Cisco Group Encrypted Transport VPN

First Published: November 17, 2006
Last Updated: October 2, 2011

Note Effective with Cisco IOS 12.4(11)T, the Multicast Rekeying feature information (originally published as Cisco IOS Release 12.4(6)T [titled *Secure Multicast*]) has been integrated into this document.

Today's networked applications, such as voice and video, are accelerating the need for instantaneous, branch-interconnected, and Quality of Service- (QoS-) enabled WANs. The distributed nature of these applications results in increased demands for scale. At the same time, enterprise WAN technologies force businesses to trade off between QoS-enabled branch interconnectivity and transport security. As network security risks increase and regulatory compliance becomes essential, Cisco Group Encrypted Transport VPN (GET VPN) eliminates the need to compromise between network intelligence and data privacy.

GET VPN eliminates the need for tunnels. By removing the need for point-to-point tunnels, meshed networks are able to scale higher while maintaining network-intelligence features that are critical to voice and video quality, such as QoS, routing, and multicast. GET VPN offers a new standards-based IP security (IPsec) security model that is based on the concept of "trusted" group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship.

GET VPN is a set of features that are necessary to secure IP multicast group traffic or unicast traffic over a private WAN that originates on or flows through a Cisco IOS device. GET VPN combines the keying protocol Group Domain of Interpretation (GDOI) with IPsec encryption to provide users with an efficient method to secure IP multicast traffic or unicast traffic. GET VPN enables the router to apply encryption to nontunneled (that is, "native") IP multicast and unicast packets and eliminates the requirement to configure tunnels to protect multicast and unicast traffic.

Cisco Group Encrypted Transport VPN provides the following benefits:

- Provides data security and transport authentication, helping to meet security compliance and internal regulation by encrypting all WAN traffic
- Enables high-scale network meshes and eliminates complex peer-to-peer key management with group encryption keys
- For Multiprotocol Label Switching (MPLS) networks, maintains network intelligence (such as full-mesh connectivity, natural routing path, and QoS]

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

- Grants easy membership control with a centralized key server
- Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub
- Reduces traffic loads on customer premises equipment (CPE) and provider-edge (PE) encryption devices by using the core network for replication of multicast traffic, avoiding packet replication at each individual peer site

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Cisco Group Encrypted Transport VPN" section on page 71.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Prerequisites for Cisco Group Encrypted Transport VPN

- You must be using Cisco IOS Release 12.4(11)T.
- The following Cisco VPN acceleration modules are supported:
  - Cisco AIM-VPN/SSL Module for Cisco integrated services routers
  - Cisco VPN acceleration Module 2+ for Cisco 7200 series routers and 7301 routers
- You should be knowledgeable about IPsec and Internet Key Exchange (IKE).
- You should know how to configure multicast and unicast routing on a Cisco IOS global router.
- When configuring the IKE policy, the IKE lifetime should be set to the minimum of 5 minutes so that unnecessary resources are not wasted on the maintenance of the IKE security association (SA). After the registration IKE SA is established, the registration SAs no longer have to be maintained because the rekey SA has been created and will be used to accept future rekeys.

Restrictions for Cisco Group Encrypted Transport VPN

- The following platforms can be configured only as shown:
  - Cisco 870 series routers: as a group member only
- If you are encrypting high packet rates for count-based anti-replay, ensure that you do not make the lifetime too long or it can take several hours for the sequence number to wrap. For example, if the packet rate is 100 kilopackets per second, the lifetime should be configured as less than 11.93 hours so that the SA is used before the sequence number wraps.

Information About Cisco Group Encrypted Transport VPN

To configure GET VPN, you should understand the following concepts:

- Cisco Group Encrypted Transport VPN Overview, page 3
- Cisco Group Encrypted Transport VPN Architecture, page 4
- Cisco Group Encrypted Transport VPN Features, page 10
- End-User Considerations, page 18
- System Error Messages, page 18

Cisco Group Encrypted Transport VPN Overview

Today's networked applications, such as voice and video, are accelerating the necessity for instantaneous, branch-interconnected, and QoS-enabled WANs. And the distributed nature of these applications results in increased demands for scale. At the same time, enterprise WAN technologies force businesses to trade off between QoS-enabled branch interconnectivity and transport security. As network security risks increase and regulatory compliance becomes essential, GET VPN, a next-generation WAN encryption technology, eliminates the need to compromise between network intelligence and data privacy.

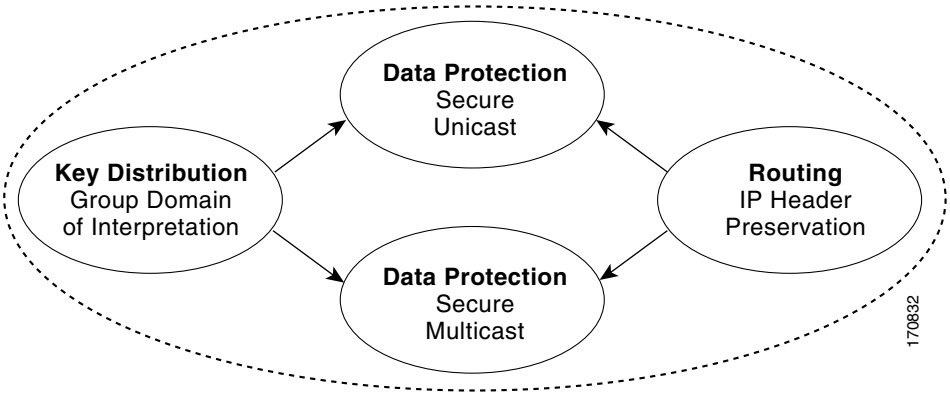
With the introduction of GET, Cisco now delivers a new category—tunnel-less VPN—that eliminates the need for tunnels. By removing the need for point-to-point tunnels, meshed networks can scale higher while maintaining network-intelligence features critical to voice and video quality. GET offers a new standards-based security model that is based on the concept of "trusted" group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship. By using trusted groups instead of point-to-point tunnels, "any-any" networks can scale higher while maintaining network-intelligence features (such as QoS, routing, and multicast), which are critical to voice and video quality.

GET-based networks can be used in a variety of WAN environments, including IP and Multiprotocol Label Switching (MPLS). MPLS VPNs that use this encryption technology are highly scalable, manageable, and cost-effective, and they meet government-mandated encryption requirements. The flexible nature of GET allows security-conscious enterprises either to manage their own network security over a service provider WAN service or to offload encryption services to their providers. GET simplifies securing large Layer 2 or MPLS networks that require partial or full-mesh connectivity.

Cisco Group Encrypted Transport VPN Architecture

GET VPN is an enhanced solution that encompasses Multicast Rekeying, a Cisco solution for enabling encryption for "native" multicast packets, and unicast rekeying over a private WAN. Multicast Rekeying and GET VPN is based on GDOI as defined in Internet Engineering Task Force (IETF) RFC 3547. In addition, there are similarities to IPsec in the area of header preservation and SA lookup. Dynamic distribution of IPsec SAs has been added, and tunnel overlay properties of IPsec have been removed. Figure 1 further illustrates the concepts of GET VPN and their relationships among one another.

Figure 1 GET VPN Concepts and Relationships



This section includes the following subsections:

Key Distribution: Group Domain of Interpretation

GDOI

GDOI is defined as the Internet Security Association Key Management Protocol (ISAKMP) Domain of Interpretation (DOI) for group key management. In a group management model, the GDOI protocol operates between a group member and a group controller or key server (GCKS), which establishes security associations (SAs) among authorized group members. The ISAKMP defines two phases of negotiation. GDOI is protected by a Phase 1 ISAKMP security association. The Phase 2 exchange is defined in IETF RFC 3547. The topology shown in Figure 2 and the corresponding explanation show how this protocol works.

Group Member

The group member registers with the key server to get the IPsec SA or SAs that are necessary to communicate with 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, and before the current IPsec SAs expire, so that there is no loss of traffic.

Key Server

The responsibilities of the key server include maintaining the policy and creating and maintaining the keys for the group. When a group member registers, the key server downloads this policy and the keys to the group member. The key server also rekeys the group before existing keys expire.

The key server has two modes: servicing registration requests and sending rekeys. A group member can register at any time and receive the most current policy and keys. When a group member registers with the key server, the key server verifies the group ID that the group member is attempting to join. If this ID is a valid group ID, the key server sends the SA policy to the group member. After the group member acknowledges that it can handle the downloaded policy, the key server downloads the respective keys.

There are two types of keys that the key server can download: the key encryption key (KEK) and the traffic encryption key (TEK). The TEK becomes the IPsec SA with which the group members within the same group communicate. The KEK encrypts the rekey message.

The GDOI server sends out rekey messages either because of an impending IPsec SA expiration or because the policy has changed on the key server (using command-line interface [CLI]). The rekey messages may also be retransmitted periodically to account for possible packet loss. Packet loss can occur because rekey messages are sent without the use of any reliable transport. There is no efficient feedback mechanism by which receivers can indicate that they did not receive a rekey message, so retransmission seeks to bring all receivers up to date.

Figure 2 Protocol Flows That Are Necessary for Group Members to Participate in a Group

The above topology shows the protocol flows that are necessary for group members to participate in a group, which are as follows:

1. Group members register with the key server. The key server authenticates and authorizes the group members and downloads the IPsec policy and keys that are necessary for them to encrypt and decrypt IP multicast packets.
2. Group members exchange IP multicast packets that are encrypted using IPsec.
3. As needed, the key server “pushes” a rekey message to the group members. The rekey message contains new IPsec policy and keys to use when old IPsec SAs expire. Rekey messages are sent in advance of the SA expiration time to ensure that valid group keys are always available.

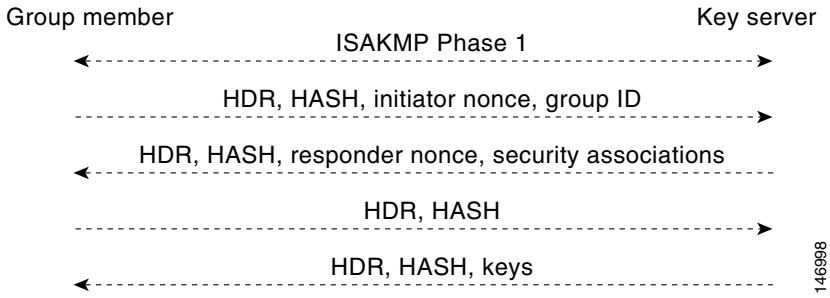
How Protocol Messages Work with the Cisco IOS

Multicast Rekeying uses the GDOI protocol (IETF RFC 3547) to distribute the policy and keys for the group. The GDOI protocol is between a key server and a group member. The key server creates and maintains the policy and keys, and it downloads the policy and keys to the authenticated group members. The group members are authenticated by the key server and communicate with other authenticated group members that are in the same group using the IPsec SAs that the group members have received from the key server.

The GDOI protocol is protected by an ISAKMP Phase 1 exchange. The GDOI key server and the GDOI group member must have the same ISAKMP policy. This Phase 1 ISAKMP policy should be strong enough to protect the GDOI protocol that follows. The GDOI protocol is a four-message exchange that follows the Phase 1 ISAKMP policy. The Phase 1 ISAKMP exchange can occur in main mode or aggressive mode.

Figure 3 shows the ISAKMP Phase 1 exchange.

Figure 3 ISAKMP Phase 1 Exchange and GDOI Registration



The above messages (the ISAKMP Phase 1 messages and the four GDOI protocol messages) are referred to as the GDOI registration, and the entire exchange that is shown above is a unicast exchange between the group member and the key server.

After the registration is successful, the key server sends a multicast rekey to all the group members that have registered within a group. During the registration, the group member receives the address of the multicast group and registers with the multicast group that is required to receive the multicast rekeys.

Note The GDOI protocol uses User Datagram Protocol (UDP) port 848 (with Network Address Translation-Traversal (NAT-T), it floats to 4500).

IPsec

IPsec is a well-known RFC that defines an architecture to provide various security services for traffic at the IP layer. The components and how they fit together with each other and into the IP environment are described in IETF RFC 2401.

Communication Flow Between Key Servers and Group Members to Update IPsec SAs

Key servers and group members are the two components of the GET VPN architecture. The key server holds and supplies group authentication keys and IPsec SAs to the group members.

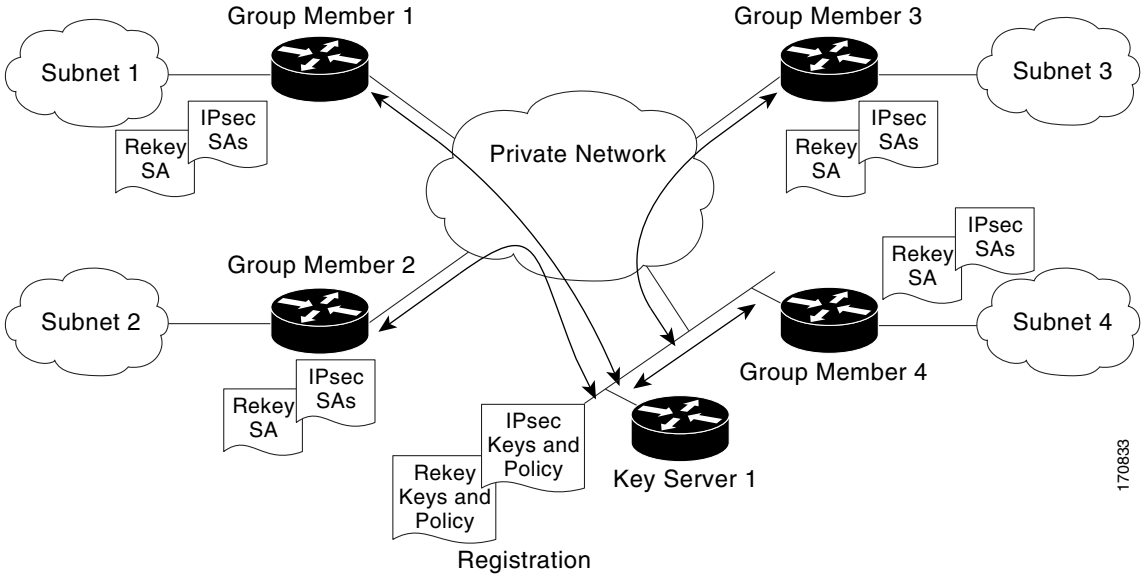
Group members provide encryption service to the interesting traffic (traffic that is worthy of being encrypted and secured by IPsec).

Communication among the key server and group members is encrypted and secured. GDOI supports the use of two keys: The TEK and the KEK. The TEK is downloaded by the key server to all the group members. The downloaded TEK is used by all the group members to communicate securely among each other. This key is essentially the group key that is shared by all the group members. The group policies and IPsec SAs are refreshed by the key server using periodic rekey messages to the group members. The KEK is also downloaded by the key server and is used by the group members to decrypt the incoming rekey messages from the key server.

The key server generates the group policy and IPsec SAs for the GDOI group. The information generated by the key server includes multiple TEK attributes, traffic encryption policy, lifetime, source and destination, a Security Parameter Index (SPI) ID that is associated with each TEK, and the rekey policy (one KEK).

Figure 4 illustrates the communication flow between group members and the key server. The key server, after receiving registration messages from a group member, generates the information that contains the group policy and new IPsec SAs. The new IPsec SA is then downloaded to the group member. The key server maintains a table that contains the IP address of each group member per group. When a group member registers, the key server adds its IP address in its associated group table, thus allowing the key server to monitor an active group member. A key server can support multiple groups. A group member can be part of multiple groups.

Figure 4 Communication Flow Between Group Members and the Key Server



IPsec and ISAKMP Timers

IPsec and ISAKMP SAs are maintained by the following timers:

- TEK lifetime—Determines the lifetime of the IPsec SA. Before the end of the TEK lifetime, the key server sends a rekey message, which includes a new TEK encryption key and transforms as well as the existing KEK encryption keys and transforms. The TEK lifetime is configured only on the key server, and the lifetime is "pushed down" to the group members using the GDOI protocol. The TEK lifetime value depends on the security policy of the network. If the **set security-association lifetime** command is not configured, the default value of 86400 seconds takes effect. To configure a TEK lifetime, see the "Setting up an IPsec Lifetime Timer" section on page 27.

- KEK lifetime—Determines the lifetime of the GET VPN rekey SAs. Before the end of the lifetime, the key server sends a rekey message, which includes a new KEK encryption key and transforms as well as new TEK encryption keys and transforms. The KEK lifetime is configured only on the key server, and the lifetime is pushed down to group members dynamically using the GDOI protocol. The KEK lifetime value must greater than the TEK lifetime value (it is recommended that the KEK lifetime value be at least three times greater than the TEK lifetime value). If the **rekey lifetime** command is not configured, the default value of 86400 seconds takes effect. To configure a KEK lifetime, see the "Setting up a Multicast Rekey" section on page 24.
- ISAKMP SA lifetime—Defines how long each ISAKMP SA should exist before it expires. The ISAKMP SA lifetime is configured on a group member and on the key server. If the group members and key servers do not have a cooperative key server, the ISAKMP SA is not used after the group member registration. In this case (no cooperative key server), the ISAKMP SA can have a short lifetime (a minimum of 60 seconds). If there is a cooperative key server, all key servers must have long lifetimes to keep the ISAKMP SA "up" for cooperative key server communications. If the **lifetime** command is not configured, the default value of 86400 seconds takes effect. To configure an ISAKMP SA lifetime, see the "Setting up an ISAKMP Lifetime Timer" section on page 28.

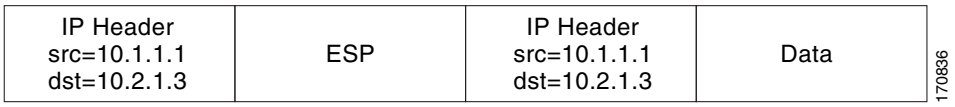
Routing

GET VPN routing is explained in the following section.

Header Preservation

As shown in Figure 5, IPsec-protected data packets carry the original source and destination in the outer IP header rather than replacing them with tunnel endpoint addresses. This technique is known as IPsec Tunnel Mode with Address Preservation.

Figure 5 Header Preservation



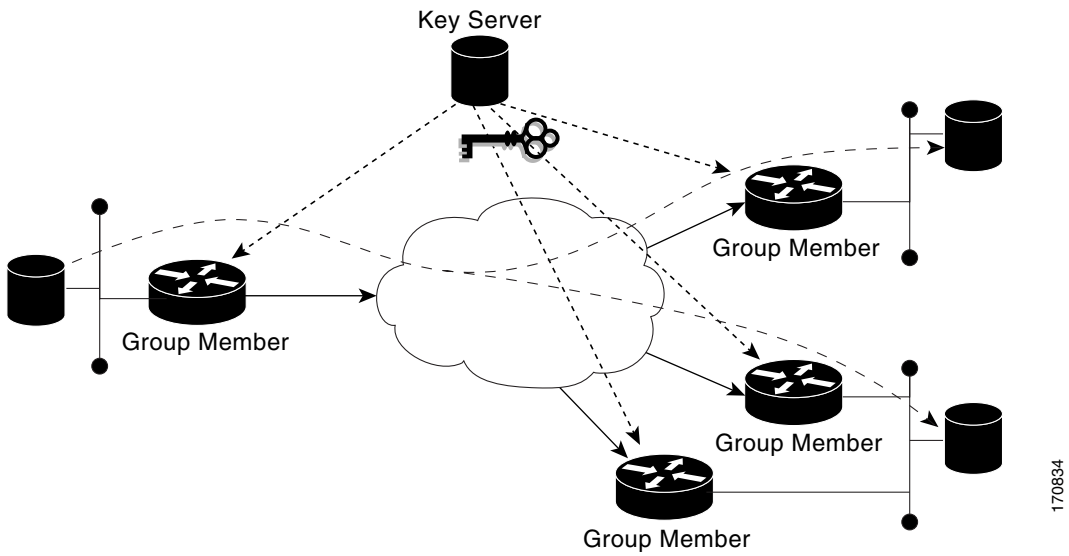
Address preservation allows GET VPN to use the routing functionality present within the core network. Address preservation allows routing to deliver the packets to any customer-edge device (CE) in the network that advertises a route to the destination address. Any source and destination matching the policy for the group will be treated in a similar manner. In the situation where a link between IPsec peers is not available, address preservation also helps combat traffic "black-hole" situations.

Header preservation also maintains routing continuity throughout the enterprise address space and in the WAN. As a result, end host addresses of the campus are exposed in the WAN (for MPLS, this applies to the edge of the WAN). For this reason, GET VPN is applicable only when the WAN network acts as a "private" network (for example, in a MPLS network).

Secure Data Plane Multicast

The multicast sender uses the TEK that is obtained from the key server and encrypts the multicast data packet with header preservation before it switches out the packet. The replication of the multicast packet is carried out in the core on the basis of the (S,G) state that is retained in the multicast data packet. This process is illustrated in Figure 6.

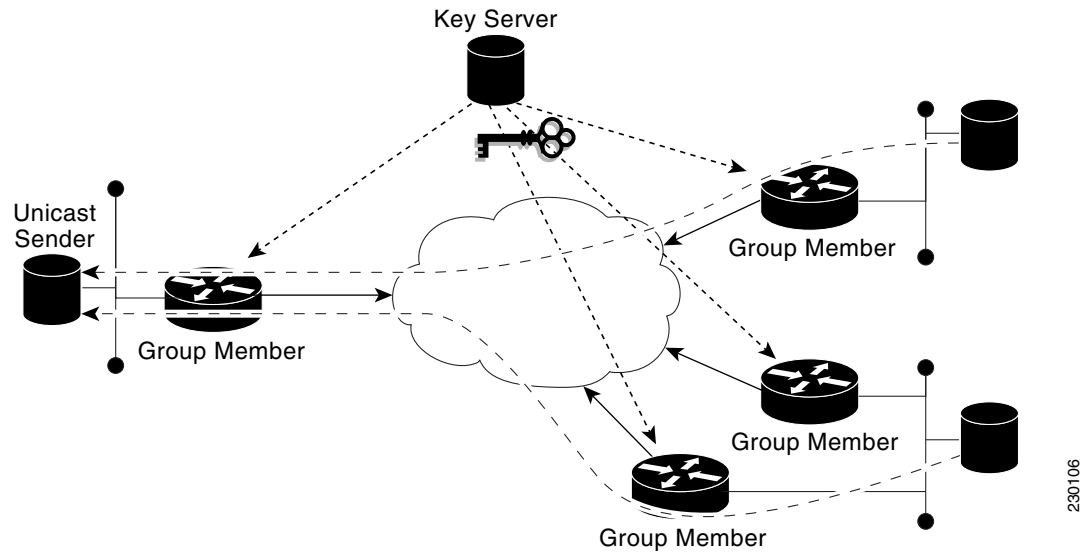
Figure 6 Secure Data Plane Multicast Process



Secure Data Plane Unicast

The unicast sender uses the TEK that is obtained from the key server and encrypts the unicast data packet with header preservation before it switches out the packet to the destination. This process is illustrated in Figure 7.

Figure 7 Secure Data Plane Unicast Process



Cisco Group Encrypted Transport VPN Features

This section includes the following subsections:

Rekeying

Rekey messages are used to refresh IPsec SAs. When the IPsec SAs or the rekey SAs are about to expire, one single rekey message for a particular group is generated on the key server. No new IKE sessions are created for the rekey message distribution. The rekey messages are distributed by the key server over an existing IKE SA.

Rekeying can use multicast or unicast messages. GET VPN supports both unicast and multicast rekeying.

Multicast Rekeying

Multicast rekeys are sent out using an efficient multicast rekey. Following a successful registration, the group member registers with a particular multicast group. All the group members that are registered to the group receives this multicast rekey. Multicast rekeys are sent out periodically on the basis of the configured lifetime on the key server. Multicast rekeys are also sent out if the IPsec or rekey policy is changed on the key server. Triggered by the configuration change, the rekey sends out the new updated policy to all the group members with an efficient multicast rekey.

Unicast Rekeying and SAs

In a large unicast group, to alleviate latency issues, the key server generates rekey messages for only a small number of group members at a time. The key server is ensured that all group members receive the same rekey messages for the new SA before the expiration of the old SA. Also, in a unicast group, after receiving the rekey message from the key server, a group member sends an encrypted acknowledge (ACK) message to the key server using the keys that were received as part of the rekey message. When the key server receives this ACK message, it notes this receipt in its associated group table, which accomplishes the following:

- The key server keeps a current list of active group members.
- The key server sends rekey messages only to active members.

In addition, in a unicast group, the key server removes the group member from its active list and stops sending the rekey messages to that particular group member if the key server does not receive an ACK message for three consecutives rekeys. If no ACK message is received for three consecutive rekeys, the group member has to fully reregister with the key server after its current SA expires if the group member is still interested in receiving the rekey messages. The ejection of a nonresponsive group member is

accomplished only when the key server is operating in the unicast rekey mode. The key server does not eject group members in the multicast rekey mode because group members cannot send ACK messages in that mode.

As in multicast rekeying, if retransmission is configured, each rekey will be retransmitted the configured number of times.

Rekey transport modes and authentication can be configured under a GDOI group.

If unicast rekey transport mode is not defined, multicast is applied by default.

If the TEK rekey is not received, the group member reregisters with the key server in a maximum of 5% of the TEK lifetime or 60 seconds before the current IPsec SA expires. The key server has to send out the rekey before the group member reregistration occurs. If no retransmission is configured, the key server sends the rekey 90 seconds before the SA expires. If retransmission is configured, the rekey occurs earlier thant 90 seconds to let the last retransmission be sent 90 seconds before the SA expires.

The key server uses the formula in the example below to calculate when to start sending the rekey to all unicast group members. The unicast rekey process on the key server sends rekeys to unicast group members in groups of 50 within a loop. The time spent within this loop is estimated to be 5 seconds.

A key server rekeys group members in groups of 50, which equals two loops. For example, for 100 group members:

Number of rekey loops = (100 group members)/50 = 2 loops

Time it takes to rekey one loop (estimation) = 5 seconds

Time to rekey 100 group members in two loops of 50: 2 * 5 seconds = 10 seconds

So, the key server pushes the rekey time back as follows:

If the TEK timeout is 300: 300 - 10 = 290

But, the start has to be earlier than the TEK expiry (as in the multicast case).

So, 90 seconds is subtracted from the actual TEK time: 290 - 90 = 200 seconds.

If retransmissions are configured, the rekey timer is moved back more.

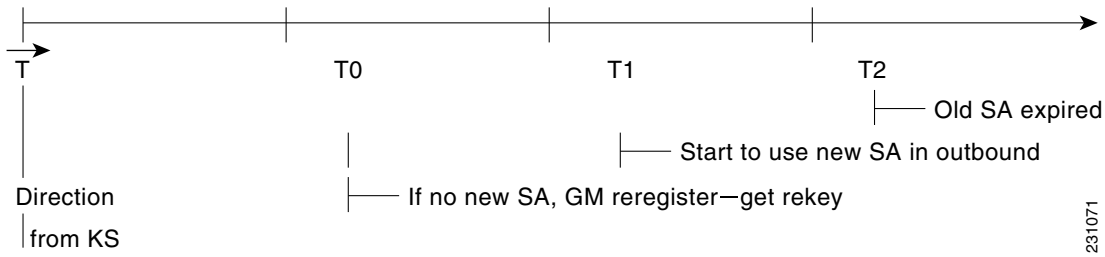
For three retransmissions every 10 seconds: 200 - (3 * 10) = 170.

IPsec SA Usage on the Group Members

When a rekey is received and processed on a group member, the new IPsec SA (the Security Parameter Index [SPI]) is installed. There is a period of time when the old and the new IPsec SAs are used. After a certain specified interval, the old IPsec SA is deleted. This overlap is ensures that all group members receive the current rekey and insert the new IPsec SAs. This behavior is independent of the transport method (multicast or unicast rekey transport) for the rekeys from the key server.

On the group member, approximately 30 seconds before the old SA expires, the group member starts to use the new SA in the outbound direction to encrypt the packet. Approximately 60 seconds before the old SA expires, if no new SA is received on the group member side via a rekey from the key server, the group member reregisters.

Figure 8 IPsec SA Usage on a Group Member



In Figure 8, time T2 is when the old SA expires. T1 is 30 seconds before T2, which is when the group member (GM) starts to use the new SA in the outbound direction. T0 is another 30 seconds before T2. If no new SA is received at T0, the group member has to reregister. T is another 30 seconds from T0. The key server (KS) should send a rekey at T.

Configuration Changes Can Trigger a Rekey By a Key Server

Configuration changes on a key server can trigger a rekey by the key server. Please refer to the following sample configuration as you read through the events that will or will not cause a rekey.

```
crypto ipsec transform-set gdoi-p esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-p
 set security-association lifetime seconds 900
set transform-set gdoi-p
!
crypto gdoi group diffint
 identity number 3333
 server local
  rekey algorithm aes 128
  rekey address ipv4 121
  rekey lifetime seconds 3600
  no rekey retransmit
  rekey authentication mypubkey rsa mykeys
  sa ipsec 1
   profile gdoi-p
   match address ipv4 120
   replay counter window-size 3
```

Changes That Will Trigger a Rekey on a Key Server

- Any change in the TEK configuration (“sa ipsec 1” in the above example).
  - If the ACL (“match address ipv4 120” in the above example) is changed. Any addition, deletion, or change in the ACL causes a rekey.
  - If TEK replay is enabled or disabled on the key server, rekey is sent. Reconfiguring the replay window size does not trigger a rekey.
  - Removal or addition of the IPsec profile in the TEK (“profile gdoi-p” in the above example).
  - Changing from multicast to unicast transport.
  - Changing from unicast to multicast transport.

Changes That Will Not Trigger a Rekey on a Key Server

The following configuration changes on the key server will not trigger a rekey from the key server:

- Replay counter window size is changed under the TEK (“sa ipsec 1” in the above example).

- Changing the IPsec transform in the transform set.
- Configuring or removing rekey retransmit.
- Removing or configuring the rekey ACL.
- Changing the TEK lifetime ("set security-association lifetime seconds 300" in the above example) or changing the KEK lifetime ("rekey lifetime seconds 500" in the above example).
- Adding, deleting, or changing the rekey algorithm ("rekey algorithm aes 128" in the above example).

Group Member Access Control List

For GET VPN, the traffic that has to be protected is defined statically on the key server using the access control list (ACL). The group member gets information about what has to be protected from the key server. This structure allows the key server to choose and change the policy dynamically as needed. In Secure Multicast, the key server ACL is defined inclusively. The ACL includes only the exact traffic that should be encrypted, with an implicit deny causing all other traffic to be allowed in the clear (that is, if there is no permit, all other traffic is allowed).

GET VPN employs a different philosophy: the definition of which packets should be encrypted is delivered independently. GET VPN supports only statically defined traffic selectors. Policy can be defined by using both deny and permit ACLs on the key server. Only the deny ACL is allowed to be manually configured on a group member. The policies that are downloaded from the key server and configured on the group member are merged. Any ACL that is configured on the group member has predominance over what is downloaded from the key server.

After the group member gets the ACL from the key server, the group member creates a temporary ACL and inserts it into the database. This ACL will be deleted if the group member is removed from the GDOI group for any reason. The packets that are going out of the interface are dropped by the group member if a packet matches the ACL but no IPsec SA exists for that packet.

The key server can send a set of traffic selectors, which may not exactly match the group member ACL on the group member. If such differences occur, the differences have to be merged and resolved. Because the group member is more aware of its topology than the key server, the downloaded ACLs are appended at the end of the group member ACL. The group member ACL (except the implicit deny) is inserted into the database first, followed by the downloaded key server ACL. The database is prioritized, and the database search stops whenever a matched entry is found.

For information about configuring a group member ACL, see "Setting up Group Member ACLs" section on page 26."

Time-Based Anti-Replay

Anti-replay is an important feature in a data encryption protocol such as IPSec (RFC 2401). Anti-replay prevents a third party from eavesdropping on an IPsec conversation, stealing packets, and injecting those packets into a session at a later time. The time-based anti-replay mechanism helps ensure that invalid packets are discarded by detecting the replayed packets that have already arrived at an earlier time.

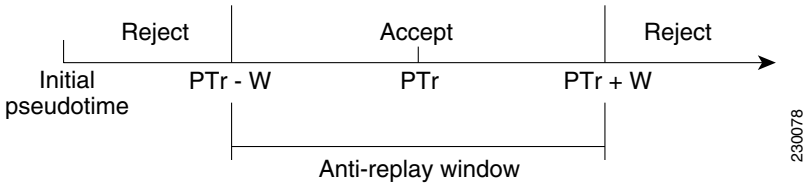
GET VPN uses the Synchronous Anti-Replay (SAR) mechanism to provide anti-replay protection for multisender traffic. SAR is independent of real-world Network Time Protocol (NTP) clock or sequential-counter mechanisms (which guarantee packets are received and processed in order). A SAR clock advances regularly. The time tracked by this clock is called pseudotime. The pseudotime is maintained on the key server and is sent periodically to the group members within a rekey message as a timestamp field called pseudoTimeStamp. GET VPN uses a Cisco proprietary protocol called Metadata to encapsulate the psuedoTimeStamp. Group members have to be resynchronized to the pseudotime of

the key server periodically. The pseudotime of the key server starts ticking from when the first group member registers. Initially, the key server sends the current pseudotime value of the key server and window size to group members during the registration process. New attributes, such as time-based replay-enabled information, window size, and the pseudotime of the keyserver, is sent under the SA payload (TEK).

The group members use the pseudotime to prevent replay as follows: the pseudoTimeStamp contains the pseudotime value at which a sender created a packet. A receiver compares the pseudotime value of senders with its own pseudotime value to determine whether a packet is a replayed packet. The receiver uses a time-based anti-replay "window" to accept packets that contain a timestamp value within that window. The window size is configured on the key server and is sent to all group members.

Figure 9 illustrates an anti-replay window in which the value PTr denotes the local pseudotime of the receiver, and W is the window size.

Figure 9 Anti-Replay Window



Keeping Clocks Synchronized

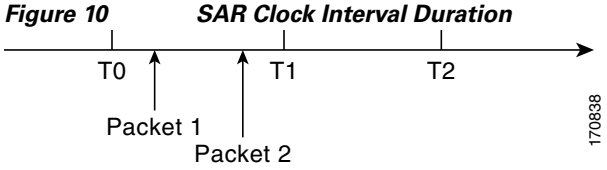
It is possible for the clocks of the group members to slip and lose synchronization with the key server. To keep the clocks synchronized, a rekey message (multicast or unicast, as appropriate), including the current pseudotime value of the key server, is sent periodically (either in a rekey message or at a minimum of every 30 minutes to the group member. If a packet fails this anti-replay check, the pseudotime of both the sender and receiver is printed, an error message is generated, and a count is increased.

To view anti-replay statistics, use the **show crypto gdoi group** *group-name* **gm replay** command on both the sender and receiver devices. If the configuration is changed by the administrator to affect the replay method of the size configuration, the key server initiates a rekey message.

Interval Duration

A tick is the interval duration of the SAR clock. Packets sent in this duration have the same pseudoTimeStamp. The tick is also downloaded to group members, along with the psuedotime from the key server. For example, as shown in Figure 10, packets sent between T0 and T1 would have the same pseudoTimeStamp T0. SAR provides loose anti-replay protection. The replayed packets are accepted if they are replayed during the window. The default window size is 100 seconds. It is recommended that you keep the window size small to minimize packet replay.

Figure 10 SAR Clock Interval Duration



Anti-Replay Configurations

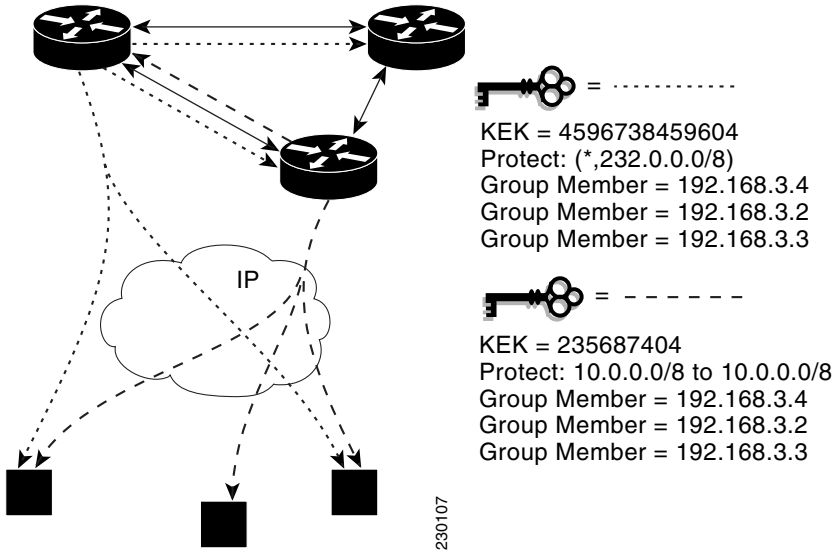
The Anti-Replay feature can be enabled under IPsec SA on a key server by using the following commands:

- **replay time window-size**—Enables the replay time option, which supports the nonsequential, or time-based, mode. The window size is in seconds. Use this mode only if you have more then two group members in a group.
- **replay counter window-size**—Enables sequential mode. This mode is useful if there are only two group members in a group.
- **no replay counter window-size**—Disables anti-replay.

Cooperative Key Server

Figure 11 illustrates cooperative key server key distribution. The text below the illustration explains the Cooperative Key Server feature.

Figure 11 Cooperative Key Server Key Distribution



Cooperative key servers provide redundancy to GET VPN. Multiple key servers are supported by GET VPN to ensure redundancy, high availability, and fast recovery if the primary key server fails. Cooperating GDOI key servers jointly manage the GDOI registrations for the group. Each key server is an active key server, handling GDOI registration requests from group members. Because the key servers are cooperating, each key server distributes the same state to the group members that register with it. Load balancing is achieved because each of the GDOI key servers can service a portion of the GDOI registrations.

The primary key server is responsible for creating and distributing group policy. The primary key server periodically sends out (or broadcasts) group information updates to all other key servers to keep those servers in synchronization. If the secondary key servers somehow miss the updates, they contact the primary key server to directly request information updates. The secondary key servers mark the primary key server as unreachable (that is, "dead") if the updates are not received for an extended period of time.

When a new policy is created on a primary key server, regardless of which key server a group member may be registered with, it is the responsibility of the primary key server to distribute rekey messages to GDOI group members.

Note If you are supporting a large number of group members in your cooperative key server setup (that is, more than 300), you should increase the buffer size by using the **buffers huge size** command.

Announcement Messages

Announcement messages are secured by IKE Phase 1 and are sent as IKE notify messages. Authentication and confidentiality that are provided by IKE is used to secure the messaging between the key servers. Anti-replay protection is provided by the sequence numbers in the announcement messages. Announcement messages are periodically sent from primary to secondary key servers.

Announcement messages include the following components that help maintain the current state.

Sender Priority of a Key Server

This value describes the priority of the sender, which is configurable using the CLI. The key server with the highest priority becomes the primary key server. If the priority values are the same, the key server with the highest IP address becomes the primary key server.

Maintaining the Role of the Sender

During the synchronization period, if the key servers are at geographically dispersed locations, they may suffer a network-partitioning event. If a network-partitioning event occurs, it is possible that more than one key server can become the primary key server for a period of time. When the network is operating normally again and all the key servers find each other, they need to be told the current role of the sender so the key servers can attain their proper roles.

Request for a Return Packet Flag

All messages are defined as one-way messages. When needed, a key server can request the current state from a peer to find out its role and/or request the current state of the group.

Group Policies

The group policies are the policies that are maintained for a group, such as group member information and IPsec SAs and keys.

Anti-replay functionalities and incorporated Cooperative announcement messages are supported. The primary key server updates the pseudotime value, sending it to all secondary key servers in the group. The secondary key servers should synchronize their SAR clocks to this updated value.

Receive Only SA

For multicast traffic using the GDOI protocol, bidirectional SAs are installed. The Receive Only feature enables an incremental deployment so that only a few sites can be verified before bringing up an entire network. To test the sites, one of the group members should send encrypted traffic to all the other group members and have them decrypt the traffic and forward the traffic "in the clear." Receive Only SA mode

allows encryption in only the inbound direction for a period of time. (See the steps below for the Receive Only SA process.) If you configure the **sa receive-only** command on the key server, Steps 2 and 3 happen automatically.

1. Mark IPsec SAs as "receive-only" on the GDOI key server.

   This action allows the group members to install SAs in the inbound direction only. Receive-only SAs can be configured under a crypto group. (See "Setting up the Group ID, Server Type, and SA Type" section on page 20.")

2. Mark GDOI TEK payloads as "receive only."

   If the **sa receive-only** command is configured, all TEKs under this group are going to be marked "receive only" by the key server when they are sent to the group member.

3. Install one-way IPsec flows.

   Every time a GDOI group member receives an IPsec SA from the key server that is marked as "receive only," the group member installs this IPsec SA only in the inbound direction rather than in both incoming and outgoing directions.

4. Test individual group members using the following local-conversion commands:

   - **crypto gdoi gm ipsec direction inbound optional**
   - **crypto gdoi gm ipsec direction both**

Local Conversion

First, individually convert each of the group members to passive mode (this change tells the outbound check that there is a valid SA) and then to bi-directional mode.

5. Globally convert from "receive only" to "receive and send."

   The following method can be used when the testing phase is over and "receive only" SAs have to be converted to bi-directional SAs.

Global Conversion

Remove the **sa receive-only** command under the group. Removing the **sa receive-only** command creates new IPsec SAs for this group and causes a rekey. On receipt, group members reinstall the SA in both directions and begin to use it in passive mode. Because the SA cannot remain in passive mode forever, the group members change those SAs to receive or send mode if there is no rekey in 5 minutes. The conversion from passive mode to bidirectional encryption mode is automatic and does not require the administrator to do anything.

Enhanced Solutions Manageability

Several **show** and **debug** commands are supported to help verify functionality. See the "Verifying and Troubleshooting Cisco Group Encrypted Transport VPN" section on page 34 for the details.

Support with VRF-Lite Interfaces

VRF-Lite application supports segmentation of traffic in the control and forwarding planes by keeping the routing tables separate for each user group (or VPN) and forwards the traffic on the associated or dedicated interfaces of each user group.

There are some deployment scenarios in which remote sites that are connecting to an MPLS VPN network might be extending segmentation from a campus to the WAN. In such an extended segmentation case, a CE-PE interface on a CE (group member or key server) device "bounds" to its associated Virtual

Routing Forwarding (VRF) instance. This VRF interface connects to an MPLS PE device where it is directly mapped to its associated Border Gateway Protocol (BGP) VRF process, in which case the crypto map is applied to a VRF interface. No other configuration changes are necessary.

End-User Considerations

Multicast rekeying can be used with all modes of multicast. The **rekey retransmit** command should be used whenever the Protocol Independent Multicast-sparse mode (PIM-SM) is configured because the PIM-SM shortest path tree (SPT) can be torn down if it does not receive continuing traffic. When traffic resumes, PIM-SM must reestablish the SPT. Retransmitting rekey packets increases the chance that group members receive the rekeys when PIM-SM is setting up the SPT.

System Error Messages

For a list of system error messages, see Appendix I: System Messages, page 73.

How to Configure Cisco Group Encrypted Transport VPN

This section includes the following required and optional tasks:

Setting up a Key Server

To set up a key server, perform the steps in the following five subtasks.

Prerequisites

Before creating the GDOI group, you must first configure IKE and the IPsec transform set, and you must create an IPsec profile. For information about how to configure IKE and the IPsec transform set and to create an IPsec profile, see the "Related Documents" subsection of the "Additional References" section on page 44.

Setting up RSA Keys to Sign Rekey Messages

To set up RSA keys that will be used to sign rekey messages, perform the following steps.

If you want to configure anti-replay, use the **replay time window-size** and **replay counter window-size** commands (see Steps 4 and 5 below).

Note

- Skip this subtask if rekey is not in use.
- If you want to configure anti-replay, use the **replay time window-size** and **replay counter window-size** commands (see Steps 4 and 5 below).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa general-keys label** *name-of-key*
4. **replay counter window-size**
5. **replay time window-size**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto key generate rsa general-keys label** *name-of-key* **Example:** `Router (config)# crypto key generate rsa general-keys label mykeys`	Generates RSA keys that will be used to sign rekey messages. **Note** Skip this command if rekey is not in use.
Step 4	**replay counter window-size** **Example:** `Router (config)# replay counter window-size`	(Optional) Turns on counter-based anti-replay protection for traffic defined inside an access list using GDOI if there are only two group members in a group.
Step 5	**replay time window-size** **Example:** `Router (config)# replay time window-size`	(Optional) Sets the window size for anti-replay protection using GDOI if there are more than two group members in a group.

What to Do Next

Set up the group ID, server type, and SA type. (See the section "Setting up the Group ID, Server Type, and SA Type" section on page 20.)

Setting up the Group ID, Server Type, and SA Type

To set up the group ID, server type, and SA type, perform the following steps.

Note For a large number of sites, it is better to take precautions and add functionality incrementally, especially when one is migrating from any other encryption solutions like Dual Multipoint VPN (DMVPN). For example, instead of setting up all the CPE devices to encrypt the traffic bidirectionally, it is possible to set up one-way encryption so that only one or fewer members of a group are allowed to send encrypted traffic. Others are allowed to receive only encrypted traffic. After the one-way encryption is validated for one or a few members, bidirectional encryption can be turned on for all the members. This "inbound only" traffic can be controlled using the **sa receive only** command under a crypto group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto gdoi group** *group-name*
4. **identity number** *number*

   or

   identity address ipv4 *address*
5. **server local**
6. **sa receive-only**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto gdoi group** *group-name* **Example:** `Router (config)# crypto gdoi group gdoigroupname`	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	**identity number** *number* or **identity address ipv4** *address* **Example:** `Router (config-gdoi-group)# identity number 3333` or `Router (config-gdoi-group)# identity address ipv4 10.2.2.2`	Identifies a GDOI group number or address.
Step 5	**server local** **Example:** `Router (config-gdoi-group)# server local`	Designates a device as a GDOI key server and enters GDOI local server configuration mode.
Step 6	**sa receive-only** **Example:** `Router (config-local-server)# sa receive-only`	Specifies that an IPsec SA is to be installed by a group member as “inbound only.”

What to Do Next

Remove the receive-only configuration on the key server so that the group members are now operating in bidirectional receive and send mode.

Setting up the Rekey

Rekey is used in the control plane by the key server to periodically refresh the policy and IPsec SAs of the group. On the group-member side, instead of fully reregistering when timers expire for any other reasons, refreshing the registration with a rekey is more efficient. The initial registration is always a unicast registration.

The key server can be configured to send rekeys in unicast or multicast mode. The rekey transport mode is determined by whether the key server can use IP multicast to distribute the rekeys. If multicast capability is not present within the network of the customer, the key server will have to be configured to send rekeys using unicast messages.

Additional options for rekey use the **rekey authentication**, **rekey retransmit,** and **rekey address ipv4** commands. If unicast transport mode is configured, the **source address** command will have to be included to specify the source address of this unicast rekey message.

Multicast is the default transport type for rekey messages. The following bulleted items explain when to use rekey transport type mulitcast or unicast:

- If all members in a group are multicast capable, do not configure the **rekey transport unicast** command.

Note The **no rekey transport unicast** command is not needed if the rekey transport type "unicast" was not configured previously under this group because multicast rekeys are on by default.

- If all members in a group are unicast, use the **rekey transport unicast** command.
- If you have mixed members in a group (that is, the majority are multicast, but a few are unicast), do not configure the **rekey transport unicast** command. The rekeys will be distributed using multicast to the majority of group members. The remainder of the group members that do not receive the multicast messages (unicast group members) will have to reregister to the key server when their policies expire. Mixed mode (that is, unicast and multicast rekey mode) is currently not supported.

Note

- If the **no rekey transport unicast** command is used, members in the GDOI group that are unable to receive the multicast rekey messages need to reregister with the key server to get the latest group policies.

  The reregistering forces the default transport type to multicast. If no transport type was configured previously, the multicast transport type will apply by default.

Prerequisites

Before configuring the **rekey authentication** command, you must have configured the router to have a RSA key generated using the **crypto key generate rsa** command and **general-keys** and **label** keywords (for example, "crypto key generate rsa general-key label my keys").

Setting up a Unicast Rekey

To set up a unicast rekey, perform the following steps.

Note In the configuration task table below, the address "ipv4 10.0.5.2" specifies the interface on the key server by which the unicast or multicast rekey messages are sent. This address is required for unicast rekeys, but it is optional for multicast rekeys. For multicast rekeys, the source address of the key server can be retrieved from the rekey ACL.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*

   or

   identity address ipv4 *address*
5. **server local**
6. **rekey transport unicast**
7. **rekey lifetime seconds** *number-of-seconds*
8. **rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions*
9. **rekey authentication {mypubkey | pubkey} rsa** *key-name*
10. **address ipv4** *ipv4-address*

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto gdoi group** *group-name* **Example:** `Router (config)# crypto gdoi group gdoigroupname`	Identifies a GDOI group and enters GDOI group configuration mode.

	Command or Action	Purpose
Step 4	**identity number** *number* or **identity address ipv4** ***address*** **Example:** `Router (config-gdoi-group)# identity number 3333` or `Router (config-gdoi-group)# identity address ipv4 10.2.2.2`	Identifies a GDOI group number or address.
Step 5	**server local** **Example:** `Router (config-gdoi-group)# server local`	Designates a device as a GDOI key server and enters GDOI local server configuration mode.
Step 6	**rekey transport unicast** **Example:** `Router (config-local-server)# rekey transport unicast`	Configures unicast delivery of rekey messages to group members.
Step 7	**rekey lifetime seconds** *number-of-seconds* **Example:** `Router (gdoi-local-server)# rekey lifetime seconds 300`	(Optional) Limits the number of seconds that any one encryption key should be used. If this command is not configured, the default value of 86400 seconds takes effect.
Step 8	**rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions* **Example:** `Router (gdoi-local-server)# rekey retransmit 10 number 3`	(Optional) Specifies the number of times the rekey message is retransmitted. If this command is not configured, there will be no retransmits.
Step 9	**rekey authentication** {**mypubkey** | **pubkey**} **rsa** *key-name* **Example:** `Router (gdoi-local-server)# rekey authentication mypubkey rsa mykeys`	(Optional) Specifies the keys to be used for a rekey to GDOI group members. This command is optional if rekeys are not required. If rekeys are required, this command is required.Se
Step 10	**address ipv4** *ipv4-address* **Example:** `Router (gdoi-local-server)# address ipv4 10.0.5.2`	(Optional) Specifies the source information of the unicast rekey message. If rekeys are not required, this command is optional. If rekeys are required, this command is required.

Setting up a Multicast Rekey

To set up a multicast rekey, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*

   or

   identity address ipv4 *address*
5. **server local**
6. **rekey address ipv4** {*access-list-name* | *access-list-number*}
7. **rekey lifetime seconds** *number-of-seconds*
8. **rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions*
9. **rekey authentication** {**mypubkey | pubkey**} **rsa** *key-name*
10. **exit**
11. **exit**
12. **access-list** *access-list-number* {**deny | permit**} **udp host** *source* [*operator* [*port*]] **host** *source* [*operator* [*port*]]

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto gdoi group** *group-name* **Example:** `Router (config)# crypto gdoi group gdoigroupname`	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	**identity number** *number* or **identity address ipv4** *address* **Example:** `Router (config-gdoi-group)# identity number 3333` or `Router (config-gdoi-group)# identity address ipv4 10.2.2.2`	Identifies a GDOI group number or address.

	Command or Action	Purpose
Step 5	**server local** **Example:** `Router (config-gdoi-group)# server local`	Designates a device as a GDOI key server and enters GDOI local server configuration mode.
Step 6	**rekey address ipv4** {*access-list-name* | *access-list-number*} **Example:** `Router (gdoi-local-server)# rekey address ipv4 121`	Defines to which multicast subaddress range group members will register.
Step 7	**rekey lifetime seconds** *number-of-seconds* **Example:** `Router (gdoi-local-server)# rekey lifetime seconds 300`	(Optional) Limits the number of seconds that any one encryption key should be used. If this command is not configured, the default value of 86400 seconds takes effect.
Step 8	**rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions* **Example:** `Router (gdoi-local-server)# rekey retransmit 10 number 3`	(Optional) Specifies the number of times the rekey message is retransmitted. If this command is not configured, there will be no retransmits.
Step 9	**rekey authentication** {**mypubkey** | **pubkey**} **rsa** *key-name* **Example:** `Router (gdoi-local-server)# rekey authentication mypubkey rsa mykeys`	(Optional) Specifies the keys to be used for a rekey to GDOI group members. This command is optional if rekeys are not required. If rekeys are required, this command is required.
Step 10	**exit** **Example:** `Router (gdoi-local-server)# exit`	Exits GDOI server local configuration mode.
Step 11	**exit** **Example:** `Router (config-gdoi-group)# exit`	Exits GDOI group configuration mode.
Step 12	**access-list** *access-list-number* {**deny** | **permit**} **udp host** *source* [*operator* [*port*]] **host** *source* [*operator* [*port*]] **Example:** `Router (config)# access-list 121 permit udp host 10.0.5.2 eq 848 host 239.0.1.2 eq 848`	Defines an extended IP access list.

Setting up Group Member ACLs

To set up group member ACLs, perform the following steps.

Note Ensure that your ACL starts with a deny statement if all traffic does not need to be encrypted.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **deny ip host** *source* **host** *source*
4. **access-list** *access-list-number* **permit ip** *source*

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* **deny ip host** *source* **host** *source* **Example:** `Router (config)# access-list 101 deny ip host 10.0.0.1 host 10.0.0.2`	Defines a denied IP access list.
Step 4	**access-list** *access-list-number* **permit ip** *source* **Example:** `Router (config)# Router (config)# access-list 103 permit ip 10.15.0.0. 0.255.255.255 10.20.0.0. 0.255.255.255`	Defines an allowed IP access list.

What to Do Next

The above access list is the same one that should be used to set up the SA. See the "Setting up the IPsec SA" section on page 29.

Setting up an IPsec Lifetime Timer

To set up an IPsec lifetime timer for a profile, perform the following steps. If this configuration task is not performed, the default is the maximum IPsec SA lifetime of 3600 seconds.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto ipsec profile** *name*
4. **set security-association lifetime seconds** *seconds*

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec profile** *name* **Example:** `Router (config)# crypto ipsec profile profile1`	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and enters crypto ipsec profile configuration mode.
Step 4	**set security-association lifetime seconds** *seconds* **Example:** `Router (ipsec-profile)# set security-association lifetime seconds 2700`	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec SAs.

What to Do Next

Configure the IPsec SA. See the "Setting up the IPsec SA" section on page 29.

Setting up an ISAKMP Lifetime Timer

To set up an ISAKMP lifetime timer, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy** *priority*
4. **lifetime** *seconds*

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp policy** *priority* **Example:** `Router (config)# crypto ipsec policy 1`	Defines an IKE policy.
Step 4	**lifetime** *seconds* **Example:** `Router (config-isakmp-policy)# lifetime 86400`	Specifies the lifetime of an IKE SA.

Setting up the IPsec SA

To set up the IPsec SA, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*

   or

   identity address ipv4 *address*
5. **server local**
6. **sa ipsec** *sequence-number*
7. **profile** *ipsec-profile-name*
8. **match address ipv4** {*access-list-number* | *access-list-name*}
9. **exit**
10. **exit**
11. **exit**
12. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
13. **crypto ipsec profile** *ipsec-profile-name*
14. **set transform-set** *transform-set-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto gdoi group** *group-name* **Example:** `Router (config)# crypto gdoi group gdoigroupname`	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	**identity number** *number* or **identity address ipv4** *address* **Example:** `Router (config-gdoi-group)# identity number 3333` or `Router (config-gdoi-group)# identity address ipv4 10.2.2.2`	Identifies a GDOI group number or address.
Step 5	**server local** **Example:** `Router (config-gdoi-group)# server local`	Designates a device as a GDOI key server and enters GDOI local server configuration mode.
Step 6	**sa ipsec** *sequence-number* **Example:** `Router (gdoi-local-server)# sa ipsec 1`	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.
Step 7	**profile** *ipsec-profile-name* **Example:** `Router (gdoi-sa-ipsec)# profile gdoi-p`	Defines the IPsec SA policy for a GDOI group.
Step 8	**match address ipv4** {*access-list-number* | *access-list-name*} **Example:** `Router (gdoi-sa-ipsec)# match address ipv4 102`	Specifies an IP extended access list for a GDOI registration.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router (gdoi-sa-ipsec)# exit`	Exits GDOI SA IPsec configuration mode.
Step 10	**exit** **Example:** `Router (gdoi-local-server)# exit`	Exits GDOI local server configuration mode.
Step 11	**exit** **Example:** `Router (config-gdoi-group)# exit`	Exits GDOI group configuration mode.
Step 12	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*] **Example:** `Router (config)# crypto ipsec transform-set gdoi-trans esp-3des esp-sha-hmac`	Defines a transform set—an acceptable combination of security protocols and algorithms.
Step 13	**crypto ipsec profile** *ipsec-profile-name* **Example:** `Router (config)# crypto ipsec profile profile1`	Defines an ISAKMP profile and enters crypto ipsec profile configuration mode.
Step 14	**set transform-set** *transform-set-name* **Example:** `Router (ipsec-profile)# set transform-set transformset1`	Specifies which transform sets can be used with the crypto map entry.

What to Do Next

Replay should be configured. If not configured, the default is counter mode.

Setting up a Group Member

To set up a group member, perform the following subtasks:

- Setting Up the Group Name, ID, and Key Server IP Address, page 31 (required)
- Setting up the Crypto Map, page 33 (required)
- Applying the Crypto Map to an Interface to Which the Traffic Has to Be Encrypted, page 34 (required)

Setting Up the Group Name, ID, and Key Server IP Address

To set up the group name, ID, and key server IP address, perform the following steps.

Note You can set up to eight key server addresses.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*

   or

   identity address ipv4 *address*
5. **server address ipv4** *address*

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto gdoi group** *group-name* **Example:** `Router (config)# crypto gdoi group gdoigroupone`	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	**identity number** *number* or **identity address ipv4** *address* **Example:** `Router (config-gdoi-group)# identity number 3333` or `Router (config-gdoi-group)# identity address ipv4 10.2.2.2`	Identifies a GDOI group number or address.
Step 5	**server address ipv4** *address* **Example:** `Router (config-gdoi-group)# server address ipv4 10.0.5.2`	Specifies the address of the server a GDOI group is trying to reach. • To disable the address, use the **no** form of the command.

What to Do Next

Set up the crypto map. See the section "Setting up the Crypto Map" section on page 33.

Setting up the Crypto Map

To set up the crypto map, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **gdoi**
4. **set group** *group-name*

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *map-name seq-num* **gdoi** **Example:** `Router (config)# crypto map mymap 10 gdoi`	Enters crypto map configuration mode and creates or modifies a crypto map entry.
Step 4	**set group** *group-name* **Example:** `Router (config-crypto-map)# set group group1`	Associates the GDOI group to the crypto map.

What to Do Next

Apply the crypto map to an interface to which the traffic has to be encrypted. See the "Applying the Crypto Map to an Interface to Which the Traffic Has to Be Encrypted" section on page 34.

Applying the Crypto Map to an Interface to Which the Traffic Has to Be Encrypted

To apply the crypto map to an interface to which the traffic has to be encrypted, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot|port*
4. **crypto map** *map-name seq-num* **gdoi**

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot|port* **Example:** `Router (config)# interface gig0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**crypto map** *map-name seq-num* **gdoi** **Example:** `Router (config-if)# crypto map gdoigroupone 10 gdoi`	Applies the crypto map to the interface.

Verifying and Troubleshooting Cisco Group Encrypted Transport VPN

The following tasks can be used to verify and troubleshoot your GET VPN configurations. These tasks are optional and are used to gather information during troubleshooting.

- Verifying Active Group Members on a Key Server, page 35
- Verifying Rekey-Related Statistics, page 35
- Verifying IPsec SAs That Were Created by GDOI on a Key Server, page 35
- Verifying Cooperative Key Server States and Statistics, page 36
- Verifying Anti-Replay Pseudotime-Related Statistics, page 37

Verifying Active Group Members on a Key Server

To verify active group members on a key server, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show crypto gdoi ks members**

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto gdoi ks members** **Example:** `Router# show crypto gdoi ks members`	Displays information about key server members.

Verifying Rekey-Related Statistics

To verify rekey-related statistics, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show crypto gdoi ks rekey**

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto gdoi ks rekey** **Example:** `Router# show crypto gdoi ks rekey`	On the key server, this command displays information about the rekeys that are being sent from the key server.

Verifying IPsec SAs That Were Created by GDOI on a Key Server

To verify IPsec SAs that were created by GDOI on a key server, perform the following steps.

SUMMARY STEPS

1. **enable**

2. **show crypto gdoi group** *group-name* **ipsec sa**
3. **show crypto ipsec sa**

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto gdoi group** *group-name* **ipsec sa** **Example:** `Router# show crypto gdoi group diffint ipsec sa`	Displays information about IPsec SAs that were created by GDOI on a key server. • In this case, information will be displayed only for group "diffint." • For information about IPsec SAs for all groups, omit the **group** keyword and *group-name* argument.
Step 3	**show crypto ipsec sa** **Example:** `Router# show crypto ipsec sa`	Displays the settings used by current SAs.

Verifying Cooperative Key Server States and Statistics

To verify cooperative key server states and statistics, perform the following steps, using one or all of the **debug** and **show** commands shown.

SUMMARY STEPS

1. **enable**
2. **debug crypto gdoi ks coop**
3. **show crypto gdoi group** *group-name* **ks coop** [**version**]

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug crypto gdoi ks coop** **Example:** `Router# debug crypto gdoi ks coop`	Displays information about a cooperative key server.
Step 3	**show crypto gdoi group** *group-name* **ks coop** [**version**] **Example:** `Router# show crypto gdoi group diffint ks coop engineer`	Displays key server information for the group "diffint."

Verifying Anti-Replay Pseudotime-Related Statistics

To verify anti-replay pseudotime-related statistics, perform the following steps using one or all of the **clear**, **debug**, and **show** commands.

SUMMARY STEPS

1. **enable**
2. **clear crypto gdoi group** *group-name* **replay**
3. **debug crypto gdoi replay**
4. **show crypto gdoi group** *group-name*
5. **show crypto gdoi group** *group-name* **ks replay**

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear crypto gdoi group** *group-name* **replay** **Example:** `Router# clear crypto gdoi group diffint replay`	Clears the replay counters.
Step 3	**debug crypto gdoi replay** **Example:** `Router# debug crypto gdoi replay`	Displays information about the pseudotime stamp that is contained in a packet.

Step 4	**show crypto gdoi group** *group-name* **Example:** `Router# show crypto gdoi group diffint`	Displays information about the current pseudotime of the group member. It also displays the different counts that are related to the anti-replay for this group.
Step 5	**show crypto gdoi group** *group-name* **ks replay** **Example:** `Router# show crypto gdoi group diffint ks replay`	Displays information about the current pseudotime of the key server.

Configuration Examples for Cisco Group Encrypted Transport VPN

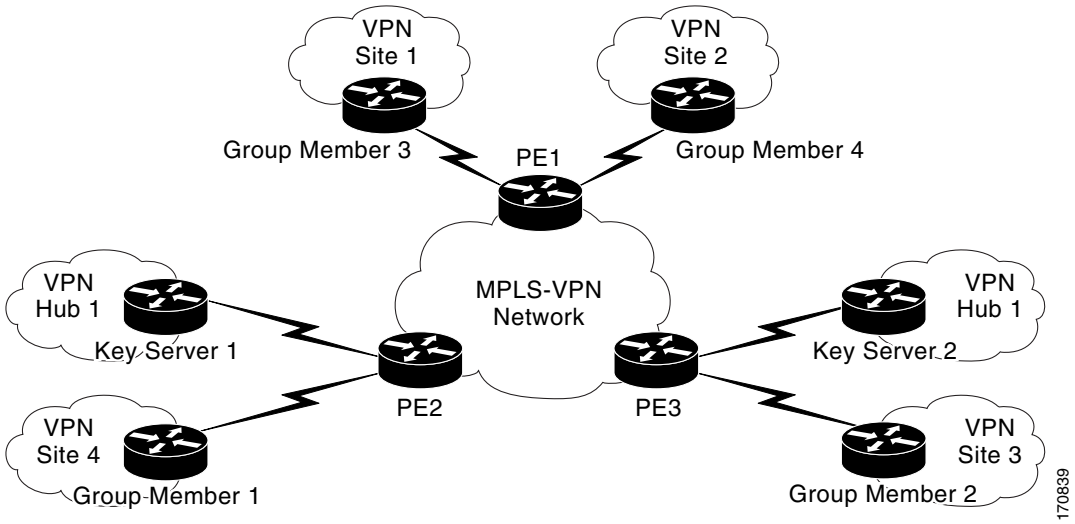
This section includes the following case study and configuration examples:

Key Server and Group Member Case Study

The following case study includes encrypting traffic CE-CE in an MPLS VPN environment.

The MPLS VPN core interconnects VPN sites as is shown in Figure 12. VPN site CPEs, Group Member 1 through Group Member 4, are grouped into a single GDOI group that correlates with a VPN with which these sites are a part. This scenario is an intranet VPN scenario. All the key servers and group members are part of the same VPN. Key Server 1 and Key Server 2 are the cooperative key servers that support VPN members Group Member 1 through Group Member 4. Key Server 1 is the primary key server and Key Server 2 is the secondary key server.

Figure 12 Key Server and Group Member Scenario



The following configuration examples are based on the case study in Figure 12.

Key Server 1: Example

Key server 1 is the primary key server.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname KS1
!
logging buffered 100000 debugging
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
ip domain name cisco.com
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 400
crypto isakmp key cisco address 10.1.1.13
crypto isakmp key cisco address 10.1.1.9
crypto isakmp key cisco address 10.1.1.1
crypto isakmp key cisco address 10.1.1.5
crypto isakmp key cisco address 10.1.1.21
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
```

```
!
crypto ipsec profile gdoi-profile-group1
 set security-association lifetime seconds 1800
 set transform-set gdoi-trans-group1
!
crypto gdoi group group1
 identity number 1
 server local
  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa group1-export-general
  rekey transport unicast
  sa ipsec 1
   profile gdoi-profile-group1
   match address ipv4 101
   replay counter window-size 64
  address ipv4 10.1.1.17
  redundancy
   local priority 10
   peer address ipv4 10.1.1.21
   !
interface Ethernet0/0
 ip address 10.1.1.17 255.255.255.252
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.18
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
end
```

Key Server 2: Example

Key Server 2 is the secondary key server.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname KS2
!
logging buffered 100000 debugging
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
ip domain name cisco
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 400
crypto isakmp key cisco address 10.1.1.9
crypto isakmp key cisco address 10.1.1.1
```

```
crypto isakmp key cisco address 10.1.1.5
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.13
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-profile-group1
 set security-association lifetime seconds 1800
 set transform-set gdoi-trans-group1
!
crypto gdoi group group1
 identity number 1
 server local

  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa group1-export-general
  rekey transport unicast
  sa ipsec 1
   profile gdoi-profile-group1
   match address ipv4 101
   replay counter window-size 64
  address ipv4 10.1.1.21
  redundancy
   local priority 1
   peer address ipv4 10.1.1.17
   !
interface Ethernet0/0
 ip address 10.1.1.21 255.255.255.252
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.22
!

access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
end
```

Group Member 1: Example

Group Member 1 is part of a GDOI group that correlates with a VPN with which these sites are a part.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM1
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.21
!
```

```
crypto gdoi group group1
 identity number 1
 server address ipv4 10.1.1.17
 server address ipv4 10.1.1.21
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.252
 crypto map map-group1
!
router bgp 1000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.1.0 mask 255.255.255.0
 neighbor 10.1.1.2 remote-as 5000
 no auto-summary
!
ip classless
!
End
```

Group Member 2: Example

Group Member 2 is part of a GDOI group that correlates with a VPN with which these sites are a part.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname GM2
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.21
!
crypto gdoi group group1
 identity number 1
 server address ipv4 10.1.1.17
 server address ipv4 10.1.1.21
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 10.1.1.5 255.255.255.252
 crypto map map-group1
!
router bgp 2000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.2.0 mask 255.255.255.0
```

```
 neighbor 10.1.1.6 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

Group Member 3: Example

Group Member 3is part of a GDOI group that correlates with a VPN with which these sites are a part.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM3
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.21
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
crypto gdoi group group1
 identity number 1
 server address ipv4 10.1.1.17
 server address ipv4 10.1.1.21
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 10.1.1.9 255.255.255.252
 crypto map map-group1
!
router bgp 3000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.3.0 mask 255.255.255.0
 neighbor 10.1.1.10 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

Group Member 4: Example

Group Member 4 is part of a GDOI group that correlates with a VPN with which these sites are a part.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM4
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.21
!
crypto gdoi group group1
 identity number 1
 server address ipv4 10.1.1.17
 server address ipv4 10.1.1.21
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 10.1.1.13 255.255.255.252
 crypto map map-group1
!
router bgp 4000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.4.0 mask 255.255.255.0
 neighbor 10.1.1.14 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

Additional References

The following sections provide references related to the Cisco Group Encrypted Transport VPN feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands (listed in an index)	Cisco IOS Master Command List
Cisco IOS security commands	Cisco IOS Security Command Reference

Related Topic	Document Title
Configuring IKE and IKE policy	"Configuring Internet Key Exchange for IPSec VPNs"section of the *Cisco IOS Security Configuration Guide:Secure Connectivity,* Release 12.4
Configuring an IPsec transform	"Configuring Security for VPNs with IPSec" section of the *Cisco IOS Security Configuration Guide:Secure Connectivity,* Release 12.4

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3547	The Group Domain of Interpretation

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

New Commands

- address ipv4 (GDOI)
- crypto gdoi gm
- local priority
- peer address ipv4
- redundancy (GDOI)
- rekey transport unicast
- replay counter window-size
- replay time window-size
- sa receive-only

Modified Commands

- clear crypto gdoi
- debug crypto gdoi
- rekey address ipv4
- show crypto gdoi

address ipv4 (GDOI)

To set the source address, which is used as the source for packets originated by the local key server, use the **address ipv4** command in GDOI local server configuration mode. To remove the source address, use the **no** form of this command.

address ipv4 *ip-address*

no address ipv4 *ip-address*

Syntax Description

ip-address	Source address of the local key server.

Command Default

A source address is not configured.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

When this command is used with unicast rekeys, the address is used as the source of the outgoing rekey message. When this command is used with redundancy, the address is used as the source of the outgoing announcement message. If both unicast rekeying and redundancy are configured, the same address is the source of both types of packets.

If multicast rekeying is configured and the **address ipv4** command is configured, the address (*ip-address)* is the source of the outgoing multicast packet. If multicast is configured but the **address ipv4** command is not configured, the access control list (ACL) specified in the **rekey address ipv4** command identifies the source of the outgoing multicast packet.

Examples

The following example shows the local server IP address is 10.1.1.0:

```
server local
 rekey algorithm aes 192
 rekey address ipv4 121
 rekey lifetime seconds 300
 rekey retransmit 10 number 2
 rekey authentication mypubkey rsa mykeys
 address ipv4 10.1.1.0
 sa ipsec 1
```

Related Commands

Command	Description
rekey address ipv4	Sends a rekey to a destination multicast address.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

clear crypto gdoi

To clear the state of the current session of a Group Domain of Interpretation (GDOI) group member with the key server, use the **clear crypto gdoi** command in privileged EXEC mode.

clear crypto gdoi [**group** *group-name* | **ks coop counters** | **ks policy** | **replay counter**]

Syntax Description

group *group-name*	(Optional) Name of the group.
ks coop counters	(Optional) Clears the counters for the cooperative key server.
ks policy	(Optional) Clears all policies on the key server. **Note** (Configuring this keyword does not trigger the reelection of the key servers.)
replay counter	(Optional) Clears the anti-replay counters.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The **group** and **replay** keywords and the *group-name* argument were added.

Usage Guidelines

If this command is issued on the group member, the policy of the group member is deleted, and the group member reregisters with the key server.

If this command is issued on the key server, the state on the key server is deleted. If redundancy is configured and this command is issued on the key server, the key server goes back into election mode to elect a new primary key server.

Examples

If the following command is issued on the key server, the state on the key server is cleared. If the command is issued on a group member, the state is cleared for the entire group and a reregistration to the key server is forced.

```
clear crypto gdoi
```

If the following command is issued on the key server, the state of the group that is specified is cleared on the key server. If the command is issued on a group member, the state of the group that is specified is cleared on the group member, and reregistration to the key server is forced.

```
clear crypto gdoi group group1
```

The following command clears the anti-replay counters for the GDOI groups:

```
clear crypto gdoi replay counter
```

The following command clears the counters for the cooperative key server:

```
clear crypto gdoi ks coop counters
```

The following command clears all policy on the key server but does not trigger the reelection of the key servers:

```
clear crypto gdoi ks policy
```

crypto gdoi gm

For group members to change the IP security (IPsec) security association (SA) status, use the **crypto gdoi gm** command in privileged EXEC mode.

crypto gdoi gm group *group-name* {**ipsec direction inbound optional | ipsec direction inbound only | ipsec direction both**}

Syntax Description

group *group-name*	Name of the group.
ipsec direction inbound optional	Allows a group member to change the IPsec SA status to inbound optional. IPsec SA will accept cipher or plain text or both and will encrypt the packet before forwarding it.
ipsec direction inbound only	Allows a group member to change the IPsec SA status to inbound only. IPsec SA will accept cipher or plain text or both and will forward the packet in clear text.
ipsec direction both	Allows a group member to change the IPsec SA status to both inbound and outbound. IPsec SA will accept only cipher text and will encrypt the packet before forwarding it.

Command Default

If the **sa receive-only** command is specified on the key server, the group member remains in receive-only mode.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is executed on group members. This command and its various keywords aid in testing individual group members and verifies that the group members are encrypting or decrypting traffic. This command and its keywords can be used only after the **sa receive-only** command has been configured on the key server.

The **ipsec direction inbound optional** keyword is used for situations in which all group members have been instructed to install the IPsec SAs as inbound only but for which a group member wants to install the IPsec SAs as inbound optional.

The **ipsec direction inbound only** keyword is used when a group member wants to change a previously set IPsec SA status to inbound only.

The **ipsec direction both** keyword is used when a group member has to change a previously set IPsec SA status to both inbound and outbound. In this setting, the group member accepts only cipher text.

Examples

The following example shows how to determine whether a group member can accept cipher text.

On Group Member 1, configure the following:

```
crypto gdoi gm group groupexample ipsec direction inbound only
```

On Group Member 2, configure the following:

```
crypto gdoi gm group groupexample ipsec direction inbound optional
```

Then Ping Group Member 1.

Group Member 2 will have encrypted the packet and will send an encrypted packet to Group Member 1, which then decrypts that packet. If the traffic is from Group Member 1 to Group Member 2, Group Member 1 will forward the packet in clear text, and Group Member will accept it.

Related Commands

Command	Description
sa receive-only	Specifies that an IPsec SA is to be installed by a group member as "inbound only."

debug crypto gdoi

To display information about a Group Domain of Interpretation (GDOI) configuration, use the **debug crypto gdoi** command in privileged EXEC mode. To disable crypto GDOI debugging, use the **no** form of this command.

debug crypto gdoi [**detail** | **error** | **event** | **gm** | **infra** | **ks** [**coop**] | **packet** | **replay** | **terse**]

no debug crypto gdoi [**detail** | **error** | **event** | **gm** | **infra** | **ks** [**coop**] | **packet** | **replay** | **terse**]

Syntax Description

detail	(Optional) Displays detailed debug information.
error	(Optional) Displays information about error debugs.
event	(Optional) Displays user-level information.
gm	(Optional) Displays information about group members.
infra	(Optional) Displays information about the GDOI infrastructure.
ks	(Optional) Displays information about key servers.
coop	(Optional) Displays information about cooperative key servers.
packet	(Optional) Displays information about packet-level debugs (administrator-level information).
replay	(Optional) Displays information about the pseudotime stamp that is contained in a packet.
terse	(Optional) Displays lowest-level debugs (message-level information).
Note	The **detail**, **error**, **event**, **packet**, and **terse** keywords can be used with the other nonlevel keywords (for example, **gm error**, **infra error**, **ks coop event, replay error**).

Command Default

Debugging is turned off.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The **detail**, **error**, **event**, **gm**, **infra**, **ks**, **coop**, **packet**, **replay**, and **terse** keywords were added.

Usage Guidelines

Using this command displays various GDOI debugs. For debugging information for cooperative key servers, use the **debug crypto gdoi ks coop** command.

Examples

The following example shows group member registration debug output:

```
Router# debug crypto gdoi

00:00:40: GDOI:(0:0:N/A:0):GDOI group diffint
00:00:40: %CRYPTO-5-GM_REGSTER: Start registration for group diffint using address
10.0.3.1
00:00:40: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
00:00:40: GDOI:(0:1001:HW:0:3333):beginning GDOI exchange, M-ID of 1167145075
00:00:40: GDOI: Group Number is 3333
00:00:40: GDOI:(0:1001:HW:0:3333):GDOI: GDOI ID sent successfully
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI SA Payload, message ID + 1167145075
00:00:40: GDOI:(0:1001:HW:0):processing GDOI SA KEK Payload
00:00:40: GDOI:(0:0:N/A:0):    KEK_ALGORITHM 5
00:00:40: GDOI:(0:0:N/A:0):    KEY_LENGTH 24
00:00:40: GDOI:(0:0:N/A:0):    KEY_LIFETIME 299
00:00:40: GDOI:(0:0:N/A:0):    SIG_HASH_ALG 2
00:00:40: GDOI:(0:0:N/A:0):    SIG_ALG 1
00:00:40: GDOI:(0:0:N/A:0):    SIG_KEY_LEN 94
00:00:40: GDOI:(0:0:N/A:0): Completed KEK Processing
00:00:40: GDOI:(0:1001:HW:0):processing GDOI SA TEK Payload
00:00:40: GDOI:(0:1001:HW:0:3333): Completed TEK Processing
00:00:40: GDOI:(0:1001:HW:0):processing GDOI SA TEK Payload
00:00:40: GDOI:(0:1001:HW:0:3333): Completed TEK Processing
00:00:40: GDOI:(0:1001:HW:0:3333):GDOI ACK sent successfully by GM
00:00:40: GDOI:received payload type 18
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI Seq Payload, message_id  1167145075
00:00:40: GDOI:(0:1001:HW:0:3333):Completed SEQ Processing for seq 0
00:00:40: GDOI:received payload type 17
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI KD Payload, message_id  1167145075
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI Key Packet, message_id  38649336
00:00:40: GDOI:(0:1001:HW:0:3333):procesing TEK KD: spi is 56165461, spi
00:00:40: GDOI:(0:1001:HW:0:3333):TEK Integrity Key 20 bytes
00:00:40: GDOI:(0:1001:HW:0:3333):Completed KeyPkt Processing
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI Key Packet, message_id  38649336
00:00:40: GDOI:(0:1001:HW:0:3333):procesing TEK KD: spi is 56165522, spi
00:00:40: GDOI:(0:1001:HW:0:3333):TEK Integrity Key 20 bytes
00:00:40: GDOI:(0:1001:HW:0:3333):Completed KeyPkt Processing
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI Key Packet, message_id  38649336
00:00:40: GDOI:(0:1001:HW:0:3333): Processing KEK KD
00:00:40: GDOI:(0:1001:HW:0:3333):KEK Alg Key 32 bytes
00:00:40: GDOI:(0:1001:HW:0:3333):KEK Sig Key 94 bytes
00:00:40: GDOI:(0:1001:HW:0:3333):Completed KeyPkt Processing
00:00:40: %GDOI-5-GM_REGS_COMPL: Registration complete for group diffint using address
10.0.3.1

enc(config-if)#
00:00:40: GDOI:(0:0:N/A:0):Registration installed 2 new ipsec SA(s) for group diffint.
```

The following output example shows key server registration debugs:

```
Router# debug crypto gdoi

00:00:40: GDOI:(0:1001:HW:0):processing GDOI ID payload, message ID = 1167145075
00:00:40: GDOI:(0:1001:HW:0):The GDOI ID is a Number: 3333
00:00:40: GDOI:(0:0:N/A:0): Adding KEK Policy to the current ks_group
00:00:40: GDOI:(0:0:N/A:0):Setting MULTICAST TEK rekey lifetime 30
00:00:40: GDOI:(0:0:N/A:0):Setting MULTICAST TEK rekey lifetime 30
00:00:40: GDOI:(0:1001:HW:0:3333):GDOI SA sent successfully by KS
00:00:40: GDOI:(0:1001:HW:0:3333):GDOI KD sent successfully by KS
```

The following output example shows group member rekey debugs:

```
Router# debug crypto gdoi

00:02:00: GDOI:(0:1002:HW:0):Received Rekey Message!
00:02:00: GDOI:(0:1002:HW:0):Signature Valid!
00:02:00: GDOI:received payload type 18
00:02:00: GDOI:(0:1002:HW:0):processing GDOI Seq Payload, message_id  0
00:02:00: GDOI:(0:1002:HW:0):Completed SEQ Processing for seq 8
00:02:00: GDOI:(0:1002:HW:0):processing GDOI SA Payload, message ID + 0
00:02:00: GDOI:(0:1002:HW:0):processing GDOI SA KEK Payload
00:02:00: GDOI:(0:1002:HW:0):    KEK_ALGORITHM 5
00:02:00: GDOI:(0:1002:HW:0):    KEY_LENGTH 24
00:02:00: GDOI:(0:1002:HW:0):    KEY_LIFETIME 219
00:02:00: GDOI:(0:1002:HW:0):    SIG_HASH_ALG 2
00:02:00: GDOI:(0:1002:HW:0):    SIG_ALG 1
00:02:00: GDOI:(0:1002:HW:0): Completed KEK Processing
00:02:00: GDOI:(0:1002:HW:0):processing GDOI SA TEK Payload
00:02:00: GDOI:(0:1002:HW:0): Completed TEK Processing
00:02:00: GDOI:(0:1002:HW:0):processing GDOI SA TEK Payload
00:02:00: GDOI:(0:1002:HW:0): Completed TEK Processing
00:02:00: GDOI:received payload type 17
00:02:00: GDOI:(0:1002:HW:0):processing GDOI KD Payload, message_id  0
00:02:00: GDOI:(0:1002:HW:0):processing GDOI Key Packet, message_id  38649336
00:02:00: GDOI:(0:1002:HW:0):procesing TEK KD: spi is 49193284, spi
00:02:00: GDOI:(0:1002:HW:0):TEK Integrity Key 20 bytes
00:02:00: GDOI:(0:1002:HW:0):Completed KeyPkt Processing
enc(config-if)#
00:02:00: GDOI:(0:1002:HW:0):processing GDOI Key Packet, message_id  38649336
00:02:00: GDOI:(0:1002:HW:0):procesing TEK KD: spi is 49193345, spi
00:02:00: GDOI:(0:1002:HW:0):TEK Integrity Key 20 bytes
00:02:00: GDOI:(0:1002:HW:0):Completed KeyPkt Processing
00:02:00: GDOI:(0:1002:HW:0):processing GDOI Key Packet, message_id  38649336
00:02:00: GDOI:(0:1002:HW:0): Processing KEK KD
00:02:00: GDOI:(0:1002:HW:0):Completed KeyPkt Processing
```

local priority

To set the local key server priority, use the **local priority** command in GDOI redundancy configuration mode. To remove the local key server priority that was set, use the **no** form of this command.

local priority *number*

no local priority *number*

Syntax Description

number	Priority number of the local server. Value = 1 through 10.

Command Default

If the local priority is not set by this command, the local priority defaults to 1.

Command Modes

GDOI redundancy configuration

Command History1

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Configure the priority to determine the order of preference of the key servers (the higher priority device becomes the primary key server). If the priority of two devices is the same, the IP address is used to set the priority. The higher the IP address, the higher the priority.

Note If the **no local priority** option is configured, the default value of 1 is set for that key server.

Examples

The following example shows that the key server 10.1.1.1 has the higher priority and, therefore, becomes the primary key server:

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
 peer address ipv4 10.33.5.6
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
peer address ipv4	Configures a GDOI redundant peer key server.

Command	Description
redundancy	Enters GDOI redundancy configuration mode and allows for peer key server redundancy.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

peer address ipv4

To configure a Group Domain of Interpretation (GDOI) redundant peer key server, use the **peer address ipv4** command in GDOI redundancy configuration mode. To remove the peer key server that was configured, use the **no** form of this command.

peer address ipv4 *ip-address*

no peer address ipv4 *ip-address*

Syntax Description

ip-address	IP address of the peer key server.

Command Default

(Redundancy does not function correctly if at least one peer is not configured under the local key server configuration on a key server.)

Command Modes

GDOI redundancy configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

For redundancy between key servers to operate correctly, there have to be at least two key servers in a redundant group. Therefore, at least one other peer must be defined on a key server using the **peer address ipv4** command. The local key server sets up an Internet Key Exchange (IKE) session with the peer that is defined using this command and proceeds to communicate using IKE informational messages to complete the election process using the specified IP address of the peer.

Examples

The following example shows that two peer key servers have been configured: 10.41.2.5 and 10.33.5.6.

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
 peer address ipv4 10.33.5.6
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
local priority	Sets the local key server priority.
redundancy	Enters GDOI redundancy configuration mode and allows for key server redundancy.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

redundancy (GDOI)

To enable Group Domain of Interpretation (GDOI) redundancy configuration mode and to allow for key server redundancy, use the **redundancy** command in GDOI local server configuration mode. To disable GDOI redundancy, use the **no** form of this command.

redundancy

no redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Key server redundancy is not supported for a key server.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command must be configured before configuring related redundancy commands, such as for key server peers, local priority, and timer values. Use the **local priority** command to set the local key server priority. Use the **peer address ipv4** command to configure the peer address that belongs to the redundancy key server group.

Examples

The following example shows that key server redundancy has been configured:

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
 peer address ipv4 10.33.5.6
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
local priority	Sets the local key server priority.
peer address ipv4	Configures the peer key server.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey address ipv4

To specify the source or destination information of the rekey message, use the **rekey address ipv4** command in GDOI local server configuration mode. To remove a source or destination address, use the **no** form of this command.

rekey address ipv4 {*access-list-number* | *access-list-name*}

no rekey address ipv4 {*access-list-number* | *access-list-name*}

Syntax Description

access-list-number	IP access list number. The number can be from 100 through 199, or it can be in the expanded range of 2000 through 2699.
access-list-name	Access list name.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If rekeys are not required, this command is optional. If rekeys are required, this command is required.

The source is usually the key server interface from which the message leaves, and the destination is the multicast address on which the group members receive the rekeys (for example, access-list 101 permit 121 permit udp host 10.0.5.2 eq 848 host 192.168.1.2. eq 848).

Examples

The following example shows that the rekey address is access list "101":

```
rekey address ipv4 101
```

The following example shows that a rekey message is to be sent to access control list (ACL) address 239.10.10.10:

```
crypto gdoi group gdoigroup1
 identity number 1111
 server local
  rekey address ipv4 120
  rekey lifetime seconds 400
  no rekey retransmit
  rekey authentication mypubkey rsa ipseca-3845b.examplecompany.com
access-list 120 permit udp host 10.5.90.1 eq 848 host 239.10.10.10 eq 848
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey transport unicast

To configure unicast delivery of rekey messages to group members, use the **rekey transport unicast** command in global configuration mode. To remove unicast delivery of rekey messages and enable the default to multicast rekeying, use the **no** form of this command.

rekey transport unicast

no rekey transport unicast

Syntax Description

This command has no arguments or keywords.

Command Default

If **rekey transport unicast** is not specified or **no rekey transport unicast** is specified, multicast rekeying is the default.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is configured on the key server under the **server local** command, along with other rekey configurations.

Examples

The following example shows that unicast delivery of rekey messages to group members has been configured:

```
crypto gdoi group diffint
 identity number 3333
 server local
  rekey lifetime seconds 300
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa mykeys
  rekey transport unicast
  sa ipsec 1
   profile gdoi-p
   match address ipv4 120
   replay counter window-size 64
   address ipv4 10.0.5.2
```

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

replay counter window-size

To turn on counter-based anti-replay protection for traffic defined inside an access list using Group Domain of Interpretation (GDOI) if there are only two group members in a group, use the **replay counter window-size** command in GDOI SA IPsec configuration mode. To disable counter-based anti-replay protection, use the **no** form of this command.

replay counter window-size *seconds*

no replay counter window-size

Syntax Description

seconds	Number of seconds of the interval duration of the Sychronous Anti-Replay (SAR) clock. Values = 64, 128, 256, 512, and 1024. Default window size = 64.

Command Default

Counter-based anti-replay is not enabled.

Command Modes

GDOI SA IPsec configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is configured on the key server.

Note GDOI anti-replay can be either counter based or time based. Use this command for counter-based anti-replay protection. For time-based anti-replay protection, use the **replay time window-size** command.

Examples

The following example shows that the anti-replay window size for unicast traffic has been set to 512:

```
crypto gdoi group gdoigroup1
 identity number 1111
 server local
  rekey address ipv4 120
  rekey lifetime seconds 400
  no rekey retransmit
  rekey authentication mypubkey rsa ipseca-3845b.examplecompany.com
 sa ipsec 10
   profile group1111
   match address ipv4 101
   replay counter window-size 512
```

Related Commands

Command	Description
replay time window-size	Sets the the window size for anti-replay protection using GDOI if there are more than two group members in a group.
sa ipsec	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.

replay time window-size

To set the window size for anti-replay protection using Group Domain of Interpretation (GDOI) if there are more than two group members in a group, use the **replay time window-size** command in GDOI SA IPsec configuration mode. To disable time-based anti-replay, use the **no** form of this command.

replay time window-size *seconds*

no replay time window-size

Syntax Description

seconds	Number of seconds of the interval duration of the Sychronous Anti-Replay (SAR) clock. The value range is 1 through 100. The default value is 100.

Command Default

Time-based anti-replay is not enabled.

Command Modes

GDOI SA IPsec configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is configured on the key server.

Note GDOI anti-replay can be either counter based or time based. This command turns on time-based anti-replay. For counter-based anti-replay protection, use the **replay counter window-size** command.

Examples

The following example shows that the number of seconds of the interval duration of the SAR clock has been set to 1:

```
sa ipsec 10
 profile group1111
 match address ipv4 101
 replay time window-size 1
```

Related Commands

Command	Description
replay counter window-size	Sets the window size for counter-based anti-replay protection for unicast traffic defined inside an access list.
sa ipsec	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.

sa receive-only

To specify that an IP security (IPsec) security association (SA) is to be installed by a group member as "inbound only," use the **sa receive-only** command in GDOI local server configuration mode. To remove the inbound-only specification, use the **no** form of this command.

sa receive-only

no sa receive-only

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, IPsec SAs are installed by group members as both inbound and outbound.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is configured on a key server. The command may be used to ease in deployment.

Examples

The following example shows that the Group Domain of Interpretation (GDOI) group is instructed by the key server to install the IPsec SAs as "inbound only":

```
crypto gdoi group gdoi_group
 identity number 1234
server local
 sa receive-only
 sa ipsec 1
  profile gdoi-p
  match address ipv4 120
```

Related Commands

Command	Description
crypto gdoi gm	Allows group members to change the IPsec SA status.
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

show crypto gdoi

To display information about a Group Domain of Interpretation (GDOI) configuration, use the **show crypto gdoi** command in privileged EXEC mode.

show crypto gdoi [**debug-condition**] [**group** *group-name*] [**gm** [**acl** | **pubkey** | **rekey** | **replay**] | **ks** [**acl** | **coop** [**version**] | **members** [*ip-address*] | **policy** | **rekey** | **replay**]] [**ipsec sa**]

Syntax Description

debug-condition	(Optional) Displays GDOI debug conditional filters.
group *group-name*	(Optional) Displays information about the group specified.
gm	(Optional) Displays information about group members.
acl	(Optional) Displays the access control list (ACL) that has been applied to the GDOI group.
pubkey	(Optional) Displays public keys downloaded from the key server.
rekey	(Optional) Displays rekey information.
replay	(Optional) Displays group information for time-based anti-replay.
ks	(Optional) Displays information about key servers.
coop	(Optional) Displays information about the cooperative key servers.
version	(Optional) Displays information about the cooperative key server and client versions.
members [*ip-address*]	(Optional) Displays information about registered group members.
policy	(Optional) Displays key server policy information.
ipsec sa	(Optional) Displays information about the IP security (IPsec) security association (SA) for all group members. • If this keyword is used with the **group** *group-name* keyword and argument option, information is displayed for only the group that is specified.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The **group** *group-name* keyword and argument and **gm**, **acl**, **rekey**, **replay**, **ks**, **coop** [**version**], **members**, **policy**, and **ipsec sa** keywords were added.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.
15.1(3)T	This command was modified. The **debug-condition** and **pubkey** keywords were added.

Usage Guidelines

Because the **show running-config** command does not display enabled debug commands, the **debug-condition** keyword is useful for displaying GDOI debug conditional filters that are enabled.

Examples

The following example shows how to display information about a configuration for a GDOI group member:

```
Router# show crypto gdoi group diffint

Group Information
   Group Name                  : diffint
   Group Identity              : 3333
   Group Members Registered    : 0
   Group Server                : 10.0.5.2


   Group Name                  : test
   Group Identity              : 4444
   Group Members Registered    : 0
   Group Server                : 10.0.5.2
```

The following example shows how to display information about a configuration when entered on a GDOI key server:

```
Router# show crypto gdoi group diffint ks

Group Information
   Group Name                  : diffint
   Group Identity              : 3333
   Group Members Registered    : 1
   Group Server                : Local
   Group Rekey Lifetime        : 300 secs
   Group Rekey
       Remaining Lifetime      : 84 secs
   IPSec SA Number             : 1
     IPSec SA Rekey Lifetime   : 120 secs
     Profile Name              : gdoi-p
   SA Rekey
       Remaining Lifetime      : 64 secs
   access-list 120 permit ip host 10.0.1.1 host 192.168.1.1
   access-list 120 permit ip host 10.0.100.2 host 192.168.1.1

   Group Member List for Group diffint :
   Member ID                   : 10.0.3.1

   Group Name                  : test
   Group Identity              : 4444
   Group Members Registered    : 0
   Group Server                : Local
   Group Rekey Lifetime        : 600 secs
   IPSec SA Number             : 1
     IPSec SA Rekey Lifetime   : 120 secs
     Profile Name              : gdoi-p
   access-list 120 permit ip host 10.0.1.1 host 192.168.1.1
   access-list 120 permit ip host 10.0.100.2 host 192.168.1.1
```

The following example shows how to display GDOI key server information for registered GMs when entered on a GDOI key server:

```
Router# show crypto gdoi ks members

Group Member Information :

Detail :

Number of rekeys sent for group diffint : 10

Group Member ID   : 5.0.6.1
```

```
Group ID          : 3333
Group Name        : diffint
Key Server ID     : 5.0.10.1
Rekeys sent       : 10
Rekeys retries    : 0
Rekey Acks Rcvd   : 10
Rekey Acks missed : 0

Sent seq num :    2    3    1    2
Rcvd seq num :    2    3    1    2

Group Member ID   : 5.0.5.1
Group ID          : 3333
Group Name        : diffint
Key Server ID     : 5.0.8.1
Rekeys sent       : 10
Rekeys retries    : 0
Rekey Acks Rcvd   : 10
Rekey Acks missed : 0

Sent seq num :    2    3    1    2
Rcvd seq num :    2    0    0    0
```

The following example shows how to verify the RSA public key that is downloaded from the key server:

```
Router# show crypto gdoi gm pubkey

GDOI Group: diffint
    KS IP Address: 10.0.9.1
    conn-id: 1020    my-cookie:BFC164DB    his-cookie:3F2C75D9
    Key Data:
      305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00B508E9 EDD36AE1
      B7AFEB96 74AAD793 4AAA549B 91809707 25AE59E7 E7359CB3 6C938C82 5ED17AC3
      9E1B1611 DF3791DD FBAC8C4B EEEDC4F5 46C4472A BAAE0870 69020301 0001
```

For RSA public keys, the key server sends the group member the RSA public key when the group member registers. When the key server sends a rekey, it signs it using the RSA private key. After the group member receives this rekey, it verifies the signature using the public key that it downloaded from the key server (therefore, the group member knows that it received the rekey from the key server).

Table 1 describes the significant fields shown in the displays.

Table 1 show crypto gdoi Field Descriptions

Field	Description
GDOI Group	The group to which the group member belongs.
KS IP Address	Address of the key server from which the GM received the RSA public key during registration.
conn-id	Connection ID.
My-cookie	My-cookie & his-cookie fields are the same as the ones in the **show crypto gdoi gm rekey detail** command.
His-cookie	My-cookie & his-cookie fields are the same as the ones in the **show crypto gdoi gm rekey detail** command.
Key Data	The contents of the key itself.

Related Commands

Command	Description
crypto key pubkey-chain rsa	Enters public key configuration mode (so you can manually specify other devices' RSA public keys).
rsa-pubkey	Defines the RSA manual key to be used for encryption or signature during IKE authentication.

Feature Information for Cisco Group Encrypted Transport VPN

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for Cisco Group Encrypted Transport VPN

Feature Name	Releases	Feature Information
Secure Multicast	12.4(6)T	The secure multicast part of this feature was first introduced in Cisco IOS Release 12.4(6)T in *Secure Multicast*. However, all pertinent information from that document has been integrated and updated in this current document (*Cisco Group Encrypted Transport VPN*).
Cisco Group Encrypted Transport VPN	12.4(11)T	Cisco Group Encrypted Transport VPN is an optimal encryption solution for large-scale IP or MPLS sites that require any-to-any connectivity with minimum convergence time, low processing, provisioning, managing, and troubleshooting overhead. The following commands were introduced or modified by this feature: **address ipv4 (GDOI), clear crypto gdoi, crypto gdoi gm, debug crypto gdoi, local priority, peer address ipv4, redundancy, rekey address ipv4, rekey transport unicast, replay counter window-size, replay time window-size, sa receive-only**, **show crypto gdoi.**

Glossary

DOI—Domain of Interpretation. For Internet Security Association Key Management Protocol (ISAKMP), a value in the security association (SA) payload that describes in which context the key management message is being sent (IPsec or Group Domain of Interpretation).

GDOI—Group Domain of Interpretation. For ISAKMP, a means of distributing and managing keys for groups of mutually trusted systems.

group member—Device (Cisco IOS router) that registers with a group that is controlled by the key server for purposes of communicating with other group members.

group security association—SA that is shared by all group members in a group.

IPsec—IP security. Data encryption protocol for IP packets that are defined in a set of RFCs (see IETF RFC 2401).

ISAKMP—Internet Security Association and Key Management Protocol. Protocol that provides a framework for cryptographic key management protocols.

KEK—key encryption key. Key used to protect the rekey between the key server and group members.

key server—Device (Cisco IOS router) that distributes keys and policies to group members.

SA—security association. SA that is shared by all group members in a group.

TEK—traffic encryption key. Key that is used to protect the rekey between group members.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.

Appendix I: System Messages

Table 3 lists GET VPN system messages and explanations.

Table 3 GET VPN System Messages

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_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.
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.

Table 3 GET VPN System Messages (continued)

Error Messages	Explanation
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.

Table 3 GET VPN System Messages (continued)

Error Messages	Explanation
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_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 pseudotime with a value that is largely different from its own pseudotime.
REPLAY_FAILED	A group member or key server has failed an anti-replay check.
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.