Cisco ECT-Based Group Encrypted Transport VPN

Introduction

The Cisco IOS® Software-based Group Encrypted Transport Virtual Private Network (Cisco IOS GET VPN) is a tunnel-less technology that provides end-to-end security for voice, video, and data in a native mode for a fully meshed network. It uses the core network's ability to route and replicate the packets between various sites within the enterprise. Cisco IOS GET VPN preserves the original source and destination addresses in the encryption header for optimal routing; hence, it is largely suited for an enterprise running over a private Multiprotocol Label Switching (MPLS)/IP-based core network. Cisco IOS GET VPN uses Group Domain of Interpretation (GDOI) as the keying protocol for encrypting and decrypting the data packets.

The Cisco® Enterprise-Class Teleworker (ECT) solution is a highly scalable Cisco IOS Software-based solution that securely integrates the network infrastructure, management infrastructure, managed services, and applications across the entire enterprise, including LAN, WAN, branch, and teleworker locations.

The solution is an integral part of the Cisco Service-Oriented Network Architecture (SONA), a framework that enables enterprise customers to build integrated systems across a fully converged, intelligent network. Using the Cisco SONA framework, the enterprise network can evolve into an Intelligent Information Network—one that offers the kind of end-to-end functions and centralized, unified control that promote true business transparency and agility.

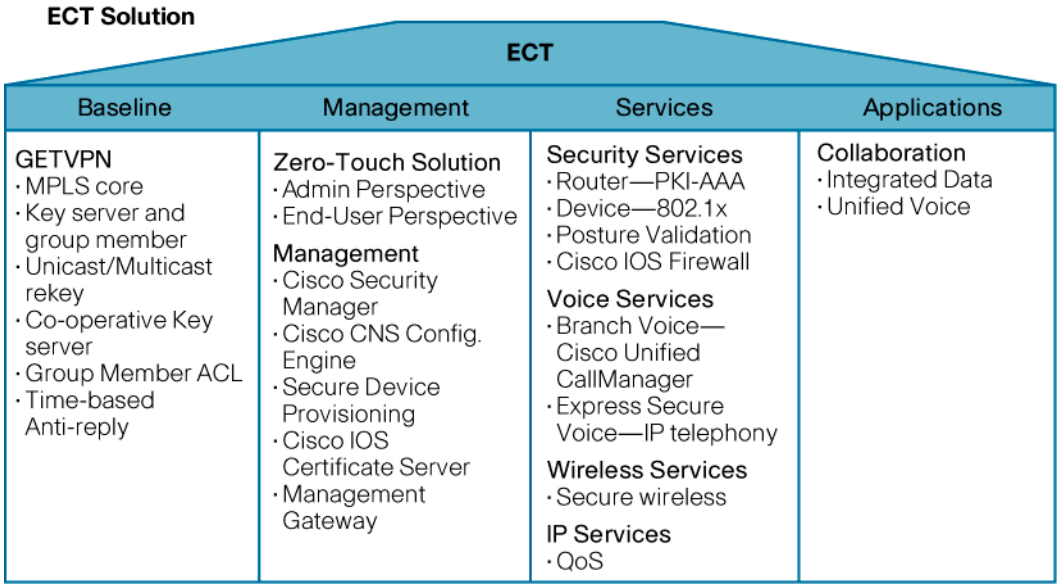
Cisco has successfully deployed the ECT solution within its own organization, increasing productivity and improving efficiency while enabling "zero-touch" deployment, manageability, and low-to-negative total cost of ownership (TCO). Enterprises and service providers can use the Cisco ECT solution to offer the benefits of network services to their end users and customers, while maintaining an effective ROI.

For the Cisco ECT/SONA Solution Overview, visit http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/prod_brochure0900aecd803fc7ec.html.

For Cisco ECT/SONA solution, services and applications support, visit http://cisco.com/go/ect/.

This deployment guide covers the integration of Cisco IOS GET VPN within the Cisco ECT/SONA framework. The ECT 'teleworker' is broadly viewed as the remote branch office for this purpose. Cisco IOS GET VPN is the baseline solution (Figure 1), interconnecting remote branch offices to the corporate network using private MPLS core along with manageability, applications, and services enabled by Cisco ECT.

Figure 1. Cisco ECT Solution Overview



Document Scope

This document provides deployment guidelines to enable Cisco IOS GET VPN in an enterprise network. This document does not cover in-depth technical details about various features comprising Cisco IOS GET VPN. Please refer to the References section for more details.

Why GET VPN?

Enterprise customers face numerous security challenges based on their network application and connectivity requirements. Though MPLS VPNs can provide a certain level of security, many critical applications need end-to-end encryption as well. Some solutions involving Dynamic Multipoint Virtual Private Network (DMVPN) or Enhanced Easy VPN can be used to achieve end-to-end encryption, but these are basically an overlay “hub-and-spoke” model. This could introduce sub-optimal routing even for a fully meshed deployed network using MPLS, delay setting up a full mesh of connections among all sites, and result in sub-optimal support for multicast causing scaling limitations and provisioning and troubleshooting overheads.

An alternative to the overlay model is to deploy virtual routing and forwarding (VRF)-aware IP security (IPsec) on provider edge (PE) routers. Here, the traffic is encrypted only between customer edge (CE) and provider edge routers. The traffic is not encrypted between provider edge routers, but is secured using MPLS labels. This has an additional overhead for provider edge routers, requiring them to decrypt the traffic before forwarding it to the core, and to encrypt the traffic before forwarding it to customer edge routers.

Cisco IOS GET VPN is a group key-based solution that provides end-to-end security for both unicast and multicast applications. Cisco IOS GET VPN is enabled in customer edge routers without using tunnels; it is a better solution than the overlay and VRF-aware IPsec solutions.

The GDOI protocol is the foundation for Cisco IOS GET VPN. GDOI is documented in RFC3547. For more information, visit http://www.ietf.org/rfc/rfc3547.txt.

For detailed information on Cisco IOS GET VPN architecture and features, visit http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008078e4f9.html.

Cisco IOS GET VPN Benefits

- Tunnel-less encryption solution

- Uses the underlying routing infrastructure
- Centralized management of policies and keys in the key server
- End-to-end security for voice, video, and data
- Any-to-any enterprise connectivity for critical applications
- Optimal routing by preserving source and destination addresses in the encryption header
- Flexibility to use unicast or multicast rekey mechanisms based on the core network support
- Multicast encryption in native mode
- Uses (requires) multicast replication in the MPLS/IP core, removing the need for a group member to replicate multiple copies for each receiver (such as a hub in a hub-and-spoke tunneled network)
- Less overhead in PE routers; they do not need to decrypt/encrypt traffic
- Efficient distribution of rekeys using multicast transport
- Zero-touch provisioning in key server for addition of new group members if planned addressing schemes are in place
- Redundancy in key server failure by using cooperative key server feature
- Prevention of replay attacks
- Selective bypass of encryption using group member ACL
- Scalable security solution for large-scale networks

Deployment Considerations

Network Addressing

It is recommended to use subnets of a single major network for the inside interfaces of all group members. This way, a simple policy can be defined in the key server, for example: ‘permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255’. This helps the group members to install a single IPsec SA for the entire network. This also eases the key server management when new group members are added. Network reachability between the group members and the key servers are critical. Routing must be set up properly before enabling the routers for the Cisco IOS GET VPN.

Group Rekey Using Unicast Transport

If any part of the enterprise network is not multicast-capable either due to the core or the enterprise itself, it is recommended to use the unicast transport mechanism to distribute rekeys for all group members. The key server will send a separate rekey for every group member and the group member must respond to the key server with an acknowledgement. The key server will retransmit rekeys if it did not receive the acknowledgement from the group member.

The number of retransmit attempts and the interval are user-configurable. If the key server did not receive the acknowledgement for up to three rekeys from a group member, no further rekeying is sent to that group member. The group member has to re-register with the key server to be able to receive the latest policies for the group.

Note: If the network is large, it poses a load on the key server to send unicast rekey messages and process the acknowledgements received from every group member.

The key server maintains all the registered group members in the database and tracks the number of rekeys sent and acknowledged per group member. This also helps to troubleshoot any issues with a specific group member.

Group Rekey Using Multicast Transport

To use multicast transport, the entire network must be multicast-capable, including the MPLS/IP core. That is to say, multicast VPN (mVPN) is required in the MPLS core. To understand more about mVPN, please visit the link provided in the References section.

When it is time for the key server to send out rekeys to the group members, it sends out a single rekey packet to the core and the core does the replication for all the group members. Since there is no acknowledgement sent by the group member, it is recommended to retransmit the rekeys an additional 2 or 3 times during every rekey period. Using multicast transport is efficient and highly recommended for a larger network as it uses the multicast replication provided by the core. In turn, it reduces the load on the key server to process the rekey messages for each group member and the acknowledgements received from every group member. Moreover, the group member does not send any acknowledgements as required in the unicast transport mechanism.

Note: If the network is large and a small part of the network is not multicast-capable, the customer can still use the multicast transport mechanism for rekeying. This will cause that small set of group members to re-register, but this poses a little load on the key server when compared to the load the key server will have if the entire network is using unicast transport. Each unicast group member forced to re-register will do so before the current group key expires. This avoids any loss of data traffic.

Group Member Access Control List

Group member access control lists (ACLs) are optionally required on selective group members to permit exceptions to the key server policy. Ideally, the use cases for this ACL are to permit routing protocol packets and any other control traffic between the customer edge and provider edge routers unencrypted or to allow unencrypted traffic between the key server and the group member due to the network topology and addressing. The ACL must contain only “deny” statements to allow the specified traffic to go in the clear text; “permit” statements are not allowed. To help understand the usage, a group member ACL is deployed in this configuration.

Cooperative Key Server

This feature of Cisco IOS GET VPN synchronizes the policies and keys distributed by several cooperating key servers deployed in the network. There can be a maximum of 8 key servers. Only one key server can act as the primary, which coordinates the actions of the group. The key servers can be placed anywhere within the enterprise network as long as they are reachable. There are two reasons for keeping multiple key servers: so the group member can register with the nearest key server, and for key server redundancy.

From the key server perspective, if the primary key server goes offline due to network partition or device failure, one of the remaining key servers will assume the role of primary based on an election and start distributing the rekeys. The election of the primary key server is based on the highest priority, which is configurable. In case of more than one key server having the same highest priority, the election is based on the highest IP address. However, if the previous primary key server comes back online, it will only assume the role of secondary. It will not immediately become the primary again. In case of a network partition, it is quite possible that two or more key servers may function as the standalone primaries. Hence during the network rejoin, a new primary is selected for the network. It is a rare case scenario for all 8 key servers to become primaries and involved in a network rejoin.

Note: Rekey configuration, policies defined, and anti-replay configurations must be identical in all key servers.

Multiple Key Servers Configured in Group Member

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.

Note: In case of bringing up the network for the first time, it is recommended to enable cooperative key server first. Once the primary and secondary key servers are running with the policies and the group keys synchronized, the selective group members can be configured with primary or secondary key servers for further registrations. For the network comprising multiple standalone key servers, enabling cooperative key server will be treated as network merge and the newly elected primary will send out rekeys to all group members. In case of adding a new key server and a set of new group members to the existing network, it is advisable to bring up cooperative key servers first and then to configure group members with respective key servers for registrations.

Time-Based Anti-Replay

Cisco IOS GET VPN uses a time-based anti-replay mechanism to protect the group members from replay attacks in a multisender environment. The time window, within which the group member accept the packets, is user-configurable up to 100 seconds. It is highly recommended to use the default value of five seconds for better protection. Time-based anti-replay must be enabled manually. The replay method and the time window must be the same in all the cooperative key servers.

Manageability

Managing the key server and the group member can be done using a separate dedicated IPsec tunnel, either by the enterprise itself or by the service provider. The management traffic should be excluded from the key server policy. Refer to the Management section for more details.

Network Infrastructure

Recommended Platforms and Images

Images based on Cisco IOS Software Release 12.4(11)T are recommended for both key server and group member routers. The recommended image subset is ‘adventerprisek9’ for both the key server and the group member routers.

Key server: Cisco 2800/3800 Series Integrated Service Routers, Cisco 7200 Series Routers, Cisco 7301 Routers

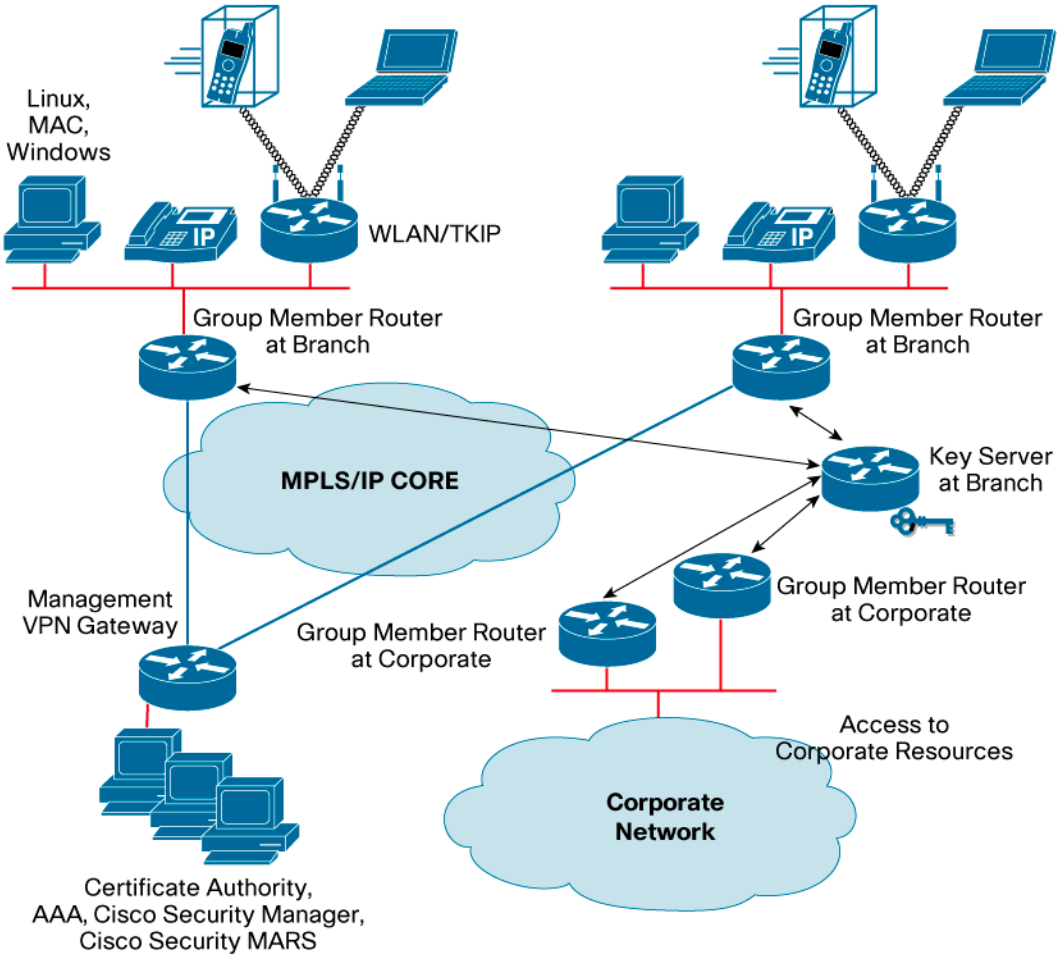
Group member: Cisco 1800/2800/3800 Series Integrated Service Routers, Cisco 7200 Series Routers, Cisco 7301 Routers

Note: The Cisco 871 Integrated Service Router can also be used as a group member if the customer is deploying this solution with very few IPsec SAs (1 to 3). In case of using more IPsec SAs and if a multiple rekey happens in the network before the expiration of existing IPsec SAs,

the group member may easily override the hardware resources of the Cisco 871 and further policies may not be installed properly. This is purely a hardware limitation.

Topology

Figure 2. Modified ECT Topology with GET VPN (Logical View)

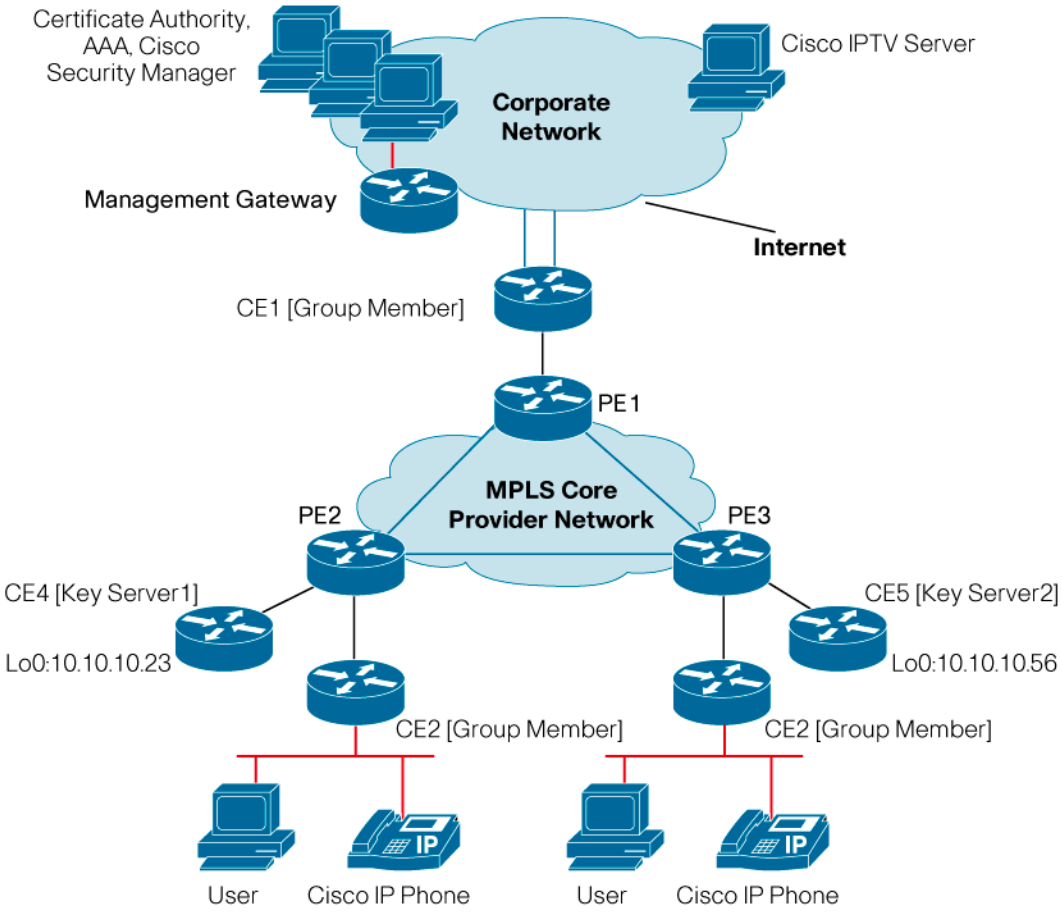


Deployment

1. Baseline Solution

From the Cisco IOS GET VPN deployment perspective, the IP/MPLS core is just a transport medium. Hence, the enterprise customer just needs to configure the key server and group members in their networks. In most cases, the key server and group members are the customer edge routers maintained by the customer. The customer edge router, acting as a group member, will encrypt the multicast traffic and forward it to the MPLS core for replication. The MPLS core is responsible for multicast packet replication for all other group members distributed across the core. This can be achieved only if the original data source and destination networks are routable, since the original network addresses are used on the IPsec/IP header (header preservation) after encrypting the multicast packet.

Figure 3. Enterprise Network Topology Using GET VPN (Physical View)



This deployment shows the configuration steps required for an enterprise-owned key server solution using a single group. This deployment is based on the ECT topology shown above (Figure 3) for enabling end-to-end security between the corporate network and multiple branches running over the MPLS core. The core network is enabled with MPLS/VPN and mVPN technologies to provide both unicast and multicast security for the enterprise VPN network. As shown in the topology, two key servers are deployed and connected to different provider edge routers and the group members are configured with the nearest key server.

Pre-requisites

- The enterprise network must have full network reachability between the routers configured as key server and group member.
- Customer edge routers should be configured for a group member or key server based on the deployment.
- Port UDP 848 must be open in the firewall located in front of group members and key servers for successful GDOI protocol registration.
- To use multicast data encryption and group rekeying through multicast transport, the core must support end-to-end multicast. For the MPLS core, multicast VPN must be enabled in the core.
- Protocol Independent Multicast (PIM) sparse-mode must be enabled in the provider edge-facing interfaces of the group members and the key servers.

- PIM Rendezvous Point (RP) must be reachable from all the group members and the key servers for the multicast group address used for group rekeying.
- DNS, NTP, PKI, and AAA servers must be reachable in the network.

This deployment has integrated PKI, PKI AAA, Cisco IOS Firewall, Context-Based Access Control (CBAC), Dynamic Host Configuration Protocol (DHCP) Server, Network Address Translation (NAT) for Internet-bound traffic, and quality of service (QoS) for prioritizing voice traffic, along with Cisco IOS GET VPN to demonstrate a complete Cisco ECT solution. Complete configuration for these features is provided in the Full Configuration section.

Key Server Configuration

!!!! Before starting key server configuration, generate the RSA key used for rekey. !!!!

```
keyserver1(config)#crypto key generate rsa general-keys label rekeyrsa
modulus 1024
```

With Unicast Rekeying

!!!! The following configuration enables the key server in a router. Each group defined in the key server has an identity that is shared among the members within the group. Here the identity is set to 1234 for group 'GROUP-VPN'. The key server also defines the policies using access-list sa-acl to be distributed to group members upon registration. Further rekeys are sent through unicast transport mechanism with 2 more retransmits at 10 seconds apart. The key server uses this retransmit configuration to resend rekeys in case the acknowledgements are not received from the group member for the rekey sent earlier. The lifetime validity of rekey policy is configured for 3 hours. Time-based anti-replay is enabled with default 5 seconds. !!!!

```
!
crypto gdoi group GROUP-VPN
 identity number 1234
 server local    // local keyword identified this router as key server
//
  rekey lifetime seconds 10800    // lifetime of rekey policy set to 3
hours //
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa  // Generate RSA key for
rekey //
  rekey transport unicast    // Rekeying through unicast transport //
  sa ipsec 1
   profile vpnprof   // Negotiates transform-set for group members //
   match address ipv4 sa-acl    // Policies downloadable to group
members //
   replay time window-size 5  // Time based anti-replay with 5 sec //
  address ipv4 10.10.10.23        // This is the source address of the
rekey packet //
```

Note: The policies defined in the key server are downloaded to all group members irrespective of which group member has the network addresses defined in the policy. As you can see below, this deployment use multiple policies to showcase the configuration required when using multiple networks. However, it is highly recommended to use a single major network as mentioned in the previous note.

!!!! ISAKMP and IPsec profile configuration are defined below. The lifetime configuration for the group IPsec SA is defined under the 'crypto ipsec profile' configuration below. This

configuration uses the default value of 1 hour and hence it is not explicitly shown here. This deployment uses PKI certificates for authentication; PKI-related configurations are shown in the Full Configuration section later in the document. !!!!

```
!
crypto isakmp policy 1    // isakmp policy uses pki authentication //
 encr 3des
 group 2
!
crypto ipsec transform-set 3des esp-3des esp-sha-hmac
!
crypto ipsec profile vpnprof
 set transform-set 3des
!
```

!!!! The following configuration shows that there is no crypto map associated with any physical interface. !!!!

```
!
interface Loopback0
 ip address 10.10.10.23 255.255.255.255
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/1
 description Connected to PE2
 ip address 10.10.10.26 255.255.255.252
 ip pim sparse-dense-mode
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
```

!!!! The following ACL defines the policies to be pushed to group members.

Note: The policies are defined for both unicast and multicast data. The group members use subnets within 10.1.0.0 to 10.1.3.255 for inside interfaces and the corporate network has multiple major networks, including other subnets of 10.0.0.0/8 and 172.16.0.0, 192.168.0.0 networks. Since both the inside interfaces and the CE-PE interfaces fall under the same major network 10.0.0.0/8, only the inside interface subnets are defined in the policy for encryption. In addition, the group member at the corporate network needs the IPsec SA to support the traffic from corporate to branches. This is why the ACL contains mirrored entries. It is highly recommended to use a single major network for the entire network to reduce these ACL entries. !!!!

```
!
ip access-list extended sa-acl
 permit ip 10.1.0.0 0.0.3.255 10.0.0.0 0.255.255.255
 permit ip 10.1.0.0 0.0.3.255 192.168.0.0 0.0.255.255
 permit ip 10.1.0.0 0.0.3.255 172.16.0.0 0.15.255.255
 permit ip 10.0.0.0 0.255.255.255 10.1.0.0 0.0.3.255
 permit ip 172.16.0.0 0.15.255.255 10.1.0.0 0.0.3.255
 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.3.255
 permit ip any 239.192.0.0 0.0.255.255
```

```
!
```

To Convert Unicast Rekeying to Multicast Rekeying

!!! With retaining all other configuration, removing “rekey transport unicast” will enable the key server to send rekeys using multicast transport. Also, the multicast group address, to which rekeys are sent, needs to be configured. PIM must be enabled on the respective interfaces. !!!

```
!
crypto gdoi group GROUP-VPN
 identity number 1234
 server local        // local keyword identifies this router as key
server //
  rekey address ipv4 rekey-multicast-group //multicast group address
to which rekey is sent//
  rekey lifetime seconds 10800    // Validity of key encrypting
traffic keys //
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa  // Generate RSA key for
rekey //
  sa ipsec 1
   profile vpnprof             // Negotiates transform-set for group
members //
   match address ipv4 sa-acl    // Policies downloadable to group
members //
   replay time window-size 5  // Time based anti-replay with 5 sec //
```

!!! The following configuration shows PIM is enabled in the loopback interface also as the rekey uses the loopback interface as the source address. The source address is also defined in the access list used by the rekey. !!!

```
!
ip multicast-routing    // Enable multicast routing //
!
interface Loopback0
 ip address 10.10.10.23 255.255.255.255
 ip pim sparse-dense-mode  // PIM enabled //
!
interface GigabitEthernet0/1    // No crypto map is applied in
interface //
 description Connected to PE2
 ip address 10.10.10.26 255.255.255.252
 ip pim sparse-dense-mode  // PIM enabled //
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
// The following access list defines the multicast group to which
rekeys are sent. //
ip access-list extended rekey-multicast-group
 permit udp host 10.10.10.23 eq 848 host 239.192.1.190 eq 848
!
// This deployment uses auto-RP for this multicast group
239.192.1.190. Optionally, static RP can be configured. //
```

```
!
ip pim rp-address 10.10.10.26 multicast_rp_blockdensemode
!
ip access-list standard multicast_rp_blockdensemode
 remark ACL to block dense-mode operation of client broadcasts
 remark during routing instability (applied to pim rp-address command)
 deny   224.0.1.39
 deny   224.0.1.40
 permit any
!
```

!!!! The following ACL defines the policies to be pushed to group members.

Note: The first deny ACL for multicast group 239.192.1.190 is specified to allow the group members to receive the rekey packets sent using multicast transport. For this configuration, rekeying using multicast transport use group address 239.192.1.190. Since the policy includes encryption for all multicast groups in the 239.192.x.x range, the group members would expect the rekey packets also to be encrypted by the traffic encryption key, which is not possible and hence the group member will drop the rekey packet. This is why the explicit deny is mentioned at the top of the access list. The other option is to specify the group member access list in all the group members, which is cumbersome. !!!!

```
!
ip access-list extended sa-acl
 deny   ip any host 239.192.1.190
 permit ip 10.1.0.0 0.0.3.255 10.0.0.0 0.255.255.255
 permit ip 10.1.0.0 0.0.3.255 192.168.0.0 0.0.255.255
 permit ip 10.1.0.0 0.0.3.255 172.16.0.0 0.15.255.255
 permit ip 10.0.0.0 0.255.255.255 10.1.0.0 0.0.3.255
 permit ip 172.16.0.0 0.15.255.255 10.1.0.0 0.0.3.255
 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.3.255
 permit ip any 239.192.0.0 0.0.255.255
!
```

Note: The policies defined in the key server ACL did not include “deny” statements for customer edge/provider edge communication, including routing traffic, PIM, and other control plane traffic. If customer edge/provider edge addressing involves a subnet from any of the protected traffic (as defined using “permit” statements), it is recommended to configure “deny” statements for customer edge/provider edge traffic at the top of the ACL. The optional configuration of the group member ACL is provided in the group member configuration.

Enabling Cooperative Key Server

The above configuration is sufficient to enable the key server as a standalone for an enterprise network. Let us now configure the cooperative key server. First, a few things need to be considered:

- Generate RSA keys in the primary key server (as required for rekeys) and export both private and public keys. Import these keys into all secondary key servers. This is required in case the primary key server goes down; the rekeys sent by the newly elected primary key server will still be decrypted by the group member.

- The default redundancy timers are large and hidden. However, if the customer needs to change those timers to speed up the detection of the key server failure, one must enable “service internal” to access those timers.
- 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 priorities for selecting the primary key server for easy setup and troubleshooting.
- Rekey configuration, policies defined, and anti-replay configurations must be the same between all key servers.

The procedure to export and import RSA keys is given below.

```
!
keyserver1(config)#crypto key generate rsa general-keys label rekeyrsa
modulus 1024 exportable
% Generating 1024 bit RSA keys, keys will be exportable...[OK]
```

!!! Export this key to the terminal. !!!

```
keyserver1(config)#crypto key export rsa rekeyrsa pem terminal 3des
passphrase
```

!!! Import this key using cut-and-paste on all the other key servers. Exportable option is to allow this procedure for any other key servers deployed later. !!!

```
keyserver2(config)# crypto key import rsa rekeyrsa pem exportable
terminal passphrase
!
```

Now, let us enable redundancy in both key servers.

Primary Key Server

```
!
crypto gdoi group GROUP-VPN
server local
  redundancy           // enabling cooperative key server function //
   local priority 100   // priority decides the role of this key
server //
   peer address ipv4 10.10.10.56 // All other key servers must be
configured //
!
```

Secondary Key Server

```
!
crypto gdoi group GROUP-VPN
server local
  redundancy           // enabling cooperative key server function //
   local priority 75     // priority decides the role of this key
server //
   peer address ipv4 10.10.10.23 // All other key servers must be
configured //
Group Member Configuration
```

!!!! IPsec transform-sets and profile configurations are not required as they are part of the negotiation with the key server when establishing the GDOI session. Only ISAKMP configurations are required to be defined to allow the group member and the key server to authenticate each other. !!!!

```
!
```

```
crypto isakmp policy 1  //Using PKI authentication. Refer to the Full
Configuration. //
encr 3des
group 2
!
crypto isakmp keepalive 10
!
```

!!!!

Note: For using preshared key authentication method, preshared keys are needed in each group member only to authenticate the key server. It is not required to define preshared keys to authenticate other group members. !!!!

!!!! Group member is defined with same identity and location of key server. !!!!

```
!
crypto gdoi group getvpn
 identity number 1234
 server address ipv4 10.10.10.56   // Registration with secondary key
server //
 server address ipv4 10.10.10.23  // If previous server is not
reachable, then register with this server //
!
```

!!!! Crypto map has a new type `gdoi' and is tied to group member created above. !!!!

```
!
crypto map gdoi 1 gdoi
 set group getvpn
 match address no-encryption-acl     // GM ACL defined here //
!
```

!!!! GDOI is enabled by applying crypto map to outside physical interface. !!!!

```
!
 interface FastEthernet0/0
 description outside interface to PE2
 ip address 10.10.10.42 255.255.255.240
 ip pim sparse-dense-mode      // To support multicast rekey //
 duplex auto
 speed auto
 crypto map gdoi       // crypto map enabled in physical interface //
!
interface Vlan10
 description Inside interface
 ip address 10.1.1.1 255.255.255.248
 ip tcp adjust-mss 1360
!
```

!!!!

Note: The following GM ACL has deny statements. The first statement allows any communication to the key server in clear text. There is no crypto map enabled in the key server, so it cannot understand an encrypted packet. Without this line, group member would encrypt the packet based on the policy defined in the key server. The third line makes the group member

accept the multicast rekey packet sent to the group 239.192.1.190. This is due to the common policy defined in the key server to allow encryption for all 239.192.x.x range addresses.
The alternative is to deny the policy itself defined in the key server. The other suggested line for this ACL is to deny traffic between CE-to-PE-only communication, such as routing protocol adjacency, PIM transport, etc. !!!!

```
!
ip access-list extended no-encryption-acl
 deny ip 10.1.1.0 0.0.0.255 host 10.10.10.23
 deny ip host 10.10.10.42 host 10.10.10.41 // excludes routing traffic
to PE from encryption //
 deny ip any host 239.192.1.190
!
```

2. Management

Out-of-band management of remote group members and key servers is done using a separate dedicated IPsec tunnel. For this, a separate management gateway is deployed to which all remote devices build a management tunnel. It is recommended to place this management gateway outside of any group members. In case of network issues for any remote device, the remote device can be always reachable through this management tunnel.

The servers for PKI, AAA, and any other management stations are placed behind this management gateway (Figure 3). As part of PKI authentication, the group member may need to download a Certificate Revocation List (CRL), and any AAA validations. Hence the group member will bring up this management tunnel before successful registration with the key server.

Note: As shown in this deployment below, it is recommended to use a separate subnet and assign host addresses to a loopback interface in each remote device. This would simplify excluding only this subnet from the key server policy.

In addition, this management tunnel will be useful for secure provisioning of new group members or key servers using Secure Device Provisioning (SDP). The SDP servers should be placed behind the management gateway. For more information about provisioning, visit http://www.cisco.com/en/US/products/ps6809/products_ios_protocol_option_home.html.

Key Server

The deny entries configured at the top of the access list exclude the management traffic from the group key encryption for the group members. This is required because the management gateway resides in one of the corporate subnets.

```
!
ip access-list extended sa-acl
 1 deny   ip 10.1.3.0 0.0.0.31 172.16.1.96 0.0.0.31
 2 deny   ip 172.16.1.96 0.0.0.31 10.1.3.0 0.0.0.31
```

Group Member

The management gateway uses a separate PKI server as part of the ECT_PKI recommendation. The group member should enroll with the PKI server. Here is the configuration needed for enabling the management tunnel.

```
!
ip host management-ca 172.16.1.102
```

```
!
crypto pki trustpoint mgmt-ca          // IOS CA //
 enrollment url http://mgmt-ca:80
 serial-number
 revocation-check crl
 source interface Loopback0
 auto-enroll 60
!
crypto ipsec transform-set mgmt-3des esp-3des esp-sha-hmac
```

!!! The following crypto map has added another instance ‘ipsec-isakmp’ for management tunnel. !!!

```
!
crypto map gdoi 1 gdoi           // get vpn configuration //
 set group getvpn
 match address no-encryption-acl
 qos pre-classify
crypto map gdoi 2 ipsec-isakmp  // for management tunnel //
 description Management Tunnel
 set peer 172.16.10.1
 set transform-set mgmt-3des
 match address mgmt_acl
!
interface Loopback0       // Used as source for management traffic //
 ip address 10.1.3.1 255.255.255.255
!
```

!!! This deployment use BGP routing protocol between CE-PE. Hence the management network is advertised in BGP. !!!

```
!
router bgp 65002
 network 10.1.3.1 mask 255.255.255.255
!
```

!!! Only the group member’s Loopback 0 is allowed to use management tunnel as defined in mgmt_acl. !!!

```
!
ip access-list extended mgmt_acl
 permit ip host 10.1.3.1 172.16.1.96 0.0.0.31
!
ip access-list extended fw_acl
 permit udp any any eq isakmp    // permit isakmp to bring up
management tunnel //
!
```

3. Services and Applications

As part of Cisco ECT services and applications, this deployment has integrated Cisco IOS Firewall, CBAC, NAT, QoS, IP telephony, and multicast features in the group members. The configuration is given below.

Cisco IOS Firewall

```
interface FastEthernet0/0
 description outside interface to PE2
```

```
 ip access-group fw_acl in          //IOS firewall for security //
```

!!!! The following Cisco IOS Firewall should only open ports for traffic required for critical functions such as DNS, NTP, AAA, routing, etc. !!!

```
!
ip access-list extended fw_acl
 permit esp any any
 permit udp any any eq 848    // required for the key server
registration //
 permit udp any any eq isakmp
 permit tcp 10.10.10.0 0.0.0.255 eq bgp 10.10.10.0 0.0.0.255        //
to permit BGP //
 permit tcp 10.10.10.0 0.0.0.255 10.10.10.0 0.0.0.255 eq bgp
 permit pim any any            // to build PIM adjacencies with PE //
 permit igmp any any
 permit udp any host 224.0.1.39       // to permit PIM auto-RP
messages //
 permit udp any host 224.0.1.40
 permit ip 172.16.1.96 0.0.0.31 10.10.10.0 0.0.0.255   // to permit
pki, aaa responses //
 permit tcp host 10.10.10.23 10.10.10.0 0.0.0.255 eq 22  //for admin
purpose//
 permit udp host 172.16.1.97 eq ntp any
 permit udp any any eq bootpc
 permit icmp any any
 deny   ip any any log
!
```

CBAC

!!! CBAC dynamically open ports for IP telephony (voice) and other TCP applications. !!!

```
!
ip inspect name test tcp
ip inspect name test udp
ip inspect name test realaudio
ip inspect name test rtsp
ip inspect name test tftp
ip inspect name test ftp
ip inspect name test h323
ip inspect name test netshow
ip inspect name test streamworks
ip inspect name test esmtp
ip inspect name test skinny
ip inspect name test sip
!
interface Vlan10
 description Inside interface
 ip inspect test in          // CBAC enabled //
```

NAT

!!! NAT is applied only for Internet-bound traffic. Traffic to the corporate network is excluded from nat_acl. !!!

```
 interface FastEthernet0/0
 description outside interface
 ip nat outside
!
interface Vlan10
 description inside interface
 ip nat inside
!
ip nat inside source list nat_acl interface FastEthernet0 overload
!
ip access-list extended nat_acl
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.0.15.255
 deny   ip any 192.168.0.0 0.0.255.255
 permit ip 10.1.1.0 0.0.0.7 any
```

Quality of Service

!!! This policy prioritizes voice traffic and the shaping policy is shown for an example. The actual policy and requirements may vary based on customer needs. !!!

```
class-map match-any call-setup
 match  dscp af31
 match  dscp af32
 match  dscp cs3
 match  precedence 3
class-map match-any internetwork-control
 match  dscp cs6
 match access-group name gdoi_acl
class-map match-any qos
 match access-group name test
class-map match-any voice
 match  dscp ef
 match  dscp cs5
 match  precedence 5
!
policy-map voip_getvpn
 description Note LLQ for ATM/DSL G.729=64K, G.711=128K
 class voice
  priority 128
 class call-setup
  bandwidth percent 2
 class internetwork-control
  bandwidth percent 5
 class class-default
  fair-queue
  random-detect
policy-map shaper
 class class-default
  shape average 10000000
```

```
  service-policy voip_getvpn
!
ip access-list extended gdoi_acl
 permit udp any eq 848 any eq 848
!
crypto map gdoi 1 gdoi
 qos pre-classify            // enables qos for encyrpted traffic //
!
interface FastEthernet0/0
 description outside interface to PE2
 service-policy output shaper    // Apply Qos policy to interface //
```

IP Multicast

!!! Cisco IPTV server is deployed in the corporate network streaming multicast data traffic. PIM RP 192.168.1.13 is also placed in the corporate network. The following configuration is required in all the remote group members to join the multicast network. !!!

```
!
ip multicast-routing
!
interface Vlan10
 description Inside interface
  ip pim sparse-dense-mode
!
ip pim rp-address 192.168.1.13 multicast_rp_blockdensemode
!
ip access-list standard multicast_rp_blockdensemode
 remark ACL to block dense-mode operation of client broadcasts
 remark during routing instability (applied to pim rp-address command)
 deny   224.0.1.39
 deny   224.0.1.40
 permit any
!
```

Limitations

- An additional device is needed to function as the key server.
- All key servers and group members must run atleast Cisco IOS Software Release 12.4(11)T based images or later.
- Key servers and Group members behind Network Address Translation (NAT) are not supported due to the preservation of source and destination addresses.
- Not suitable for public-Internet-based deployment due to the preservation of source and destination addresses.
- Policies defined in the key server are downloaded to all group members even if no multicast source or receiver is connected or active for that group member.
- If a group member has to be removed from a group, two steps must be taken. First, the authentication credentials of the group member need to be deleted. Second, the IPsec and rekey policy must be deleted, which causes all of the group members to re-register.

- Default redundancy timers are high and the detection of primary key server failure can take as long as 18 minutes. However, you can reduce the values for those timers using manual configuration.
- Group member ACLs cannot have permit statements.
- Provisioning support in Cisco Security Manager for the group members and the key servers is available only through flexconfig templates.
- If a group member cannot successfully register with the key server, the group member may transmit all data traffic in clear text. The user must deploy necessary outbound ACLs in the group member to protect from sending clear-text traffic. An example ACL "block_clear_text" is given in the Full Configuration section for group member 1.
- If the group member did not receive rekeys and further registration fails, data traffic protected by the policy will also be dropped. Workaround is to do "clear crypto gdoi" in the group member for re-registration.

Reference

- Group Domain of Interpretation—RFC 3547 http://www.ietf.org/rfc/rfc3547.txt
- Cisco Enterprise-Class Teleworker Solution http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/prod_brochure0900aecd803fc7ec.html
- Public Key Infrastructure Integration with Cisco Enterprise-Class Teleworker Solution http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6807/prod_white_paper0900aecd805249e3.shtml
- Cisco IOS IPsec High Availability for Management Gateway Configuration http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd80278edf.shtml
- Implementing Group Domain of Interpretation in a Dynamic Multipoint VPN http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6811/prod_white_paper0900aecd804c363f.shtml
- Cisco IOS Secure Multicast http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6552/prod_white_paper0900aecd8047191e.shtml
- Cisco IOS GET VPN Architecture and Features http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/htgetvpn.htm
- Multicast VPN http://www.cisco.com/en/US/products/ps6651/products_ios_protocol_option_home.html

Full Configuration

Full Configuration—Key Server 1

```
keyserver1#sh startup-config
Using 5372 out of 522232 bytes
!
version 12.4
service timestamps debug datetime localtime
service timestamps log uptime
service password-encryption
service internal
!
hostname keyserver1
!
boot-start-marker
boot system flash disk2:c7200-adventerprisek9-mz.124-11.T
boot-end-marker
!
logging buffered 100000
enable secret  <removed>
!
aaa new-model
!
aaa group server radius pki-aaa-server        // AAA server resides in
management subnet //
 server-private 172.16.1.106 auth-port 1812 acct-port 1813 key
<removed>
!
aaa authentication login admin group tacacs+ enable
aaa authorization exec admin group tacacs+
aaa authorization network pkiaaa group pki-aaa-server
!
aaa session-id common
clock timezone pst -8
clock summer-time pdt recurring
ip cef
!
ip domain name cisco.com
ip host ios-cert-server 172.16.1.117
ip name-server 192.168.1.183
ip multicast-routing
ip ssh rsa keypair-name sshrsa
!
multilink bundle-name authenticated
!
crypto pki trustpoint ios-cert-server
 enrollment url http://ios-cert-server:80
 serial-number
 revocation-check crl
```

```
 rsakeypair keyserver1.cisco.com
 auto-enroll 60
 authorization list pkiaaa          // verifies the device
authorization in AAA server //
!
crypto pki certificate chain ios-cert-server
 certificate <removed>
 certificate ca <removed>
!
controller ISA 1/1
!
crypto isakmp policy 1                    !!! PKI authentication !!!
 encr 3des
 group 2
!
crypto isakmp policy 2
 encr 3des
!
!
crypto ipsec transform-set 3des esp-3des esp-sha-hmac
crypto ipsec transform-set aes esp-aes esp-sha-hmac
!
crypto ipsec profile vpnprof
 set transform-set 3des
!
crypto gdoi group GROUP-VPN
 identity number 1234
 server local
  rekey address ipv4 rekey-multicast-group        // not required for
unicast rekeying //
  rekey lifetime seconds 10800
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa
  rekey transport unicast
  sa ipsec 1
   profile vpnprof
   match address ipv4 sa-acl
   replay time window-size 5
  address ipv4 10.10.10.23
  redundancy
   local priority 100
   peer address ipv4 10.10.10.56
!
interface Loopback0
 ip address 10.10.10.23 255.255.255.255
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/1
 description Connected to PE2
 ip address 10.10.10.26 255.255.255.252
```

```
 ip pim sparse-dense-mode
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no keepalive
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
router bgp 65002
 no synchronization
 bgp log-neighbor-changes
 network 10.10.10.23 mask 255.255.255.255
 neighbor 10.10.10.25 remote-as 65001
 no auto-summary
!
no ip http server
no ip http secure-server
!
ip pim rp-address 192.168.1.13 multicast_rp_blockdensemode          //
RP for multicast data //
!
ip access-list standard multicast_rp_blockdensemode
 remark ACL to block dense-mode operation of client broadcasts
 remark during routing instability (applied to pim rp-address command)
 deny   224.0.1.39
 deny   224.0.1.40
 permit any
!
ip access-list extended rekey-multicast-group
 permit udp host 10.10.10.23 eq 848 host 239.192.1.190 eq 848
 permit udp host 10.10.10.56 eq 848 host 239.192.1.190 eq 848
ip access-list extended sa-acl
 deny   ip any host 239.192.1.190
 deny   ip 10.1.3.0 0.0.0.31 172.16.1.96 0.0.0.31       // to exclude
management traffic //
```

```
 deny   ip  172.16.1.96 0.0.0.31 10.1.3.0 0.0.0.31      // to exclude
management traffic //
 permit ip 10.1.0.0 0.0.3.255 10.0.0.0 0.255.255.255
 permit ip 10.1.0.0 0.0.3.255 192.168.0.0 0.0.255.255
 permit ip 10.1.0.0 0.0.3.255 172.16.0.0 0.15.255.255
 permit ip 10.0.0.0 0.255.255.255 10.1.0.0 0.0.3.255
 permit ip 172.16.0.0 0.15.255.255 10.1.0.0 0.0.3.255
 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.3.255
 permit ip any 239.192.0.0 0.0.255.255
!
logging alarm informational
!
tacacs-server host 192.168.1.137
tacacs-server timeout 3
tacacs-server directed-request
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 password 7 < removed >
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login authentication admin
line vty 5 15
 transport input ssh
 transport output all
!
ntp clock-period 17179850
ntp server 172.16.1.97 prefer
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end
keyserver1#
```

Full Configuration—Key Server 2

```
keyserver2#sh startup-config
Using 5100 out of 522232 bytes
!
version 12.4
service timestamps debug datetime localtime
service timestamps log uptime
```

```
service password-encryption
service internal
!
hostname keyserver2
!
boot-start-marker
boot system flash disk2:c7200-adventerprisek9-mz.124-11.T
boot-end-marker
!
logging queue-limit 100
logging buffered 100000
enable secret  <removed>
!
aaa new-model
!
aaa group server radius pki-aaa-server
 server-private 172.16.1.106 auth-port 1812 acct-port 1813 key
<removed>
!
aaa authentication login admin group tacacs+ enable
aaa authorization exec admin group tacacs+
aaa authorization network pkiaaa group pki-aaa-server
!
aaa session-id common
clock timezone pst -8
clock summer-time pdt recurring
!
ip cef
ip domain name cisco.com
ip host ios-cert-server 172.16.1.117
ip name-server 192.168.1.183
!
ip multicast-routing
ip ssh rsa keypair-name sshrsa
!
multilink bundle-name authenticated
!
crypto pki trustpoint ios-cert-server
 enrollment url http://ios-cert-server:80
 serial-number
 revocation-check crl
 rsakeypair keyserver2.cisco.com
 auto-enroll 60
!
crypto pki certificate chain ios-cert-server
 certificate <removed>
 certificate ca <removed>
!
crypto isakmp policy 1
 encr 3des
```

```
 group 2
!
crypto ipsec transform-set 3des esp-3des esp-sha-hmac
crypto ipsec transform-set aes esp-aes esp-sha-hmac
!
crypto ipsec profile vpnprof
 set transform-set 3des
!
crypto gdoi group GROUP-VPN
 identity number 1234
 server local
  rekey address ipv4 rekey-multicast-group
  rekey lifetime seconds 10800
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa rekeyrsa
  rekey transport unicast
  sa ipsec 1
   profile vpnprof
   match address ipv4 sa-acl
   replay time window-size 5
  address ipv4 10.10.10.56
  redundancy
   local priority 75
   peer address ipv4 10.10.10.23
!
interface Loopback0
 ip address 10.10.10.56 255.255.255.255
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/1
 description Connected to PE3
 ip address 10.10.10.54 255.255.255.252
 ip pim sparse-dense-mode
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
router bgp 65002
 no synchronization
 bgp log-neighbor-changes
```

```
 network 10.10.10.56 mask 255.255.255.255
 neighbor 10.10.10.53 remote-as 65001
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.10.10.53
!
no ip http server
no ip http secure-server
!
ip pim rp-address 192.168.1.13 multicast_rp_blockdensemode
!
ip access-list standard multicast_rp_blockdensemode
 remark ACL to block dense-mode operation of client broadcasts
 remark during routing instability (applied to pim rp-address command)
 deny   224.0.1.39
 deny   224.0.1.40
 permit any
!
ip access-list extended rekey-multicast-group
 permit udp host 10.10.10.23 eq 848 host 239.192.1.190 eq 848
 permit udp host 10.10.10.56 eq 848 host 239.192.1.190 eq 848
ip access-list extended sa-acl
 deny   ip any host 239.192.1.190
 deny   ip 10.1.3.0 0.0.0.31 172.16.1.96 0.0.0.31       // to exclude
management traffic //
 deny   ip  172.16.1.96 0.0.0.31 10.1.3.0 0.0.0.31      // to exclude
management traffic //
 permit ip 10.1.0.0 0.0.3.255 10.0.0.0 0.255.255.255
 permit ip 10.1.0.0 0.0.3.255 192.168.0.0 0.0.255.255
 permit ip 10.1.0.0 0.0.3.255 172.16.0.0 0.15.255.255
 permit ip 10.0.0.0 0.255.255.255 10.1.0.0 0.0.3.255
 permit ip 172.16.0.0 0.15.255.255 10.1.0.0 0.0.3.255
 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.3.255
 permit ip any 239.192.0.0 0.0.255.255
logging alarm informational
!
tacacs-server host 192.168.1.137
tacacs-server timeout 3
tacacs-server directed-request
!
control-plane
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
 password < removed >
 stopbits 1
```

```
line aux 0
 stopbits 1
line vty 0 4
 login authentication admin
line vty 5 15
 transport input ssh
 transport output all
!
ntp clock-period 17179914
ntp server 172.16.1.97
!
end
keyserver2#
```

Full Configuration—Group Member 1 [Branch Office]

```
group-member1#sh startup-config
Using 5735 out of 196600 bytes
!
version 12.4
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname group-member1
!
boot-start-marker
boot system flash:c1841-adventerprisek9-mz.124-11.T
boot-end-marker
!
logging buffered 100000
enable secret  <removed>
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
clock timezone PST -8
clock summer-time PDT recurring
ip cef
!
no ip dhcp use vrf connected
no ip dhcp conflict logging
!
ip dhcp pool client          !!! DHCP server for internal devices !!!
   network 10.1.1.0 255.255.255.248
   domain-name cisco.com
   option 150 ip 192.168.1.70
   netbios-name-server 192.168.1.238
```

```
   dns-server 192.168.1.183
   default-router 10.1.1.1
!
ip ftp source-interface Vlan10
ip tftp source-interface Vlan10
ip domain lookup source-interface Vlan10
ip domain name cisco.com
ip host ios-cert-server 172.16.1.117
ip host mgmt-ca 172.16.1.102
ip multicast-routing
ip inspect name test tcp                          !!! CBAC policy !!!
ip inspect name test udp
ip inspect name test realaudio
ip inspect name test rtsp
ip inspect name test tftp
ip inspect name test ftp
ip inspect name test h323
ip inspect name test netshow
ip inspect name test streamworks
ip inspect name test esmtp
ip inspect name test skinny
ip inspect name test sip
no ip igmp snooping
login on-failure log
!
multilink bundle-name authenticated
!
crypto pki trustpoint ios-cert-server    !!! PKI configuration for GET
VPN !!!
 enrollment url http://ios-cert-server:80
 serial-number
 ip-address none
 password 7 < removed >
 revocation-check crl
 source interface Loopback0              // this will force the
management tunnel bringup //
 auto-enroll 60
!
crypto pki trustpoint mgmt-ca               !!! PKI configuration for
Management tunnel !!!
 enrollment url http://mgmt-ca:80
 serial-number
 revocation-check crl
 source interface Loopback0
 auto-enroll 60
!
crypto pki certificate chain ios-cert-server
 certificate <removed>
 certificate ca <removed>
!
```

```
crypto pki certificate chain mgmt-ca
 certificate <removed>
 certificate ca <removed>
!
class-map match-any call-setup
 match  dscp af31
 match  dscp af32
 match  dscp cs3
 match  precedence 3
class-map match-any internetwork-control
 match  dscp cs6
 match access-group name gdoi_acl
class-map match-any qos
 match access-group name test
class-map match-any voice
 match  dscp ef
 match  dscp cs5
 match  precedence 5
!
policy-map voip_getvpn
 description Note LLQ for ATM/DSL G.729=64K, G.711=128K
 class voice
  priority 128
 class call-setup
  bandwidth percent 2
 class internetwork-control
  bandwidth percent 5
 class class-default
  fair-queue
  random-detect
policy-map shaper
 class class-default
  shape average 10000000
  service-policy voip_getvpn
!
crypto isakmp policy 1             !!! PKI authentication enabled !!!
 encr 3des
 group 2
crypto isakmp keepalive 10
!
crypto gdoi group getvpn           !!! GETVPN group configuration !!!
 identity number 1234
 server address ipv4 10.10.10.56       // registration with secondary
key server //
 server address ipv4 10.10.10.23
!
crypto map gdoi 1 gdoi                          !!! GETVPN !!!
 set group getvpn
 match address no-encryption-acl
 qos pre-classify                                    // Qos //
```

```
crypto map gdoi 2 ipsec-isakmp         !!! Management Tunnel !!!
 description Management Tunnel
 set peer 172.16.10.1
 set transform-set mgmt-3des
 match address mgmt_acl
!
interface Loopback0
 description Management interface
 ip address 10.1.3.1 255.255.255.255
!
interface FastEthernet0/0
 description outside interface to PE2
 no ip dhcp client request tftp-server-address
 ip address 10.10.10.42 255.255.255.252
 ip access-group fw_acl in
 ip access-group block_clear_text out          // Blocking corporate
data traffic in clear text //
 ip pim sparse-dense-mode
 duplex auto
 speed auto
 crypto map gdoi                // GETVPN enabled in the interface //
 service-policy output shaper
!
interface FastEthernet0/1
 description inside interface
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/0/0
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet0/0/1
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet0/0/2
 switchport access vlan 10
!
interface FastEthernet0/0/3
 switchport access vlan 10
!
interface Vlan1
 no ip address
!
interface Vlan10
 description inside interface
 ip address 10.1.1.1 255.255.255.248
```

```
 ip pim sparse-dense-mode
 ip inspect test in
!
interface Async0/1/0
 no ip address
 encapsulation slip
!
interface Async0/1/1
 no ip address
 encapsulation slip
!
router bgp 65002                          !!! BGP routing with PE !!!
 no synchronization
 bgp log-neighbor-changes
 network 10.1.1.0 mask 255.255.255.248
 network 10.1.3.1 mask 255.255.255.255
 neighbor 10.10.10.41 remote-as 65001
 no auto-summary
!
no ip http server
no ip http secure-server
ip pim rp-address 192.168.1.13 multicast_rp_blockdensemode  // PIM RP
for multicast data //
!
ip access-list standard multicast_rp_blockdensemode
 remark ACL to block dense-mode operation of client broadcasts
 remark during routing instability (applied to pim rp-address command)
 deny   224.0.1.39
 deny   224.0.1.40
 permit any
!
ip access-list extended fw_acl     !!! IOS Firewall configuration !!!
 permit esp any any
 permit udp any any eq 848
 permit udp any any eq isakmp
 permit tcp 10.10.10.0 0.0.0.255 eq bgp 10.10.10.0 0.0.0.255
 permit tcp 10.10.10.0 0.0.0.255 10.10.10.0 0.0.0.255 eq bgp
 permit pim any any
 permit igmp any any
 permit udp any host 224.0.1.39
 permit udp any host 224.0.1.40
 permit ip 172.16.1.96 0.0.0.31 10.10.10.0 0.0.0.255
 permit tcp host 10.10.10.23 10.10.10.0 0.0.0.255 eq 22
 permit udp host 172.16.1.97 eq ntp any
 permit udp any any eq bootpc
 permit icmp any any
 deny   ip any any log
ip access-list extended block_clear_text  !!! Blocking clear text !!!
 permit esp any any         // corporate traffic as encrypted only //
 permit udp any eq 848 any eq 848
```

```
 permit pim any any
 permit ip host 10.10.10.42 host 10.10.10.41
 deny ip 10.1.0.0 0.0.3.255 10.0.0.0 0.255.255.255  // deny corporate
traffic in clear text //
 deny ip 10.1.0.0 0.0.3.255 192.168.0.0 0.0.255.255
 deny ip 10.1.0.0 0.0.3.255 172.16.0.0 0.15.255.255
 permit ip any any  // permit internet bound traffic in clear text //
ip access-list extended no-encryption-acl              !!! GM ACL !!!
 deny   ip 10.1.1.0 0.0.0.255 host 10.10.10.23
 deny ip host 10.10.10.42 host 10.10.10.41
 deny   ip any host 239.192.1.190
ip access-list extended mgmt_acl
 permit ip host 10.1.3.1 172.16.1.96 0.0.0.31
ip access-list extended gdoi_acl
 permit udp any eq 848 any eq 848
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
line 0/1/0 0/1/1
 stopbits 1
 speed 115200
 flowcontrol hardware
line vty 0 4
 exec-timeout 0 0
!
scheduler allocate 20000 1000
ntp clock-period 17178752
ntp server 172.16.1.97
!
end
group-member1#
```

Full Configuration—Group Member 2 [Corporate Network]

```
group-member2#sh startup-config
Using 4759 out of 522232 bytes
!
version 12.4
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname group-member2
!
```

```
boot-start-marker
boot system flash disk2:c7200-adventerprisek9-mz.124-11.T
boot-end-marker
!
logging buffered 2000000
no logging console
enable secret  <removed>
!
no aaa new-model
clock timezone pst -8
clock summer-time pdt recurring
!
ip cef
ip domain name cisco.com
ip host ios-cert-server.cisco.com 172.16.1.117
ip name-server 192.168.1.183
!
ip multicast-routing
!
multilink bundle-name authenticated
!
crypto pki trustpoint ios-cert-server
 enrollment url http://ios-cert-server:80
 serial-number
 revocation-check crl
 rsakeypair group-member2.cisco.com
 auto-enroll 60
!
crypto pki certificate chain ios-cert-server
 certificate <removed>
 certificate ca <removed>
!
controller ISA 4/1
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
crypto ipsec fragmentation after-encryption
crypto gdoi group getvpn
 identity number 1234
 server address ipv4 10.10.10.23
 server address ipv4 10.10.10.56
!
crypto map gdoi 1 gdoi
 set group getvpn
 match address no-encryption-acl
!
```

```
interface Loopback0
 ip address 10.10.10.20 255.255.255.255
!
interface GigabitEthernet0/1
 description interface connected to corporate gateway
 ip address 10.10.10.2 255.255.255.252
 ip pim sparse-dense-mode
 ip multicast boundary 1 out
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
interface GigabitEthernet0/2
 description interface connected to corporate gateway
 ip address 10.10.10.6 255.255.255.252
 ip pim sparse-dense-mode
 ip multicast boundary 1 out
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
interface GigabitEthernet0/3
 description interface connected to PE1
 ip address 10.10.10.9 255.255.255.252
 ip pim sparse-dense-mode
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
 crypto map gdoi
!
router ospf 1
 log-adjacency-changes
 redistribute bgp 65002 subnets
 passive-interface GigabitEthernet0/3
 network 10.10.10.0 0.0.0.3 area 0
 network 10.10.10.4 0.0.0.3 area 0
 network 10.10.10.8 0.0.0.3 area 0
 network 10.10.10.20 0.0.0.0 area 0
!
router bgp 65002
 no synchronization
 bgp log-neighbor-changes
 network 10.10.10.20 mask 255.255.255.255
 redistribute ospf 1 match internal external 1 external 2
 neighbor 10.10.10.10 remote-as 65001
 neighbor 10.10.10.10 default-originate
```

```
 no auto-summary
!
ip route 192.168.1.0 255.255.255.0 10.10.10.5
!
no ip http server
no ip http secure-server
!
ip pim autorp listener
!
ip access-list standard multicast_rp_blockdensemode
 remark ACL to block dense-mode operation of client broadcasts
 remark during routing instability (applied to pim rp-address command)
 deny   224.0.1.39
 deny   224.0.1.40
 permit any
!
ip access-list extended no-encryption-acl
 deny   ip host 10.10.10.9 host 10.10.10.10
 deny   ip any host 239.192.1.190
logging alarm informational
access-list 1 permit 239.192.1.190
access-list 1 deny   any
!
control-plane
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 password 7 < removed >
 login
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
password 7 < removed >
 login
!
ntp clock-period 17180026
ntp server 172.16.1.97
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
```

```
end
group-member2#
```

Verification

Key Server 1—Primary Key Server

!!! Show crypto isakmp sa in primary key server should contain IKE sa for all secondary key servers. !!!

```
keyserver1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.10.10.30    10.10.10.23    MM_NO_STATE          0    0 ACTIVE
10.10.10.56    10.10.10.23    GDOI_IDLE         1752    0 ACTIVE    //
secondary key server //
IPv6 Crypto ISAKMP SA
keyserver1#
```

!!! Show crypto gdoi gives an overall info about rekey, replay, policy, group members etc. for all groups. For specific group, use “show crypto gdoi group” cli. !!!

```
keyserver1#sh crypto gdoi
Group Information
    Group Name               : GROUP-VPN
    Group Identity           : 1234
    Group Members            : 11
    IPSec SA Direction       : Both
    Active Group Server      : Local
    Redundancy               : Configured
        Local Address        : 10.10.10.23
        Local Priority       : 100
        Local KS Status      : Alive
        Local KS Role        : Primary
    Group Rekey Lifetime     : 10800 secs
    Group Rekey
        Remaining Lifetime   : 8691 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2
    Group Retransmit
        Remaining Lifetime   : 0 secs
      IPSec SA Number        : 1
      IPSec SA Rekey Lifetime: 3600 secs
      Profile Name           : getvpn
      Replay method          : Time Based
      Replay Window Size     : 5
      SA Rekey
         Remaining Lifetime  : 61 secs
      ACL Configured         : access-list sa-acl
    Group Server list        : Local
keyserver1#
```

!!! To get information that are specific to key server, use show crypto gdoi ks. The available options for this cli will display the output for all groups defined in the key server. !!!

```
keyserver1#sh crypto gdoi ks ?
  acl      Show ACL applied to GDOI group
  coop     Show Cooperative Key Server information
  members  Show Registered Group Member information
  policy   Show key servers policy information
  rekey    Show rekey information
  replay   Display group information for time-based antireplay
  |        Output modifiers
  <cr>
```

!!! To view the output for a specific group in the key server, use “show crypto gdoi group” cli. !!!

```
keyserver1#sh crypto gdoi group GROUP-VPN ks ?
  acl      Show ACL applied to GDOI group
  coop     Show Cooperative Key Server information
  members  Show Registered Group Member information
  policy   Show key servers policy information
  rekey    Show rekey information
  replay   Display group information for time-based antireplay
  |        Output modifiers
  <cr>
```

!!! The following cli shows the policies defined in the key server. This will list for all groups defined in the key server. !!!

```
keyserver1#sh crypto gdoi ks acl
Group Name: GROUP-VPN
 Configured ACL:
   access-list sa-acl deny ip any host 239.192.1.190
   access-list sa-acl deny ip 10.1.3.0 0.0.0.31 172.16.1.96 0.0.0.31
   access-list sa-acl deny ip 172.16.1.96 0.0.0.31 10.1.3.0 0.0.0.31
   access-list sa-acl permit ip 10.1.0.0 0.0.3.255 10.0.0.0
0.255.255.255
   access-list sa-acl permit ip 10.1.0.0 0.0.3.255 192.168.0.0
0.0.255.255
   access-list sa-acl permit ip 10.1.0.0 0.0.3.255 172.16.0.0
0.15.255.255
   access-list sa-acl permit ip 10.0.0.0 0.255.255.255 10.1.0.0
0.0.3.255
   access-list sa-acl permit ip 172.16.0.0 0.15.255.255 10.1.0.0
0.0.3.255
   access-list sa-acl permit ip 192.168.0.0 0.0.255.255 10.1.0.0
0.0.3.255
   access-list sa-acl permit ip any 239.192.0.0 0.0.255.255
keyserver1#
```

!!! The following cli gives info about all group members currently active in the key server. This database maintains the number of rekeys sent, rekey acks received per group member for unicast rekeying. For multicast rekeying, the database maintains the rekey counters globally for the group. Also the key server list the group members registered with its own followed by the members registered with the secondary key server. !!!

```
keyserver1#sh crypto gdoi ks members
Group Member Information :
Number of rekeys sent for group GROUP-VPN : 1083
```

```
Group Member ID   : 10.10.10.9
Group ID          : 1234
Group Name        : GROUP-VPN
Key Server ID     : 10.10.10.23
Rekeys sent       : 1083  // This group member is sent 1083 rekeys //
Rekey Acks Rcvd   : 1083
Rekey Acks missed : 0
Sent seq num :    6    0    0    0
Rcvd seq num :    6    0    0    0
Group Member ID   : 10.10.10.18
Group ID          : 1234
Group Name        : GROUP-VPN
Key Server ID     : 10.10.10.23
Rekeys sent       : 2              // This indicates the group member
may have reloaded recently //
Rekey Acks Rcvd   : 2
Rekey Acks missed : 0
Sent seq num :    5    6    0    0
Rcvd seq num :    5    6    0    0
```

!!! This cli shows the current policy used by all group members. !!!

```
keyserver1#sh crypto gdoi ks policy
Key Server Policy:
For group GROUP-VPN (handle: 2147483650) server 10.10.10.23 (handle:
2147483650):
  # of teks : 1  Seq num : 2
  KEK POLICY (transport type : Unicast)
    spi : 0x33D3E4913368171A2FCB3A3FB77B521
    management alg     : disabled    encrypt alg       : 3DES
    crypto iv length   : 8           key size          : 24
    Remaining life(sec): 8620        orig lifetime(sec): 10800
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : rekeyrsa
  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x66D60BBC    access-list           : sa-acl
    # of transforms    : 0             transform             :
ESP_3DES
    hmac alg           : HMAC_AUTH_SHA
    alg key size       : 24            sig key size          : 20
    orig life(sec)     : 3600          remaining life(sec)   : 3421
    override life (sec): 0             antireplay window size: 5
  Replay Value 1626653.48 secs
For group GROUP-VPN (handle: 2147483650) server 10.10.10.56 (handle:
2147483651):  // currently no policy from the secondary key server //
keyserver1#
```

!!! To check for the rekey transport mode and the number of rekeys sent and acks received per group, use this cli. !!!

```
keyserver1#sh crypto gdoi ks rekey
Group GROUP-VPN (Unicast)
```

```
    Number of Rekeys sent               : 1083
    Number of Rekeys retransmitted      : 0
    KEK rekey lifetime (sec)            : 10800
        Remaining lifetime (sec)        : 8594   /// this indicates
the remaining time to generate new KEK ///
    Retransmit period                   : 10
    Number of retransmissions           : 2
    IPSec SA 1  lifetime (sec)          : 3600
        Remaining lifetime (sec)        : 3395 /// this indicates the
remaining time to send new TEK to group members  ///
```

!!! To check the current replay value maintained by the key server, use this cli. !!!

```
keyserver1#sh crypto gdoi ks replay
Anti-replay Information For Group GROUP-VPN:
  Timebased Replay:
    Replay Value            : 1626689.53 secs
    Remaining sync time     : 1584 secs
```

!!! To verify the working of cooperative key servers, use this cli. Note the peer sessions maintained for each secondary servers in the primary key server. !!!

```
keyserver1#sh crypto gdoi ks coop
Crypto Gdoi Group Name :GROUP-VPN
        Group handle: 2147483650, Local Key Server handle: 2147483650
        Local Address: 10.10.10.23
        Local Priority: 100
        Local KS Role: Primary   , Local KS Status: Alive
        Primary Timers:
                Primary Refresh Policy Time: 20
                Remaining Time: 16
                Antireplay Sequence Number: 81279
        Peer Sessions:
        Session 1:
                Server handle: 2147483651
                Peer Address: 10.10.10.56
                Peer Priority: 75
                Peer KS Role: Secondary , Peer KS Status: Alive     //
secondary key server //
                Antireplay Sequence Number: 76
                IKE status: Established
                Counters:
                    Ann msgs sent: 81248
                    Ann msgs sent with reply request: 0
                    Ann msgs recv: 124
                    Ann msgs recv with reply request: 11
                    Packet sent drops: 31
                    Packet Recv drops: 0
                    Total bytes sent: 51840466
                    Total bytes recv: 141581
keyserver1#
```

Key Server 2—Secondary Key Server

!!! Show crypto isakmp sa in secondary key server should contain IKE sa for primary key server. !!!

```
keyserver2#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.10.10.56    10.10.10.23    GDOI_IDLE         1073    0 ACTIVE
// primary key server //
IPv6 Crypto ISAKMP SA
keyserver2#sh crypto gdoi
Group Information
    Group Name               : GROUP-VPN
    Group Identity           : 1234
    Group Members            : 12
    IPSec SA Direction       : Both
    Active Group Server      : Local
    Redundancy               : Configured
        Local Address        : 10.10.10.56
        Local Priority       : 75
        Local KS Status      : Alive
        Local KS Role        : Secondary   // secondary key server //
    Group Rekey Lifetime     : 10800 secs
    Group Rekey
        Remaining Lifetime   : 8686 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2
    Group Retransmit
        Remaining Lifetime   : 0 secs
      IPSec SA Number        : 1
      IPSec SA Rekey Lifetime: 3600 secs
      Profile Name           : getvpn
      Replay method          : Time Based
      Replay Window Size     : 5
      SA Rekey
         Remaining Lifetime  : 58 secs
      ACL Configured         : access-list sa-acl
    Group Server list        : Local
keyserver2#
```

!!! The following cli shows the policies defined in the key server. This will list for all groups defined in the key server. The acl entries must be same as in primary key server. !!!

```
keyserver2#sh crypto gdoi ks acl
Group Name: GROUP-VPN
 Configured ACL:
   access-list sa-acl deny ip any host 239.192.1.190
   access-list sa-acl deny ip 10.1.3.0 0.0.0.31 172.16.1.96 0.0.0.31
   access-list sa-acl deny ip 172.16.1.96 0.0.0.31 10.1.3.0 0.0.0.31
   access-list sa-acl permit ip 10.1.0.0 0.0.3.255 10.0.0.0
0.255.255.255
   access-list sa-acl permit ip 10.1.0.0 0.0.3.255 192.168.0.0
0.0.255.255
```

```
   access-list sa-acl permit ip 10.1.0.0 0.0.3.255 172.16.0.0
0.15.255.255
   access-list sa-acl permit ip 10.0.0.0 0.255.255.255 10.1.0.0
0.0.3.255
   access-list sa-acl permit ip 172.16.0.0 0.15.255.255 10.1.0.0
0.0.3.255
   access-list sa-acl permit ip 192.168.0.0 0.0.255.255 10.1.0.0
0.0.3.255
   access-list sa-acl permit ip any 239.192.0.0 0.0.255.255
keyserver2#
```

!!! The following output shows the database synced with primary. !!!

```
keyserver2#sh crypto gdoi ks members
Group Member Information :
Number of rekeys sent for group GROUP-VPN : 0   // This is maintained
only in primary key server //
Group Member ID   : 10.10.10.14
Group ID          : 1234
Group Name        : GROUP-VPN
Key Server ID     : 10.10.10.56   // GM registered with the secondary
key server //
Rekeys sent       : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0
Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0
Group Member ID   : 10.10.10.30
Group ID          : 1234
Group Name        : GROUP-VPN
Key Server ID     : 10.10.10.56
Rekeys sent       : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0
Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0
Group Member ID   : 10.10.10.9
Group ID          : 1234
Group Name        : GROUP-VPN
Key Server ID     : 10.10.10.23      // GM registered with primary //
Rekeys sent       : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0
Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0
Group Member ID   : 10.10.10.18
Group ID          : 1234
Group Name        : GROUP-VPN
Key Server ID     : 10.10.10.23
Rekeys sent       : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0
Sent seq num :    0    0    0    0
```

```
    Rcvd seq num :    0    0    0    0
```

!!! The following output shows the secondary key server is using the policy provided by primary key server. !!!

```
    keyserver2#sh crypto gdoi ks policy
    Key Server Policy:
    For group GROUP-VPN (handle: 2147483650) server 10.10.10.56 (handle:
    2147483650):
    For group GROUP-VPN (handle: 2147483650) server 10.10.10.23 (handle:
    2147483651):
      # of teks : 1  Seq num : 0
      KEK POLICY (transport type : Unicast)
        spi : 0x33D3E4913368171A2FCB3A3FB77B521
        management alg     : disabled    encrypt alg       : 3DES
        crypto iv length   : 8           key size          : 24
        Remaining life(sec): 8618        orig lifetime(sec): 10800
        sig hash algorithm : enabled     sig key length    : 1024
        sig size           : 128
        sig key name       : rekeyrsa
      TEK POLICY (encaps : ENCAPS_TUNNEL)
        spi                : 0x66D60BBC    access-list           : sa-acl
        # of transforms    : 0             transform             :
    ESP_3DES
        hmac alg           : HMAC_AUTH_SHA
        alg key size       : 24            sig key size          : 20
        orig life(sec)     : 3600          remaining life(sec)   : 3420
        override life (sec): 0             antireplay window size: 5
      Replay Value 1626655.23 secs
    keyserver2#
```

!!! The following output confirms the secondary key server didn't send any rekeys. !!!

```
    keyserver2#sh crypto gdoi ks rekey
    Group GROUP-VPN (Unicast)
        Number of Rekeys sent               : 0
        Number of Rekeys retransmitted      : 0
        KEK rekey lifetime (sec)            : 10800
            Remaining lifetime (sec)        : 8589
        Retransmit period                   : 10
        Number of retransmissions           : 2
        IPSec SA 1  lifetime (sec)          : 3600
            Remaining lifetime (sec)        : 3391
    keyserver2#
    keyserver2#sh crypto gdoi ks replay
    Anti-replay Information For Group GROUP-VPN:
      Timebased Replay:
        Replay Value             : 1626693.90 secs
        Remaining sync time      : 0 secs
```

!!! The following output shows the co-op statistics with the primary key server. !!!

```
    keyserver2#sh crypto gdoi ks coop
    Crypto Gdoi Group Name :GROUP-VPN
            Group handle: 2147483650, Local Key Server handle: 2147483650
```

```
                Local Address: 10.10.10.56
                Local Priority: 75
                Local KS Role: Secondary , Local KS Status: Alive
                Secondary Timers:
                        Sec Primary Periodic Time: 30
                        Remaining Time: 21, Retries: 0
                        Antireplay Sequence Number: 77
                Peer Sessions:
                Session 1:
                        Server handle: 2147483651
                        Peer Address: 10.10.10.23
                        Peer Priority: 100
                        Peer KS Role: Primary   , Peer KS Status: Alive
                        Antireplay Sequence Number: 15742
                        IKE status: Established
                        Counters:
                            Ann msgs sent: 73
                            Ann msgs sent with reply request: 4
                            Ann msgs recv: 30737
                            Ann msgs recv with reply request: 0
                            Packet sent drops: 7
                            Packet Recv drops: 1
                            Total bytes sent: 83587
                            Total bytes recv: 20162280
    keyserver2#
```

Group Member 1

```
    group-member1#sh crypto isakmp sa
    IPv4 Crypto ISAKMP SA
    dst             src             state          conn-id slot status
    172.16.10.1  10.10.10.42    QM_IDLE           1003    0 ACTIVE
    // Management Tunnel //
    10.10.10.23    10.10.10.42    GDOI_IDLE         1004    0 ACTIVE
    // GDOI Registration Success //
    10.10.10.42    10.10.10.23    GDOI_REKEY        1005    0 ACTIVE
    // Unicast rekey policy //
    IPv6 Crypto ISAKMP SA
    group-member1#
    group-member1#sh crypto session detail
    Crypto session current status
    Code: C—IKE Configuration mode, D—Dead Peer Detection
    K—Keepalives, N—NAT-traversal, X—IKE Extended Authentication
    Interface: FastEthernet0/0
    Session status: UP-NO-IKE
    Peer:  port 848 fvrf: (none) ivrf: (none) // SA detail for GET VPN //
          Desc: (none)
          Phase1_id: (none)
      IPSEC FLOW: permit ip 192.168.0.0/255.255.0.0 10.1.0.0/255.255.252.0
            Active SAs: 2, origin: crypto map
            Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4595156/1528
            Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4595156/1528
```

```
  IPSEC FLOW: permit ip 10.1.0.0/255.255.252.0 192.168.0.0/255.255.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4414026/1528
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4414026/1528
  IPSEC FLOW: permit ip 172.16.0.0/255.240.0.0 10.1.0.0/255.255.252.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4570071/1528
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4570071/1528
  IPSEC FLOW: permit ip 10.1.0.0/255.255.252.0 172.16.0.0/255.240.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4537173/1528
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4537173/1528
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 239.192.0.0/255.255.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4547197/1528
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4547197/1528
  IPSEC FLOW: permit ip 10.0.0.0/255.0.0.0 10.1.0.0/255.255.252.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4487481/1528
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4487481/1528
  IPSEC FLOW: permit ip 10.1.0.0/255.255.252.0 10.0.0.0/255.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 128 drop 0 life (KB/Sec) 4518234/1528
        Outbound: #pkts enc'ed 130 drop 0 life (KB/Sec) 4518230/1528
Interface: FastEthernet0/0
Uptime: 00:05:31
Session status: UP-ACTIVE
Peer: 172.16.10.1 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: mgmt-gw.cisco.com
      Desc: (none)
  IKE SA: local 10.10.10.42/500 remote 172.16.10.1/500 Active
          Capabilities:D connid:1003 lifetime:23:53:18
  IPSEC FLOW: permit ip host 10.1.3.1 172.16.1.96/255.255.255.224
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 10 drop 0 life (KB/Sec) 2487/3268
// Management tunnel //
        Outbound: #pkts enc'ed 10 drop 16 life (KB/Sec) 2487/3268
Interface: FastEthernet0/0
Session status: DOWN           // SAs excluded from TEK encryption //
Peer:  port 500 fvrf: (none) ivrf: (none)
      Desc: (none)
      Phase1_id: (none)
  IPSEC FLOW: deny ip 172.16.1.96/255.255.255.224
10.1.0.0/255.255.252.0
        Active SAs: 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
  IPSEC FLOW: deny ip 10.1.0.0/255.255.252.0
172.16.1.96/255.255.255.224
        Active SAs: 0, origin: crypto map
```

```
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
  IPSEC FLOW: deny ip 0.0.0.0/0.0.0.0 host 239.192.1.190
        Active SAs: 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
Interface: FastEthernet0/0
Uptime: 00:04:52
Session status: UP-IDLE
Peer: 10.10.10.23 port 848 fvrf: (none) ivrf: (none)
      Phase1_id: keyserver1.cisco.com
      Desc: (none)
  IKE SA: local 10.10.10.42/848 remote 10.10.10.23/848 Active
          Capabilities:D connid:1004 lifetime:23:54:58
  IKE SA: local 10.10.10.42/848 remote 10.10.10.23/848 Active
          Capabilities:(none) connid:1006 lifetime:7w0d
  IKE SA: local 10.10.10.42/848 remote 10.10.10.23/848 Active
          Capabilities:(none) connid:1005 lifetime:7w0d
group-member1#
```

!!! This cli gives overall info about the group member. !!!

```
group-member1#sh crypto gdoi
Group Information
    Group Name               : getvpn
    Group Identity           : 1234
    Rekeys received          : 16
    IPSec SA Direction       : Both
    ACL Received From KS     : gdoi_group_getvpn_temp_acl
    Active Group Server      : 10.10.10.23
    Group Server list        : 10.10.10.23
                               10.10.10.56
```

!!! Group member related outputs can be derived using “show crypto gdoi gm” cli. !!!

```
group-member1#sh crypto gdoi gm ?
  acl     Show ACL applied to GDOI group
  rekey   Show rekey information
  replay  Display group information for time-based antireplay
  |       Output modifiers
  <cr>
```

!!! This cli gives the output of policies downloaded from the key server. !!!

```
group-member1#sh crypto gdoi gm acl
Group Name: getvpn
 ACL Downloaded From KS 10.10.10.23:
   access-list  deny ip any host 239.192.1.190
   access-list  deny ip 10.1.3.0 0.0.0.31 172.16.1.96 0.0.0.31
   access-list  deny ip 172.16.1.96 0.0.0.31 10.1.3.0 0.0.0.31
   access-list  permit ip 10.1.0.0 0.0.3.255 10.0.0.0 0.255.255.255
   access-list  permit ip 10.1.0.0 0.0.3.255 192.168.0.0 0.0.255.255
   access-list  permit ip 10.1.0.0 0.0.3.255 172.16.0.0 0.15.255.255
   access-list  permit ip 10.0.0.0 0.255.255.255 10.1.0.0 0.0.3.255
```

```
   access-list  permit ip 172.16.0.0 0.15.255.255 10.1.0.0 0.0.3.255
   access-list  permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.3.255
   access-list  permit ip any 239.192.0.0 0.0.255.255
 ACL Configured Locally:
  Map Name: gdoi
   access-list no-encryption-acl deny ip host 10.10.10.42 host
10.10.10.41
   access-list no-encryption-acl deny ip 10.1.1.0 0.0.0.255 host
10.10.10.23
   access-list no-encryption-acl deny ip any host 239.192.1.190
group-member1#
```

!!! This cli shows the rekeys received and acks sent for this group member. !!!

```
group-member1#sh crypto gdoi gm rekey
Group getvpn (Unicast)
    Number of Rekeys received (cumulative)       : 16
    Number of Rekeys received after registration : 16
    Number of Rekey Acks sent                    : 16
group-member1#
```

!!! This cli shows the replay statistics for this group member. !!!

```
group-member1#sh crypto gdoi gm replay
Anti-replay Information For Group getvpn:
  Timebased Replay:
    Replay Value             : 959903.19 secs
    Input Packets            : 32837    Output Packets           :
22738
    Input Error Packets      : 0        Output Error Packets     : 0
    Time Sync Error          : 0        Max time delta           :
0.05 secs
```

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

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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

ETMG_206862.BR 1/07