit set if needed if *“crypto ipsec df-bit clear”* is configured. In some IOS releases the DF bit of the original packet may not be cleared during fragmentation. Some networking devices like firewall which is connected beyond the receiving side GM may treat this as an anomaly when it it sees fragments with DF bit set.

Path MTU Discovery (PMTUD): The ICMP Fragmentation notification traffic needs to be excluded in the encryption policy for the PMTUD to work. Otherwise GM will drop the notification if any of the core routers send it back to the traffic originator. Even then the traffic originator may not be able to calculate the path MTU accurately. This is because the reported MTU does not account for the encryption overhead caused by GM.

You may need to include the following deny ACEs in the Global ACL in KSs or Local ACL in GMs to ICMP Fragmentation notification to reach the end host.

```
deny icmp any any unreachable
deny icmp any any time-exceeded
```

GETVPN on Multiple Interfaces

If a GM has more than one physical interfaces connecting to the MPLS network for fail-over or load balancing purposes, same GETVPN crypto map can be applied on both interfaces. In that case it is recommended to configure a loopback interface and communication between GM and KS uses that IP address. This way rekeys can be received through any physical interface. Otherwise, GM will be forced to re-register, once primary interface goes down and traffic gets forwarded through second interface. The following configuration needs to be added force a specific interface to be used for crypto identity.

```
crypto map <getvpn crypto map> local-address <interface>
```

Other Considerations

- Registration load on the KS can be reduced by distributing it among the coop Key Servers. This can be achieved by changing the order of the Key Servers in the Group Member configuration. GM attempts to register with the first KS configured. So by appropriately shuffling this order on each GM, a proper load balance can be achieved. Maximum Key Servers supported by GETVPN is currently eight.
- There is a maximum of 100 ACEs is supported by the crypto ACL configured per group on the KS including deny statements. So care should be taken to cover the entire address space using fewer lines. Use of symmetric ACEs (eg. 'permit ip any any' or 'permit ip 10/8 10/8') can simplify the ACL even more since traffic in both direction will be covered by single line.
- It is better to install the KSs in separate locations so that the GMs can reach the remaining Key Servers if the connection to one or more of the KS sites failed. Also choose the sites with more reliable connectivity and better bandwidth to install the Key Servers. The KS should have physically diverse paths through which the COOP protocol can be maintained. The backup path between the KS does not need to support high volume data plane loads – only KS COOP traffic loads.
- Host the management systems (like Certificate Server, Network Management tool, NTP server etc.) in a separate address space so that it is easier to exclude them in the encryption ACL.
- Increasing the buffer size and interface queues may improve the coop KS feature.

```
  buffers huge size 64000
  interface <outside>
  ! Interface connecting to the other Key Servers
  hold-queue 4096 in
  hold-queue 4096 out
!
```

- Network Address Translation (NAT) is not supported by GETVPN. NAT must be performed before encryption or after decryption when GET is used.
- End to end PMTU does not work in GETVPN.
- Port range is not supported in the crypto ACL.
- Key servers support ACL that are compliant with RFC 4301. The KS can only contain source IP address, destination IP address, source port, destination port, and protocol. All other options are unsupported.

- If the crypto ACL is modified when the GETVPN session is already established, it will cause a rekey. Rekey will happen only when the ACL modification is complete and user exits the configuration mode. Only exception is when the scheduled rekey happens when the user is still in the process of modifying the ACL. In that case the partially modified ACL will be sent to the GMS during this rekey.
- The coop Key Servers should have the same IOS version and the same GETVPN configuration. Beginning with 22T, the KS and GM may use a longer registration window that is automatically calculated based on the TEK lifetime. The recommendation is to upgrade the KS first followed by upgrades to the GM. This insures that the GM's are not repeatedly re-registering to a KS that has not yet created a new TEK according to the GM's assumed larger registration window.
- When a policy on the KS needs to be modified, it is better to modify it on the secondary Key Servers first and do the primary KS as last.
- ASR release 3 supports only static RP method for multicast rekeying.

Rekey Triggering

The following policy changes on the GDOI group configuration on Key Server will trigger an immediate re-keying even if the current SA is still valid.

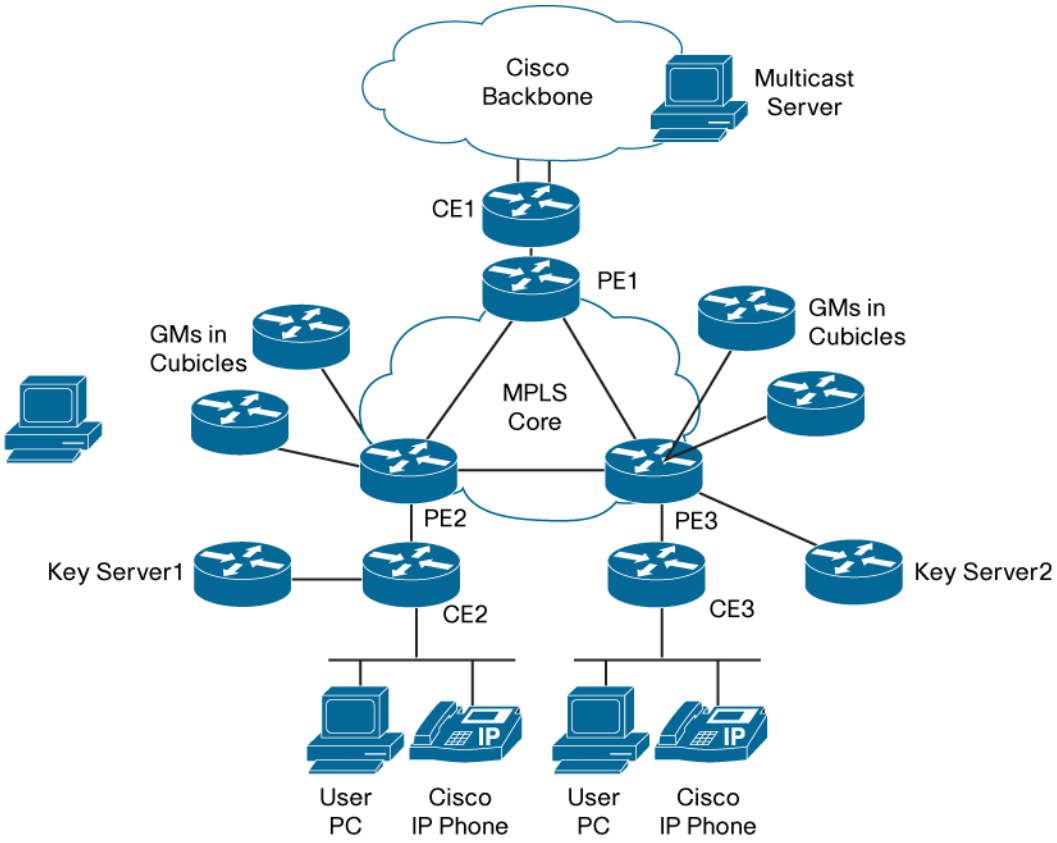
- Modifying crypto ACL.
- Modifying IPSec transform set.
- Changing the rekey method (unicast to multicast or vice versa).
- Changing rekey multicast address (if multi cast rekeying is used).
- Enabling RSA based rekey-authentication.
- Changing the RSA key used for rekey authentication.
- Changing the rekey encryption algorithm used.
- Changing the configuration to use a different crypto profile.
- Enabling/disabling the replay detection.

Note: If TBAR is enabled, the Key Server will send pseudotime sync updates to Group Members every 2 hours (7200 seconds) over a rekey packet. So, if your TEK lifetime is configured to be greater than 2 hours, you will see rekey packets every 2 hours, which will have the pseudotime sync updates.

References

1. CISCO IOS GETVPN start page: http://www.cisco.com/go/getvpn
2. GETVPN Design and Implementation Guide: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6525/ps9370/ps7180/GETVPN_DIG_version_1_0_External.pdf
3. Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4: http://www.cisco.com/en/US/customer/products/ps6350/products_installation_and_configuration_guides_list.html
4. Cisco IOS Configuration Fundamentals Command Reference, Release 12.4T: http://www.cisco.com/en/US/customer/products/ps6441/prod_command_reference_list.html
5. Cisco IOS Security Configuration Guide, Release 12.4: http://www.cisco.com/en/US/customer/products/ps6350/products_installation_and_configuration_guides_list.html
6. GETVPN Configuration Guide: http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_encrypt_trns_vpn.html
7. GDOI RFC: http://www.ietf.org/rfc/rfc3547.txt

Appendix A: Sample Configuration



Key Server 1

```
!
upgrade fpd auto
version 12.4
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
service internal
!
hostname sample-ks1
!
!
logging message-counter syslog
logging queue-limit 100
logging buffered 65555
enable secret 5 <removed>.
!
aaa new-model
```

```
!
!
aaa session-id common
clock timezone pst -8
clock summer-time PDT recurring
ip source-route
ip cef
!
ip domain name mydomain.com
ip host tftp-server <removed>
ip host my-ca <removed>
ip name-server <removed>
ip name-server <removed>
ip multicast-routing
no ipv6 cef
!
crypto pki trustpoint my-ca
 enrollment mode ra
 enrollment url <url>
 serial-number
 revocation-check crl
 auto-enroll
!
crypto pki certificate chain my-ca
 certificate <removed>
 30820468 30820350 A0030201 02020A53 9331FB00 00000004 39300D06 092A8648
 certificate ca <removed>
 30820436 3082031E A0030201 02021072 7973B81B EA4AA142 1ABE701F
memory-size iomem 0
!
crypto isakmp policy 1
 encr aes
 group 2
!
!
crypto isakmp keepalive 15 periodic
!
```

```
crypto IPSec transform-set aes128 esp-aes esp-sha-hmac
!
crypto IPSec profile profile1
 set security-association lifetime seconds 7200
 set transform-set aes128
!
!This config is specific to GETVPN
crypto gdoi group gdoi-group1
 identity number 1357924680
 server local
 rekey algorithm aes 128
 rekey address ipv4 rekey-multicast-group
 rekey lifetime seconds 28800
 rekey retransmit 10 number 3
 rekey authentication mypubkey rsa rekeyrsa
 ! remove the below line for multicast rekeying
 rekey transport unicast
 sa IPSec 1
  profile profile1
  match address ipv4 getvpn-acl
  replay time window-size 5
 address ipv4 10.32.178.56
 redundancy
  local priority 191
  peer address ipv4 10.32.178.23
  peer address ipv4 10.32.178.57
!
!
interface Loopback0
 ip address 10.32.178.56 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet0/1
 ip address 10.32.178.54 255.255.255.252
 ip pim sparse-mode
 duplex full
 speed 1000
```

```
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
router bgp 65002
 bgp log-neighbor-changes
 neighbor 10.32.178.53 remote-as 65001
 !
 address-family ipv4
 neighbor 10.32.178.53 activate
 no auto-summary
 no synchronization
 network 10.32.178.56 mask 255.255.255.255
 exit-address-family
 !
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.32.178.53
no ip http server
ip http secure-server
ip pim ssm range 1
! Multicast group ACL !
ip access-list extended rekey-multicast-group
```

```
permit ip any host 239.192.1.190
!! Group ACL to send all GMs !!
ip access-list extended getvpn-acl
 deny udp any eq 848 any eq 848
 deny ip any 224.0.0.0 0.255.255.255
 deny pim any host 224.0.0.13
 deny tcp any any eq ssh
 deny tcp any eq ssh any
 deny tcp any any eq tacacs
 deny tcp any eq tacacs any
 deny tcp any any eq bgp
 deny tcp any eq bgp any
 deny ospf any any
 deny eigrp any any
 deny udp any any eq ntp
 deny udp any any eq snmp
 deny udp any eq snmp any
 deny udp any any eq snmp-trap
 deny udp any any eq syslog
 ! Encrypt all the rest of the traffic
 permit ip any any
!
logging alarm informational
access-list 1 permit 239.192.0.0 0.0.255.255
!
!
control-plane
!
mgcp fax t38 ecm
!
dial-peer cor custom
!
line con 0
 exec-timeout 0 0
 stopbits 1
```

```
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
line vty 5 15
 exec-timeout 0 0
 transport input ssh
 transport output all
line vty 16 1869
!
exception data-corruption buffer truncate
ntp server <removed>
ntp server <removed>
end
```

Key Server 2

The configuration is similar to the above (Key server-1). The major difference is in coop configuration which is written below.

```
! This configuration is specific to GETVPN!
crypto gdoi group gdoi-group1
 identity number 1357924680
 server local
 rekey algorithm aes 128
 ! Below line is igmored if unicast rekey is configured
 rekey address ipv4 rekey-multicast-group
 rekey lifetime seconds 28800
 rekey retransmit 10 number 3
 rekey authentication mypubkey rsa rekeyrsa
 ! Remove below line for multicast rekeying
 rekey transport unicast
 sa IPSec 1
  profile profile1
  match address ipv4 getvpn-acl
  replay time window-size 5
 address ipv4 10.32.178.23
 redundancy
  local priority 131
  ! Other Key Servers
```

```
  peer address ipv4 10.32.178.56
  peer address ipv4 10.32.178.57
!
```

GM Configuration

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname getvpn-gm
!
boot-start-marker
boot system flash c880data-universalk9-mz.124-22.T
boot-end-marker
!
logging message-counter syslog
logging buffered 4096
!
aaa new-model
!
!
aaa authentication login default local
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PST recurring
!
crypto pki trustpoint my-ca
 enrollment mode ra
 enrollment url <enrollment url>
 serial-number
 ip-address none
 revocation-check crl
 auto-enroll
!
crypto pki certificate chain my-ca
```

```
 certificate <removed>
certificate ca <removed>

ip source-route
!
ip cef
no ip domain lookup
ip domain name mydomain.com
ip host tftp-server <removed>
ip host my-ca <removed>
ip name-server <removed>
ip multicast-routing
ip inspect name test tcp
ip inspect name test udp
ip igmp ssm-map enable
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
license boot module c880-data level advipservices
!
!
!
crypto isakmp policy 1
 encr aes
 group 2
 lifetime 300
!
!
crypto IPSec transform-set t1 esp-3des esp-sha-hmac
!
crypto IPSec profile sec-profile
 set transform-set t1
!
crypto gdoi group gdoi-group1
 identity number 1357924680
```

```
 server address ipv4 10.32.178.56
 server address ipv4 10.32.178.23
 server address ipv4 10.32.178.57
!
!
crypto map getvpn_map 1 gdoi
 set group gdoi-group1
 match address CSM_GET_GM_CRYPTO_ACL_1
!
archive
 log config
 hidekeys
!
interface FastEthernet0
 switchport access vlan 10
!
interface FastEthernet1
 switchport access vlan 10
!
interface FastEthernet2
 switchport access vlan 10
!
interface FastEthernet3
 switchport access vlan 10
!
interface FastEthernet4
 description outside interface
 ip address 10.32.178.42 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 crypto map getvpn_map
!
interface Vlan1
 no ip address
 shutdown
!
```

```
interface Vlan10
 ip address 10.32.176.25 255.255.255.248
 ip tcp adjust-mss 1360
 ip pim sparse-mode
 ip igmp join-group 239.192.1.190 source 10.32.178.57
 ip igmp join-group 239.192.1.190 source 10.32.178.56
 ip igmp join-group 239.192.1.190 source 10.32.178.23
 no autostate
!
router eigrp 100
 network 10.32.176.32 0.0.0.7
 network 64.0.0.0 0.0.0.255
 no auto-summary
!
router bgp 65002
 bgp router-id 10.32.178.42
 bgp log-neighbor-changes
 neighbor 10.32.178.41 remote-as 65001
 !
 address-family ipv4
 neighbor 10.32.178.41 activate
 no auto-summary
 no synchronization
 network 10.32.176.24 mask 255.255.255.248
 exit-address-family
!
ip forward-protocol nd
no ip http server
ip http secure-server
!
ip pim ssm range 1
!
ip access-list extended CSM_GET_GM_CRYPTO_ACL_1
 deny  ip 10.32.176.0 0.0.0.255 host 10.32.178.23
 deny  ip 10.32.176.0 0.0.0.255 host 10.32.178.56
 deny  ip 10.32.176.0 0.0.0.255 host 10.32.178.57
 deny  ip any host 239.192.1.190
```

```
access-list 1 permit 239.192.0.0 0.0.255.255
no cdp log mismatch duplex
!
line con 0
 exec-timeout 0 0
 no modem enable
line aux 0
line vty 0 4
 exec-timeout 0 0
!
scheduler max-task-time 5000
ntp server <IP address of NTP server>
ntp server <IP address of NTP server>
end
```

Appendix B: Basic GETVPN Show Commands

The following sections list the sample output of some of the common GETVPN show commands. The output is based on Cisco IOS 12.4(15)T8 version. The output may vary depending on the release.

show crypto isakmp sa

This command displays the active ISAKMP sessions on the router and is common for standard IPSec and GEVPN. Below output is from a Primary Key Server using unicast rekey method. The ISAKMP SAs with 'GDOI_IDLE' status are created as result of GMs registrations and between other COOP servers.

The SA labeled "GDOI_REKEY" is used for rekeying. The output will show the SA pointing to the last GM to which the rekey was sent. In multicast rekey method, the output will be similar except that the destination address will be the multicast group address used for rekeying.

```
#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst       src       state     conn-id status
10.32.178.56  10.32.178.9   GDOI_IDLE     1069 ACTIVE
10.32.178.46  10.32.178.56  GDOI_REKEY      0 ACTIVE
10.32.178.56  10.32.178.106  GDOI_IDLE     1067 ACTIVE
10.32.178.23  10.32.178.56  GDOI_IDLE     1062 ACTIVE
10.32.178.56  10.32.178.30  GDOI_IDLE     1068 ACTIVE
10.32.178.57  10.32.178.56  GDOI_IDLE     1061 ACTIVE
#
```

The same command executed on a GM will give the following output.

```
#show cry isakmp sa
IPv4 Crypto ISAKMP SA
```

```
dst       src       state     conn-id status
10.32.178.42  10.32.178.56  GDOI_REKEY    2302 ACTIVE
10.32.178.56  10.32.178.42  GDOI_IDLE     2301 ACTIVE
#
```

It should be noted that the GDOI_IDLE SAs between the GMs and KS will eventually time out once the SA life time is over. This is because the SAs are no more needed after the registration is over. It will get created again when GM re-registers in the event of missing rekey or executing 'clear crypto gdoi'

show crypto gdoi

This command displays the all basic details about the GETVPN status. The output is different for Key Server and Group Member.

On Key Server:

```
#show crypto gdoi
GROUP INFORMATION

  Group Name        : gdoi-group1 (Unicast)
  Group Identity      : 1357924680
  Group Members      : 9
  IPSec SA Direction    : Both
  Active Group Server   : Local
  Redundancy        : Configured
    Local Address    : 10.32.178.56
    Local Priority    : 30
    Local KS Status   : Alive
    Local KS Role    : Primary
  Group Rekey Lifetime   : 14400 secs
  Group Rekey
    Remaining Lifetime  : 14386 secs
  Rekey Retransmit Period : 10 secs
  Rekey Retransmit Attempts: 3
  Group Retransmit
    Remaining Lifetime  : 6 secs

   IPSec SA Number    : 1
   IPSec SA Rekey Lifetime: 7200 secs
   Profile Name      : profile1
   Replay method     : Disabled
   SA Rekey
```

```
     Remaining Lifetime : 886 secs
    ACL Configured     : access-list getvpn-acll

  Group Server list    : Local

#
```

On Group Member:

```
# show crypto gdoi
GROUP INFORMATION

  Group Name        : gdoi-group1
  Group Identity      : 1357924680
  Rekeys received     : 636
  IPSec SA Direction    : Both
  Active Group Server   : 10.32.178.56
  Group Server list    : 10.32.178.56
                10.32.178.23

  GM Reregisters in    : 745 secs
  Rekey Received(hh:mm:ss) : 00:01:45
  Rekeys received
     Cumulative     : 636
     After registration : 636
  Rekey Acks sent     : 20

 ACL Downloaded From KS 10.32.178.56:
  access-list deny udp any port = 848 any port = 848
  access-list deny ip any 224.0.0.0 0.255.255.255
  access-list deny pim any host 224.0.0.13
  access-list deny igmp any any
  access-list deny tcp any any port = 23
  access-list deny tcp any port = 23 any
  access-list deny tcp any port = 179 any
  access-list deny tcp any any port = 179
< removed rest of the output >
```

show crypto gdoi ks coop

This command is executed on Key Server to display the coop status.

```
#show crypto gdoi ks coop
Crypto Gdoi Group Name :gdoi-group1
    Group handle: 2147483650, Local Key Server handle: 2147483650
    Local Address: 10.32.178.56
    Local Priority: 30
    Local KS Role: Primary  , Local KS Status: Alive
    Primary Timers:
        Primary Refresh Policy Time: 20
        Remaining Time: 1
        Antireplay Sequence Number: 2335
    Peer Sessions:
    Session 1:
        Server handle: 2147483651
        Peer Address: 10.32.178.23
        Peer Priority: 5
        Peer KS Role: Secondary , Peer KS Status: Alive
        Antireplay Sequence Number: 7
        IKE status: Established
        Counters:
          Ann msgs sent: 2316
          Ann msgs sent with reply request: 2
          Ann msgs recv: 20
          Ann msgs recv with reply request: 3
          Packet sent drops: 15
          Packet Recv drops: 0
          Total bytes sent: 1526361
          Total bytes recv: 14389
    Session 2:
        Server handle: 2147483652
        Peer Address: 10.32.178.57
        Peer Priority: 3
        Peer KS Role: Secondary , Peer KS Status: Alive
        Antireplay Sequence Number: 32
        IKE status: Established
        Counters:
```

```
          Ann msgs sent: 2328
          Ann msgs sent with reply request: 4
          Ann msgs recv: 6
          Ann msgs recv with reply request: 2
          Packet sent drops: 0
          Packet Recv drops: 0
          Total bytes sent: 1534928
          Total bytes recv: 4368
#
```

show crypto gdoi ks policy

The following command will show the basic Key Server policy information.

```
#show crypto gdoi ks policy
Key Server Policy:
For group gdoi-group1 (handle: 2147483650) server 10.32.178.23 (handle: 2147483650):
 # of teks : 1 Seq num : 17
 KEK POLICY (transport type : Unicast)
  spi : 0x21B28B73C4CDCB2CC08403E2B5AA73DD
  management alg   : disabled  encrypt alg    : AES
  crypto iv length  : 16     key size     : 32
  orig life(sec): 14400    remaining life(sec): 2141
  sig hash algorithm : enabled   sig key length  : 162
  sig size      : 128
  sig key name    : rekeyrsa

 TEK POLICY (encaps : ENCAPS_TUNNEL)
  spi        : 0x3EDAD60  access-list      : getvpn-acl
  # of transforms  : 0       transform       : ESP_AES
  hmac alg      : HMAC_AUTH_SHA
  alg key size    : 32      sig key size     : 20
  orig life(sec)   : 7200      remaining life(sec)  : 142
  tek life(sec)   : 7200      elapsed time(sec)   : 758
  antireplay window size: 0
For group gdoi-group1 (handle: 2147483650) server 10.32.178.56 (handle: 2147483651):
For group gdoi-group1 (handle: 2147483650) server 10.32.178.57 (handle: 2147483652):
#
```

show crypto ipsec sa

This command will display details about the IPSec SAs active on the router. This is a common command for standared IPSec and GETVPN.

```
#show crypto ipsec sa
   PFS (Y/N): N, DH group: none
   PFS (Y/N): N, DH group: none


interface: FastEthernet4
  Crypto map tag: gdoi, local addr 10.32.178.30
  protected vrf: (none)
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 0.0.0.0 port 848
   PERMIT, flags={origin_is_acl,}
  #pkts encaps: 2545931, #pkts encrypt: 2545931, #pkts digest: 2545931
  #pkts decaps: 1899496, #pkts decrypt: 1899496, #pkts verify: 1899496
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0
   local crypto endpt.: 10.32.178.30, remote crypto endpt.: 0.0.0.0
   path mtu 1200, ip mtu 1200, ip mtu idb FastEthernet4
   current outbound spi: 0x5AE90201(1525219841)
   inbound esp sas:
   spi: 0x5AE90201(1525219841)
    transform: esp-256-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 31, flow_id: Motorola SEC 2.0:31, sibling_flags 80000040, crypto map:
gdoi
< removed rest of the output>
#
```

Appendix C: Abbreviations and Acronyms

The following table lists some of the common abbreviations and acronyms which may have been used in this document.

Abbreviation or Acronym	Expansion
3DES	Triple Data Encryption Standard (DES)
AAA	authentication
ACL	access control list
AES	Advanced Encryption Standard
CE	customer edge (device)
CLI	command line interface
CM	Central Manager
COOP	Cooperative (Protocol)
CPE	customer premises equipment
DC	data center
DHCP	Dynamic Host Configuration Protocol
DMVPN	Dynamic Multipoint VPN
DPD	dead peer detection
DSCP	Differentiated Services Code Point
DSL	digital subscriber line
DSLAM	digital subscriber line access multiplexer
FIB	Forwarding Information Base
FWSM	Firewall Switching Module (6500/7600)
GDOI	Group Domain Of Interpretation
GETVPN	Group Encrypted Transport VPN
GM	group member
GRE	Generic Routing Encapsulation
GUI	graphical user interface
HA	high availability
HSRP	Hot Standby Router Protocol
ICMP	Internet Control Messaging Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP security
ISP	Internet service provider
KEK	key encryption key
KS	key server
L2TP	Layer 2 Tunneling Protocol
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
MSDP	Multicast Source Discovery Protocol
MTU	maximum transmission unit
NAT	network address translation
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PE	provider edge
PfR	performance routing

Abbreviation or Acronym	Expansion
PKI	public key infrastructure
PSK	pre-shared keys
QoS	quality of service
SA	security association (IPSec)
SADB	security association database
SLB	server load balancing
SNMP	Simple Network Management Protocol
SP	service provider
TBAR	time-based anti-replay
TEK	traffic encryption key
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VIP	virtual IP address
VLAN	virtual local area network
VoIP	voice over IP
VPN	virtual private network
VRF	virtual routing and forwarding
VSA	VPN Services Adapter (7200)
VTI	Virtual Tunnel Interface
WAAS	Wide Area Application Services

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.

Printed in USA C07-554713-03 03/16