Group Encrypted Transport (GET) VPNs

Cisco Group Encrypted Transport virtual private network (GET VPN) is a full-mesh VPN technology that can be used in a variety of WAN environments, including IP and Multiprotocol Label Switching (MPLS). GET VPN comprises 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 IP security (IPsec) encryption to provide users with an efficient method to secure IP multicast 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 Quality of Service (QoS).
- 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.

Tip For information about the CLI configuration of GET VPN, see *Cisco Group Encrypted Transport VPN* on Cisco.com.

This chapter contains the following topics:

Understanding Group Encrypted Transport (GET) VPNs

Networked applications such as voice and video increase the need for instantaneous, branch-interconnected, and 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, Group Encrypted Transport VPN (GET VPN), a WAN encryption technology, eliminates the need to compromise between network intelligence and data privacy.

With GET, Cisco provides tunnelless VPN, which eliminates the need for IPsec 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 is a standards-based security model that is based on the concept of a trusted group to eliminate point-to-point IPsec tunnels and their associated overlay routing. Trusted group members share a common security association (SA), also known as a group SA. This enables group members to decrypt traffic that was encrypted by any other group member. By using trusted groups instead of point-to-point tunnels, full-mesh 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.

In addition to leveraging the existing IKE, IPsec and multicast technologies, a GET VPN topology includes these key elements and features:

- Group members—The routers that exchange the actual traffic within the VPN are called group members. Group members provide encryption services to the traffic. Encryption policies are defined centrally on the key server and downloaded to the group member at the time of registration. Based on these downloaded policies, a group member decides whether traffic needs to be encrypted or decrypted and what keys to use.

  Although group members primarily obtain encryption policies from the key server, you can configure local service policy ACLs on the group members to exclude traffic from encryption based on local requirements. For more information, see Understanding the GET VPN Security Policy and Security Associations, page 29-10.

  Note A device can be a group member of more than one group.

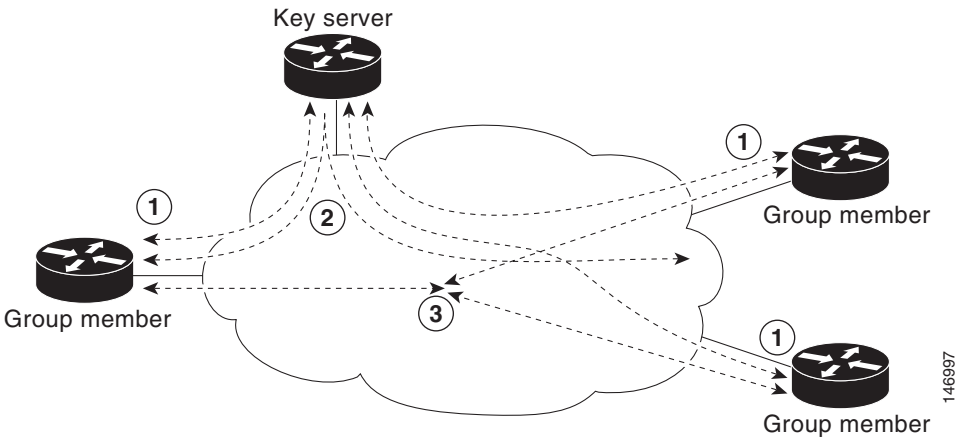
- Key servers—The routers that act as key servers are the gatekeepers to the topology. The group member must successfully register with a key server before becoming an active member of the VPN. The key servers control the shared service policy, and generate and transmit keys to group members. Key servers cannot be group members themselves, but a single key server can service more than one topology. For more information, see Understanding the GET VPN Registration Process, page 29-4.
- The Group Domain of Interpretation (GDOI) group key management protocol is used to provide a set of cryptographic keys and policies to a group of devices. In a GET VPN network, GDOI is used to distribute common IPsec keys to a group of enterprise VPN gateways (group members) that must communicate securely. Devices designated as key servers periodically refresh and send out the updated keys to the group members using a process called "rekeying."

  The GDOI protocol uses the Phase 1 Internet Key Exchange (IKE) SA. All participating VPN gateways authenticate themselves to the device providing keys using IKE. All IKE authentication methods, for example, pre-shared keys (PSKs) and public key infrastructure (PKI), are supported for initial authentication. After the VPN gateways are authenticated and provided with the appropriate security keys using the IKE SA, the IKE SA expires and GDOI is used to update the group members in a more scalable and efficient manner. For more information about GDOI, refer to RFC 3547.
- Address preservation—IPsec-protected data packets carry the original source and destination in the outer IP header rather than replacing them with tunnel endpoint addresses. 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 (CE) device 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 an MPLS network).

The following figure shows the general operation of a GET VPN topology.

Figure 29-1 General GET VPN Operation



1. Group members register with the key server using the Group Domain of Interpretation (GDOI) protocol. 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 and unicast packets. The registration process can use unicast or multicast communications.

2. Group members exchange IP packets that are encrypted using IPsec. Only the group members are an active part of the VPN.
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 security associations (SAs) expire. Rekey messages are sent in advance of the SA expiration time to ensure that valid group keys are always available.

GET VPN is provisioned using Security Manager with the following caveats:

- GET VPN-aware VRF is not supported.
- DMVPN with GET is not supported, because there is no way to define DMVPN without tunnel protection in Security Manager.
- Manual configuration of a group member to join a multicast group (ip igmp join-group) is not supported. Security Manager only provisions static source-specific multicast (SSM) mappings.

Related Topics

- Understanding the GET VPN Registration Process, page 29-4
- Understanding the GET VPN Security Policy and Security Associations, page 29-10
- Configuring GET VPN, page 29-12

Understanding the GET VPN Registration Process

In GET VPN, group members comprise the VPN topology. Traffic in the VPN is traffic between group members. For a device to become a group member, the device must successfully register with a key server. Key servers maintain the security association (SA) policy and create and maintain the keys for the group. When a group member registers, the key server downloads the policy and the keys to the group member. The key server also rekeys the group before existing keys expire.

The key server has two responsibilities: 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 the group ID is valid, the key server sends the security association policy to the group member. After the group member acknowledges that it can handle the downloaded policy, the key server downloads the respective keys.

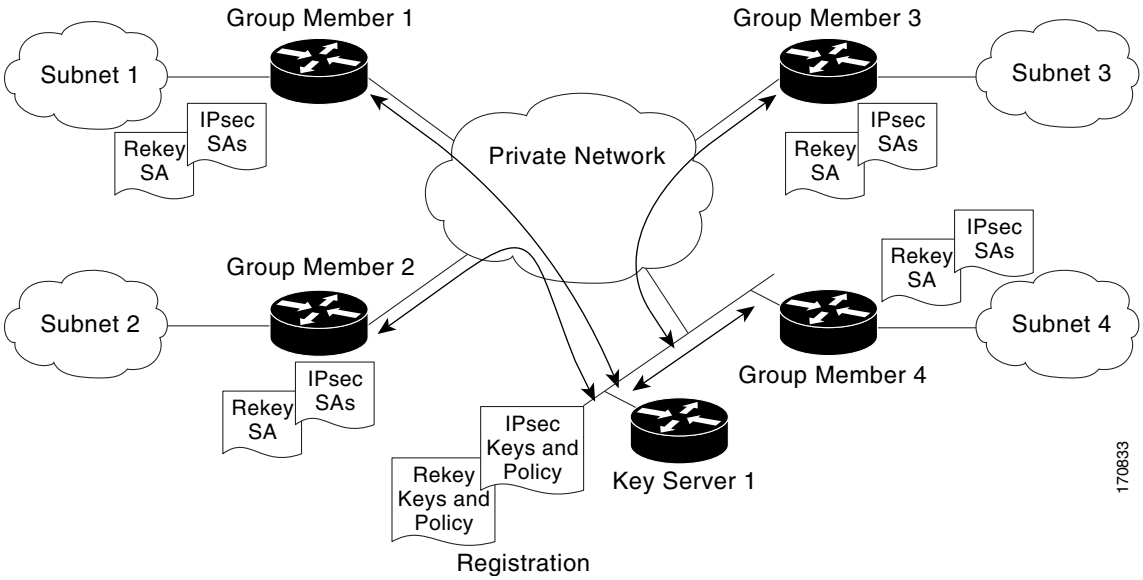
Communication among the key server and group members is encrypted and secured using two types of keys: the traffic encryption key (TEK) and the key encryption key (KEK). The TEK is downloaded by the key server to all the group members. The downloaded TEK is used by all the group members to communicate 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 sends out rekey messages either because of an impending IPsec SA expiration or because the security policy has changed on the key server. A rekey can also happen if the KEK timer has expired (the key server sends out a KEK rekey). Rekey messages might also be retransmitted periodically to account for possible packet loss. If the rekey mechanism is multicast, 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. If the rekey mechanism is unicast, the receivers send an acknowledgment message.

The key server generates the group policy and IPsec security associations (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). Note that the group member might also have a local security policy configured that is merged with the one downloaded; for complete information see Understanding the GET VPN Security Policy and Security Associations, page 29-10.

The following figure 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 29-2 Communication Flow Between Group Members and the Key Server



When you configure the GET VPN topology, you can configure the following registration-related features:

- Decide whether to use unicast or multicast for group registration and rekeying. For more information, see Choosing the Rekey Transport Mechanism, page 29-6.

Note If you use multicast, you need to enable multicast on the key servers and group members manually. Security Manager does not provision multicast commands.

- Decide whether to configure more than one key server to provide redundancy and load balancing. For more information, see Configuring Redundancy Using Cooperative Key Servers, page 29-7.
- Decide whether to configure fail-close mode on group members to protect their traffic prior to successful registration with the key server. For more information, see Configuring Fail-Close to Protect Registration Failures, page 29-8.

- Decide whether to require authorization for group members to join the group. You can use certificate authorization (which requires that you also configure the Public Key Infrastructure policy) or preshared keys. Configuring authorization is required if the key server serves more than one group. For information about the configuration options, see the Authorization Type setting described in Defining GET VPN Group Encryption, page 25-54.

Related Topics

- Generating and Synchronizing RSA Keys, page 29-13
- Configuring GET VPN, page 29-12

Choosing the Rekey Transport Mechanism

When you configure the rekey settings in the Group Encryption Policy (as described in Defining GET VPN Group Encryption, page 25-54), you must select whether to use multicast or unicast as the rekey transport mechanism. The key server uses this method whenever sending new keys and IPsec security associations (SAs) to group members or each other. There are advantages and disadvantages to each method.

Multicast is the standard choice. Using multicast, the key server sends one copy of each rekey message to all group members at once using a multicast group address, so there is no rekey delay and group members can install the updated security policy essentially simultaneously (not accounting for regular network delay). However, in some networks, multicast is either an extra cost feature, or it is simply not allowed. If you configure multicast, you must supply the multicast address that will be used by the GET VPN topology.

Unicast can be used when multicast is unavailable or undesirable. Using unicast, the key server sends directed rekey and IPsec SAs to group members, and the group member sends an acknowledgment that the message was received. Because unicast requires sending direct messages and receiving acknowledgments, the key server sends the unicast messages to a subset of the group members at a time (unless you have a relatively small VPN, perhaps fewer than 30 group members, in which case all group members might be sent messages at the same time).

Thus, the relative benefits of multicast and unicast include the following:

- With multicast, the key server does not know if a group member receives a message, whereas with unicast, there are acknowledgments. With unicast, if the key server does not receive the acknowledgment, it resends the message.
- Multicast is faster than unicast, especially for large topologies with hundreds of group members. Multicast rekey uses the same low CPU overhead whether there is one group member in the group or a few thousand.
- With unicast, if a group member continuously fails to send acknowledgments, the key server decides the group member is no longer there and stops sending rekey messages. Thus, the key server always has a list of active group members. The unresponsive group member must reregister to rejoin the GET VPN topology. Because multicast does not use acknowledgments, the key server does not know if a group member becomes unresponsive, and it does not maintain a list of active group members.

Tip To use multicast, you must enable multicast on the key servers and group members. Security Manager does not provision these commands; it only enables multicast rekey, it does not enable the router to send and receive multicast traffic. Therefore, you must manually enable multicast on the device, or use the FlexConfig policy to provision the commands (see Creating FlexConfig Policy Objects, page 7-28).

Fortunately, it is possible to mix multicast and unicast in a single GET VPN topology so long as all key servers support multicast. When deciding which transport mechanism to use, consider the following recommendations:

- If all key servers and group members, and the network, support multicast, use multicast.
- If all of the key servers and most of the group members support multicast, but a small number of group members do not support multicast, use multicast. Group members that do not support multicast will not receive rekey and IPsec SA updates. However, when the lifetime settings for these items are about to expire, unicast group members will reregister with the key server and obtain the new keys and IPsec SAs.
- If no group members, or only a few, support multicast, use unicast. The group members will then receive rekeys and IPsec SA updates from the key server and not need to reregister to get them.

Related Topics

- Understanding the GET VPN Registration Process, page 29-4
- Generating and Synchronizing RSA Keys, page 29-13
- Configuring GET VPN, page 29-12

Configuring Redundancy Using Cooperative Key Servers

The key server is the most important entity in the GET VPN network because the key server maintains the control plane. Therefore, a single key server is a single point of failure for an entire GET VPN network. Because redundancy is an important consideration for key servers, GET VPN supports multiple key servers, called cooperative (COOP) key servers, to ensure seamless fault recovery if a key server fails or becomes unreachable.

You can configure a group member to register to any available key server from a list of all COOP key servers. The group member configuration determines the registration order (see Configuring GET VPN Group Members, page 29-20 and Edit Group Member Dialog Box, page 29-21). The key server defined first is contacted first, followed by the second defined key server, and so on. It is a best practice to distribute group member registration to all available COOP key servers to reduce the IKE processing load on a single key server. Note that only the primary key server sends rekey messages.

When COOP key servers boot, all key servers assume a *secondary* role and begin an election process. One key server, typically the one having the highest priority, is elected as a *primary* key server. The other key servers remain in the secondary state. The primary key server is responsible for creating and distributing group policies to all group members and to periodically synchronize the COOP key servers.

Cooperative key servers exchange one-way announcement messages (primary to secondary). If a secondary key server does not hear from the primary key server for a certain length of time, the secondary key server tries to contact the primary key server and request updated information. If the primary key server does not respond, or if the secondary key server does not hear from the primary key server, a COOP key server reelection is triggered and a new primary key server is elected.

Up to eight key servers can be defined as COOP key servers, but more than four COOP key servers are seldom required. Because rekey information is generated and distributed from a single primary key server, the advantage of deploying more than two key servers is the ability to handle registration load in case of a network failure and reregistration taking place at the same time. This is especially important when using Public Key Infrastructure (PKI) group member authorization because IKE negotiation using PKI requires a lot more CPU power compared to IKE negotiation using pre-shared keys (PSKs).

Tips

- The RSA key must be the same on all cooperative key servers. For information on synchronizing the RSA key, see Generating and Synchronizing RSA Keys, page 29-13.
- It is a best practice to enable periodic ISAKMP keepalives between key servers so that the primary key server can track and display the state of the other secondary key servers. IKE Keepalives between group members and the key server is not required and is not supported. For information on configuring keepalives, see Configuring Global Settings for GET VPN, page 29-16.
- The COOP protocol is configured on a per GDOI group basis. A key server that is configured with multiple GDOI groups can maintain multiple unique COOP relationships with disparate key servers.

Configuring Fail-Close to Protect Registration Failures

Group members must register with the key server to become members of the GET VPN. Before a group member successfully registers with the key server, traffic passing through the group member's GET VPN interface is not encrypted. The period of time in which clear-text transmissions occur can be short (if registration succeeds) or potentially long, if the group member fails to register for any reason.

This default behavior is known as fail-open. If you consider it a violation of your security standards that traffic is sent in clear text at any time, you can configure fail-close mode to protect traffic before (or during) registration. With fail-close mode, all traffic on the interface is dropped except for the traffic you specifically identify in the fail-close ACL. Fail-close mode essentially shuts down the interface until the group member successfully registers with the key server and downloads the required keys and security policy and associations. Note that the use of fail-close mode requires as a minimum Cisco IOS Software release 12.4(22)T or 15.0; you can also configure it on all supported ASRs (see Understanding Devices Supported by Each IPsec Technology, page 25-9).

Fail-close mode is used only during the initial registration. If a group member has already successfully registered, the group member keeps the downloaded policy from the key server even if future registrations fail. However, if you use the **clear crypto gdoi** command on the group member, the subsequent registration attempt is considered a first-time attempt and fail-close mode is enforced.

You configure fail-close mode on the individual group members as described in Configuring GET VPN Group Members, page 29-20. Thus, you can enable the mode on selected group members rather than on all of them. You must specify a fail-close ACL to ensure that you do not lock yourself (and Security Manager) out of the device, preventing configuration updates and maintenance until registration succeeds.

The fail-close ACL is an extended ACL policy object and is configured as part of a crypto map on the device. You configure the rules from the perspective of the group member. Use the following tips to help you create an appropriate fail-close ACL:

- You can configure both **permit** and **deny** statements. In the fail-close ACL, "permit" means "do not send this traffic," whereas "deny" means "send this traffic in clear text." This behavior is different from that of the typical crypto map ACL, where the statements have the following meaning:
  - **Permit**—Means "encrypt this traffic." Because the group member does not have the IPsec security association required to encrypt the traffic prior to registration, the result is that the traffic is dropped.
  - **Deny**—Means "do not encrypt this traffic." In a typical crypto map ACL, a deny statement results in the matching packet being compared to the next crypto map ACL configured on the device (if any). However, if traffic matches a deny statement in the fail-close ACL, all crypto map ACL processing ends and the traffic is allowed in clear text.

The reason deny works this way in fail-close mode is because fail-close includes an implicit ACL statement that gets added at the bottom of the list of crypto map ACLs. This statement is **permit ip any any**, which matches all traffic. Because there is no IPsec security association due to the fact that registration has yet to occur, there is no way to encrypt the remaining traffic and it is dropped.

Note that because of this final permit ip any any statement, you might be able to limit yourself to deny statements in your fail-close ACL.

- The fail-close ACL is processed sequentially after the optional group member security policy ACL. However, all statements in the group member security policy ACL must be deny statements, which indicate that matching traffic should be sent in clear text. Because the security policy is processed according to normal crypto map rules, traffic that matches deny statements is subsequently compared to the fail-close ACL. If the fail-close ACL does not have matching deny statements, the traffic will subsequently be dropped by the implicit final fail-close permit ip any any statement.

  Therefore, if you use a group member security policy ACL, and you want the identified traffic to be sent in clear text regardless of the registration status of the group member, your fail-close ACL should contain all of the same statements contained in the security policy ACL at the least. It might even be possible to use the same ACL object for both ACLs.

  For more information about group member security policies, see Understanding the GET VPN Security Policy and Security Associations, page 29-10.

- The fail-close ACL is inserted as the final crypto map ACL. Thus, if you configure other features on the GET VPN interface that use crypto maps, any traffic identified on deny statements in those other ACLs will also get trapped (and dropped) by the fail-close ACL and the implicit final permit ip any any statement. Thus, configuring fail-close mode for GET VPN can influence the non-GET VPN services you configure on the interface.
- Upon successful registration, the fail-close ACL and the implicit final permit ip any any statement are removed from the crypto maps. These policies are not persistent.
- You should consider including the following rules in the fail-close ACL policy object. Remember that these rules are from the perspective of the group member:
  - SSH, SSL (HTTPS) traffic—You, and Security Manager, need to be able to access the device to configure it. To ensure that you do not lock down the device, include deny statements for SSH and SSL. For SSH, **deny tcp any eq 22 <host or network address>**. For SSL, **deny tcp any eq 443 <host or network address>**. If you specify host addresses, ensure that the Security Manager server is one of the hosts.
  - Routing traffic—To enable routing, allow the traffic for your routing process. For example, if you are using OSPF, **deny ospf any any**.
  - GDOI traffic—Regardless of the contents of the fail-close ACL, the device looks for GDOI registration messages, so you do not need to explicitly allow them to enable successful registration. However, if a group member (1) is in the path between the key server and another group member (2), a registration failure by group member (1) will prevent successful registration by the blocked group member (2). For registration on group member (2) to succeed, the fail-close ACL on group member (1) would have to allow GDOI traffic to pass. Thus, you might want to make it a general practice to allow GDOI traffic in the fail-close ACL: **deny udp any eq 848 any eq 848**.

Related Topics

- Configuring GET VPN, page 29-12
- Creating Access Control List Objects, page 6-53
- Creating Extended Access Control List Objects, page 6-54

Understanding the GET VPN Security Policy and Security Associations

GET VPN uses crypto map access control lists (ACLs) to identify the traffic that needs to be encrypted in the VPN. These ACLs also identify traffic that should be sent as clear text instead of being encrypted (essentially, traffic that lies outside of the VPN). The collection of these ACLs define the security policy for the VPN.

GET VPN provides a multi-layered security policy. You define the general policy for the entire VPN on the key server, but you can also define a separate security policy on group members to account for local variations. The group member security policy always takes priority over the policy received from the key server. When the group member registers with the key server, the group member downloads the key server's security policy and associations and the group member creates a new, single security policy crypto map ACL by concatenating the individual security policies in this order: first, the group member's ACL; second, the key server's first ACL; third, and so forth, any additional ACLs from the key server in the order defined on the key server. It is important to understand that these merged ACLs are treated as a single ACL; they are not searched as separate ACLs. Thus, if traffic matches a deny statement from the group member's ACL, that traffic is never tested against any ACL rules downloaded from the key server.

Tip If a group member leaves the GET VPN, the ACLs downloaded from the key server are removed, but the group member security policy ACL is retained and remains configured on the device.

In GET VPN security policy ACLs (and crypto map ACLs in general), the permit and deny keywords have special meaning:

- **Permit**—Means "encrypt this traffic." Permit entries are allowed only in the security policy ACLs defined on the key server (in the **Group Encryption Policy**), because encrypted traffic needs to have a full IPsec security association, which includes the transform set used for encrypting traffic, and anti-replay and IPsec lifetime configurations. If a packet matches a permit entry, but no IPsec SA exists for that packet, the packet is dropped.

  Normally, your permit rules should be symmetric, that is, the source and destination addresses should be the same. If you need to specify different source and destination addresses, you must create two rules; the second rule should be a mirror image of the first rule, with the source and destination address switched.

- **Deny**—Means "do not encrypt this traffic." In practice, this typically means that the traffic that matches the deny statement is sent in the clear. However, if you configure other features that use crypto maps, "denied" traffic is actually compared to subsequent (lower priority) crypto map ACLs to see if there is a match. IPsec security associations (SAs) are not generated for deny rules.

Following is a summary of the security policies that you can configure, in priority order:

- **Group member security policy**—When you configure the group member, as described in Configuring GET VPN Group Members, page 29-20, you can optionally select an ACL policy object that defines the local group member security policy.

  This group member ACL policy object is allowed to have deny statements only. You use this ACL to identify any traffic that you want to exclude from encryption and send in the clear. For example, if a handful of group members in the group are running a different routing protocol than the usual one, you can configure a local entry to these group members' security policy ACL to bypass encryption of the routing protocol traffic instead of defining the policy globally at the key server level.

- **Key server security policies and security associations**—When you configure the Group Encryption Policy for the GET VPN, as described in Defining GET VPN Group Encryption, page 25-54, you configure ACLs that identify the traffic that should be encrypted and protected in the VPN.

  The security policies on the key server are coupled with transform sets and other settings to define security associations; two IPsec security associations (SAs) are actually configured for every rule within the ACL, and these SAs define how the selected traffic should be encrypted. Thus, all group members use the same group SAs and they do not need to negotiate them with each other.

  Because the key server policy is appended to the group member policy, the policy might be as simple as **permit ip any any**, that is, encrypt all traffic that has not been excluded by the group member policy.

  However, you can create more complex sets of security policies and associations, setting up several separate ACL policy objects that are coupled to different transform sets to define different types of encryption.

  If you create more than one security association, you must identify their order, and they are appended to the group policy in that order. Remember, the end result is a single ACL, so if you include a deny statement in the first ACL, any permit rules for the same traffic in subsequent security associations are ignored, and the traffic is sent in clear text rather than being encrypted.

Note When you consider the security associations defined in the Group Encryption Policy as a whole, you can define up to 100 ACL permit entries. Each permit entry results in a pair of IPsec SAs; the maximum number of IPsec SAs in a group can not exceed 200. It is a best practice to summarize interesting traffic to as few permit entries as possible, and to build symmetric policies, where the source and destination addresses are the same. Unlike traditional IPSec policies, where source and destination address ranges must be uniquely defined, GET VPN is optimized when the source and destination address range are the same. If you configure a rule that has different source and destination addresses, you must also configure the mirrored rule (where the source and destination address are flipped), meaning that four SAs are consumed.

In addition to these security policies, there is an additional fail-close ACL that influences traffic patterns if you configure fail-close mode on a group member. For a complete discussion, see Configuring Fail-Close to Protect Registration Failures, page 29-8.

Related Topics

- Configuring GET VPN, page 29-12
- Creating Access Control List Objects, page 6-53
- Creating Extended Access Control List Objects, page 6-54

Understanding 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.

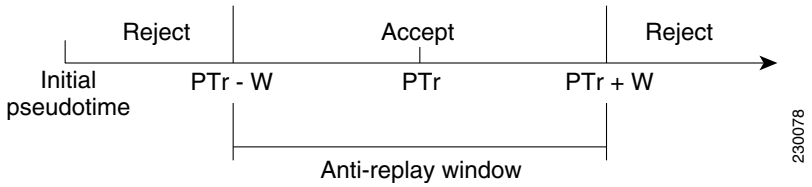
GET VPN uses the Synchronous Anti-Replay (SAR) mechanism to provide anti-replay protection for multisender traffic. SAR is independent of real-world Network Time Protocol (NTP) clock or sequential-counter mechanisms (which guarantee packets are received and processed in order). A SAR clock advances regularly. 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. 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 key server, 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.

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

You configure anti-replay in the security association definitions in the Group Encryption Policy. For more information, see Defining GET VPN Group Encryption, page 25-54 and Add New or Edit Security Association Dialog Box, page 25-58.

Figure 29-3 Anti-Replay Window



Configuring GET VPN

To configure a full mesh VPN with group encrypted transport (GET), use the Create VPN wizard as described in Creating or Editing VPN Topologies, page 25-28. When you finish the wizard, you are asked if you want to synchronize RSA keys, which is required for normal VPN functioning; for detailed information, see Generating and Synchronizing RSA Keys, page 29-13.

If you select multicast as the rekey transport mechanism, you must enable multicast on all key servers and the desired group members. For more information, see Choosing the Rekey Transport Mechanism, page 29-6.

You can change only the name and description of a GET VPN using the Edit VPN wizard. If you need to make changes to other policies and settings, open the policies from the Site-to-Site Manager page, as follows:

- For ISAKMP and IPSec settings, select **Global Settings for GET VPN**. See Configuring Global Settings for GET VPN, page 29-16.

- For IKE proposal policies, select **IKE Proposal Policy for GET VPN**. See Configuring the IKE Proposal for GET VPN, page 29-15.
- For security associations (ACL rules) and IPSec policies, select **Group Encryption Policy > Security Associations**. See Defining GET VPN Group Encryption, page 25-54.
- For preshared key policies, select **IKEv1 Preshared Key**. See Configuring IKEv1 Preshared Key Policies, page 26-48.
- For public key (PKI) policies, select **Public Key Infrastructure**. See Configuring IKEv1 Public Key Infrastructure Policies in Site-to-Site VPNs, page 26-54.
- For rekey settings, select **Group Encryption Policy > Group Settings**. See Defining GET VPN Group Encryption, page 25-54 and Generating and Synchronizing RSA Keys, page 29-13.
- For key server configuration, including RSA key synchronization, select **Key Servers**. See Configuring GET VPN Key Servers, page 29-18 and Generating and Synchronizing RSA Keys, page 29-13.
- For group membership and endpoint settings, select **Group Members**. See Configuring GET VPN Group Members, page 29-20.

Related Topics

- Understanding Group Encrypted Transport (GET) VPNs, page 29-2
- Understanding the GET VPN Registration Process, page 29-4
- Understanding the GET VPN Security Policy and Security Associations, page 29-10
- Troubleshooting GET VPN Configurations, page 29-25
- Understanding IKEv1 Preshared Key Policies in Site-to-Site VPNs, page 26-47

Generating and Synchronizing RSA Keys

When you specify the RSA key label in the Group Encryption Policy (as described in Defining GET VPN Group Encryption, page 25-54), the corresponding RSA key (public and private keys) needs to be configured on all key servers in the GET VPN topology. The key can either be a pre-existing key that you defined on the device, or it could be a new key label, and Security Manager can generate the key for you and synchronize all key servers to use the same key.

You can use the following methods to have Security Manager generate and synchronize the RSA key:

- When creating a new GET VPN using the Create VPN wizard, you are asked at the end of the wizard if you want to synchronize the keys. If you click **Yes**, Security Manager does the key synchronization immediately, and generates a new key if the key does not already exist. For information on using the Create VPN wizard, see Creating or Editing VPN Topologies, page 25-28.
- For an existing GET VPN, you can click the **Synchronize Keys** button on the Key Servers policy. Use this process whenever you add key servers or generate a new key on the primary key server. For information on configuring key server settings for existing topologies, see Configuring GET VPN Key Servers, page 29-18.

Tip For existing GET VPN topologies, if you want to generate a new RSA key, it might be easiest to update the Group Encryption Policy to specify a new, unused RSA key label, then click the Synchronize Keys button in the Key Servers policy. Because the key will not exist on any key server, Security Manager will generate the new key and import it into all key servers. You can then manually delete the old key from each key server.

Following are the uses for the RSA key:

- The key server uses the private RSA key to authenticate rekey messages from the group members.
- The key server provides the public RSA key to group members during registration.
- The key server uses the private key to sign the key encryption key (KEK) and traffic encryption key (TEK). The absence of an RSA key prevents the key server from creating the KEK and TEK.
- The RSA key is also used to sign messages between cooperative key servers.

When you start the RSA key synchronization process, the Synchronize Keys dialog box opens and shows you the overall progress as well as the results for each key server. (You can click the **Abort** button at any time to stop the process.) Security Manager performs the following steps:

1. Logs into all key servers and retrieves the RSA key information from each of them for the RSA key label configured for the VPN.
2. Determines whether any key server has a key with the required label:
   - If no key server has an RSA key with the required label, Security Manager generates the key on the primary key server (the one with the highest priority).
   - If one or more key server does not have the key, but all of the key servers that do have the key have the identical keys, Security Manager uses the existing key on any key server that has it.
   - If more than one key server has the key, but the contents of the key is different among the servers, you are asked if Security Manager can overwrite the keys. If you click **Yes**, Security Manager uses the existing key on the primary key server.

     If you click **No**, you can log into the key servers outside of Security Manager and manually adjust the keys according to your requirements. However, all key servers must have the same key contents for the RSA key. See below for an explanation of the process.
3. Creates an exportable version of the key.
4. Imports the key into each of the remaining key servers.

Tip For the synchronization process to succeed, the devices must be online and reachable and you must have Deploy authorization. If the device connection fails or times out, ensure that you can ping the key server from the Security Manager server. If it is your practice to deploy to file instead of to live devices, you might need to manually generate and synchronize the keys as described below. If you do not have sufficient authorization, you are prevented from initiating the process; someone else must do it.

Manually Generating and Synchronizing the RSA Key

If you do not want Security Manager to generate and synchronize keys, or if for some reason Security Manager cannot complete the process, you can manually generate and synchronize keys using the following sequence in Privileged EXEC (enable) configuration mode:

1. Generate the key on a key server using the following command, where **rekeyrsa** is the name of the key (you can specify a name of your choosing). You must make the key exportable.

crypto key generate rsa general-keys label rekeyrsa modulus 1024 exportable

2. Create an exportable copy of the key using the following command, where **passphrase** is a string used to encrypt the key for import (you can specify your own pass phrase):

   crypto key export rsa rekeyrsa pem terminal 3des passphrase

   This command prints out the public and private keys to the terminal, where you can copy them to the clipboard for import into the other key servers. The keys are demarcated by **----BEGIN/END PUBLIC KEY----** and **----BEGIN/END RSA PRIVATE KEY----**.Note that you can also export to a URL; see the *Cisco IOS Security Command Reference* on Cisco.com for detailed usage information.

3. Import the key into each of the other key servers using the following command:

   crypto key import rsa rekeyrsa pem exportable terminal passphrase

   When copying and pasting the keys, include the begin/end lines.

Configuring the IKE Proposal for GET VPN

Use the IKE Proposal for GET VPN page to define the IKE proposal to be used by the GET VPN topology. The IKE proposal is configured on the key servers and the group members.

These settings are for the ISAKMP security association (SA). If you are using a single key server, the ISAKMP SA is not used after initial group member registration. If you are using more than one key server (cooperative key servers), the ISAKMP SA is needed for communications among the key servers.

To open the IKE Proposal for GET VPN page:

- (Site-to-Site VPN Manager Window) Select an existing GET VPN topology and then select **IKE Proposal for GET VPN** in the Policies selector.
- (Policy view) Select **Site-to-Site VPN > IKE Proposal for GET VPN**, and then select an existing policy or create a new one.

The following table explains the settings you can configure in this policy.

Table 29-1 IKE Proposal for GET VPN Policy

Element	Description
IKE Proposal	The IKE proposal policy object that defines the settings you want to use. There are several predefined objects that you might be able to use as is. Click **Select** to open the list of existing IKE proposal objects. The object you select needs to use the same authorization method you are configuring for the group (for example, an object name with the prefix **preshared** when using preshared keys, or with the prefix **cert** when using Public Key Infrastructure (PKI) certificates). When you select an object and click **OK**, the settings defined in the object are displayed in the IKE Proposal Settings display fields. You can also see the settings by editing them in the selection list. If you do not find an appropriate pre-existing object, click the **Add (+)** button in the selection list and create a new object (see Configuring IKEv1 Proposal Policy Objects, page 26-10 for more information and detailed descriptions of the options).

Table 29-1 IKE Proposal for GET VPN Policy (continued)

Element	Description
IKE Proposal Overrides	The number of seconds that the ISAKMP SA for key servers and group members is valid. When the lifetime is exceeded, the SA expires and must be renegotiated between the peers. Values can be 1 to 86400. • If you are using cooperative key servers (more than one key server), set the key server lifetime high. The default 86400 is appropriate. • If you are using a single key server, you can set the lifetime low (but not less than 60 seconds) so that the ISAKMP SA is not retained unnecessarily. It is not used after a group member registers. • We recommend that you set the group member lifetime low as compared to the key server lifetime, especially when cooperative key servers are configured.

Related Topics

- Understanding IKE, page 26-5
- Understanding IKEv1 Preshared Key Policies in Site-to-Site VPNs, page 26-47
- Defining GET VPN Group Encryption, page 25-54
- Understanding Group Encrypted Transport (GET) VPNs, page 29-2
- Configuring GET VPN, page 29-12

Configuring Global Settings for GET VPN

Use the Global Settings for GET VPN page to define global settings for ISAKMP and IPsec that apply to devices in your GET VPN topology.

Note The lifetime settings in this policy do not apply to the ISAKMP security association lifetime for the key server and group members. Those lifetime values are configured in the IKE Proposal for GET VPN policy. For more information, see Configuring the IKE Proposal for GET VPN, page 29-15.

To open the Global Settings for GET VPN page:

- (Site-to-Site VPN Manager Window) Select an existing GET VPN topology and then select **Global Settings for GET VPN** in the Policies selector.
- (Policy view) Select **Site-to-Site VPN > Global Settings for GET VPN**, and then select an existing policy or create a new one.

The following table explains the settings you can configure in this policy.

Table 29-2 Global Settings for GET VPN

Element	Description
Enable Keepalive (Key Servers Only)	Whether to enable dead peer detection (DPD) keepalive messages between key servers. If there is more than one key server (cooperative key servers), you should enable periodic keepalive so the servers know each other's status and can elect a new primary server when necessary. Configure the following settings: • **Interval**—When you also select **Periodic**, the number of seconds between DPD messages. If you do not select Periodic, it is the number of seconds during which traffic is not received from the peer before DPD retry messages are sent. The range is from 10 to 3600 seconds. • **Retry**—The number of seconds between DPD retry messages if the DPD retry message is missed by the peer; the range is from 2 to 60 seconds. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the key server is marked as down. • **Periodic**—Whether to send DPD messages at regular intervals (regardless of traffic received from the other key servers). For GET VPN, you should select Periodic.
Identity	During Phase I IKE negotiations, peers must identify themselves to each other. Select the ISAKMP identity to use: • Address—(Default) The IP address of the interface that participates in IKE negotiations. Use the address if only one interface participates in negotiations, and its IP address is known (static). • Hostname—The fully-qualified host name (for example, router1.example.com). • Distinguished Name
SA Requests System Limit	The maximum number of SA requests allowed before IKE starts rejecting them. The specified value must equal or exceed the number of peers, or the VPN tunnels might be disconnected. You can enter a value in the range of 0-99999.
SA Requests System Threshold	The percentage of system resources that can be used before IKE starts rejecting new SA requests. The default is 75 percent.

Table 29-2 Global Settings for GET VPN (continued)

Element	Description
IPsec Settings	Select **Enable Lifetime** if you want to change the default lifetime settings for IPsec SAs. You can configure a lifetime based on the volume of traffic (in kilobytes) between group members, seconds, or both. The key expires when either of the values is reached. The defaults (which are configured even if you do not select this option) are: • **Lifetime (secs)**—3600 seconds (one hour). • **Lifetime (kbytes)**—4,608,000 kilobytes. **Tip** You can override these values for the traffic encryption key when configuring a security association. See Defining GET VPN Group Encryption, page 25-54 and Add New or Edit Security Association Dialog Box, page 25-58.

Related Topics

- Understanding IKE, page 26-5
- Understanding IPsec Proposals for Site-to-Site VPNs, page 26-19
- Understanding Group Encrypted Transport (GET) VPNs, page 29-2
- Configuring GET VPN, page 29-12

Configuring GET VPN Key Servers

Use the Key Servers policy to define key servers to be used by a GET VPN topology.

To open the Key Servers policy, in the Site-to-Site VPN Manager Window, select an existing GET VPN topology, then select **Key Servers** from the Policies list.

The table lists the key servers used in the VPN, showing the device name, identity, priority, and registration interface. For detailed information about these attributes, see Edit Key Server Dialog Box, page 29-19.

- To add a key server to the table, click the **Add Row** button and select the device from the list presented. Only devices that can be included as key servers are shown.
- To edit the characteristics of a key server, select it and click the **Edit Row** button. Fill in the Edit Key Server dialog box (see Edit Key Server Dialog Box, page 29-19).
- To delete a key server, select it and click the **Delete Row** button.
- To synchronize the RSA keys among the key servers, so that they all use the identical key, click the **Synchronize Keys** button. For detailed information about the key synchronization process, including when and why you would do it, see Generating and Synchronizing RSA Keys, page 29-13.
- To change the order of a key server when using cooperative key servers, select it and click the up or down arrow button. This order does not define which server is the primary key server (this is determined by the Priority value, the higher the value, the higher the likelihood that the server will be elected the primary key server).

  Instead, the order determines the default order in which group members will try to register with a key server. Group members register with the first key server in the list. If the first key server cannot be reached, group members register with the second key server, and so on. For more information

about key server redundancy, see Configuring Redundancy Using Cooperative Key Servers, page 29-7. Note that you can override this order for individual group members; see Configuring GET VPN Group Members, page 29-20 and Edit Group Member Dialog Box, page 29-21.

Tip You can toggle between showing the interface roles or the actual interfaces defined by those roles in the Identity and interfaces columns using the **Show** field below the table.

Related Topics

- Understanding the GET VPN Registration Process, page 29-4
- Understanding Group Encrypted Transport (GET) VPNs, page 29-2
- Configuring GET VPN, page 29-12
- Configuring VPN Topologies in Device View, page 25-19
- Filtering Tables, page 1-48

Add Key Server, Group Member Dialog Box

Use the Add Key Server and Add Group Member dialog boxes to select key servers or group members to be used in the GET VPN topology. Select the check box next to the desired devices and click **OK**.

Navigation Path

To add key servers or group members to a GET VPN topology, click the **Add Row (+)** button beneath the Key Server or Group Member table in the **GET VPN Peers** page of the Create VPN wizard, or for existing topologies, the **Key Servers** or **Group Members** policies. For detailed information, see the following topics:

- Defining GET VPN Peers, page 25-60
- Configuring GET VPN Key Servers, page 29-18
- Configuring GET VPN Group Members, page 29-20

Edit Key Server Dialog Box

Use the Edit Key Servers dialog box to change the attributes defined for a key server in a GET VPN topology.

Navigation Path

- (Create VPN Wizard) Go to the GET VPN Peers Page, select a key server and click the **Edit Row** button. See Defining GET VPN Peers, page 25-60.
- (Site-to-Site VPN Manager Window, page 25-18) Select the **Key Servers** policy, select a key server and click the **Edit Row** button. See Configuring GET VPN Key Servers, page 29-18.

Related Topics

- Understanding Group Encrypted Transport (GET) VPNs, page 29-2
- Configuring GET VPN, page 29-12

Field Reference

Table 29-3 Edit Key Server Dialog Box

Element	Description
Identity Interface	The interface that group members use to identify the key server and register with it. The default is the Loopback interface role, which identifies all Loopback interfaces.
Priority	A number between 1-100 that designates the role of the key server, either primary or secondary. The key server with the highest number becomes the primary key server. If two or more key servers are assigned the same priority, the device with the highest IP address is used. The default priority is 100 for the first key server, 95 for the second, and so on. **Note** There can be more than one primary key server if the network is partitioned.
Registration Interface	The interface on which group domain of interpretation (GDOI) registrations can be accepted. If you do not specify a registration interface, GDOI registrations can occur on any interface.

Configuring GET VPN Group Members

Use the Group Members policy to define the group members in a GET VPN topology.

To open the Group Members policy, in the Site-to-Site VPN Manager Window, select an existing GET VPN topology, then select **Group Members** from the Policies list.

The group members table lists the members of the GET VPN, showing the device name, GET-enabled interface, local interface, and security policy. For detailed information about these attributes, see Edit Group Member Dialog Box, page 29-21.

- To add a group member to the table, click the **Add Row** button and select the device from the list presented. Only devices that can be included as group members are shown.
- To edit the endpoint characteristics of a group member, select it and click the **Edit Row** button. Fill in the Edit Group Member dialog box (see Edit Group Member Dialog Box, page 29-21).

  If you select multiple group members in the table, you can also right-click and select the following commands to edit just these attributes:

  - **Edit Key Server Order**—To change the key server list and priority order for the selected group members.
  - **Edit Passive SA Mode**—To change whether the selected group members use passive SA mode.
- To delete a group member, select it and click the **Delete Row** button.

Tip You can toggle between showing the interface roles or the actual interfaces defined by those roles in the interfaces columns using the **Show** field below the table.

Related Topics

- Configuring Fail-Close to Protect Registration Failures, page 29-8
- Using Passive Mode to Migrate to GET VPN, page 29-23

- Understanding Group Encrypted Transport (GET) VPNs, page 29-2
- Configuring GET VPN, page 29-12
- Configuring VPN Topologies in Device View, page 25-19
- Filtering Tables, page 1-48

Edit Group Member Dialog Box

Use the Edit Group Members dialog box to change the attributes defined for a group member of a GET VPN topology.

Tip If you selected multiple devices and chose an edit command from the right-click menu, this dialog box shows only those options related to the edit command you chose.

Navigation Path

- (Create VPN Wizard) Go to the GET VPN Peers page, select a group member and click the **Edit Row** button. See Defining GET VPN Peers, page 25-60.
- (Site-to-Site VPN Manager Window, page 25-18) Select a GET VPN topology, then select the **Group Members** policy. Select a group member and click the **Edit Row** button. See Configuring GET VPN Group Members, page 29-20.

Related Topics

- Understanding Group Encrypted Transport (GET) VPNs, page 29-2
- Configuring GET VPN, page 29-12

Field Reference

Table 29-4 Edit Group Member Dialog Box

Element	Description
GET-Enabled Interface	The VPN-enabled outside interface to the provider edge (PE). Traffic originating or terminating on this interface is evaluated for encryption or decryption, as appropriate. You can configure multiple interfaces. Enter the name of the interface or interface role, or click **Select** to select it from a list or to create a new interface role.
Interface to be used as local address	The interface whose IP address is used to identify the group member to the key server for sending data, such as rekey information. If GET is enabled on only one interface, you do not need to specify the interface to be used as the local address. If GET is enabled on more than one interface, you must specify the interface to be used as the local address. Enter the name of the interface or interface role, or click **Select** to select it from a list or to create a new interface role.

Table 29-4 Edit Group Member Dialog Box (continued)

Element	Description
Security Policy	The local group member security ACL used to deny some group member-specific traffic over and above the security ACL downloaded from the key server. Denied traffic is sent in clear text rather than encrypted. For detailed information, see Understanding the GET VPN Security Policy and Security Associations, page 29-10. Enter the name of the ACL object or click **Select** to select it from a list or to create a new object.
Enable Fail Close Fail Close ACL	Whether to enable fail-close mode on the device, which prevents the device from transmitting clear text traffic before the device successfully registers with the key server. Fail-close mode requires as a minimum Cisco IOS Software release 12.4(22)T or 15.0; you can also configure it on all supported ASRs. **Tip** Fail-close mode is a complex feature, and you must carefully construct the fail-close ACL or you might lock yourself out of the device. Before enabling fail-close mode, read Configuring Fail-Close to Protect Registration Failures, page 29-8. You must select an ACL policy object that identifies allowable clear text traffic (using deny statements), such as SSH and SSL communications with the Security Manager server to allow for configuration updates. Enter then name of the object or click **Select** to select it or to create a new object.
Override Key Servers	Whether to override the key server list configured for the GET VPN topology as a whole for this particular group member. If you select this option, you can choose a subset of the key servers configured for the topology to be used by the selected group member, and change their priority order. This can help you load-balance registration activity among a group of cooperative key servers. For more information, see Configuring Redundancy Using Cooperative Key Servers, page 29-7. Click **Select** to change the key server list and priority order of the key servers using the Key Servers Selection dialog box. A key server must be defined for the GET VPN topology before you can modify its use for a group member.

Table 29-4 Edit Group Member Dialog Box (continued)

Element	Description
Enable Passive SA Mode	Whether to put the group member into passive security association (SA) mode, which means the group member installs the SA in the inbound direction only. This means the group member can receive encrypted data, but it sends clear text data only. This mode is useful for testing the VPN only, primarily when you are migrating from an existing VPN to a GET VPN. (The group member must be running Cisco IOS Software version 12.4(22)T or 15.0 at minimum, or be a supported ASR, to use this mode.) This setting is similar to the **Receive Only** setting in the Group Encryption Policy, which applies to the topology as a whole. This group member option overrides the setting in the Group Encryption Policy. For detailed information on how you can use these passive mode features to migrate or test a GET VPN, see Using Passive Mode to Migrate to GET VPN, page 29-23.

Using Passive Mode to Migrate to GET VPN

If you are migrating an existing VPN to the GET VPN technology, especially a clear-text VPN, you can use two features to help you migrate in a phased approach to help prevent network down-time. The features are essentially the same, and involve the passive acceptance of encrypted traffic, but you configure them on different devices in the GET VPN.

Normally, in a fully-deployed GET VPN, traffic is encrypted in both directions (bidirectional security associations, or SAs). However, during testing, you can use passive mode. In passive mode, the group member installs the SA in the inbound direction only, so that the group member receives encrypted traffic but sends traffic in clear text. You can then test the VPN to ensure that it is performing as expected before turning on full encryption.

Use the following features to configure passive mode in a GET VPN:

- **SA Receive-only mode**—You configure receive-only mode for security associations on the key servers in the topology using the Group Encryption Policy. Thus, the setting applies to the entire topology.
- **Passive SA mode**—You configure passive security association mode on individual group members. This setting overrides the SA receive-only setting; thus, you can turn on full encryption for the entire topology, but leave some group members in passive mode. This lets you test the group members in stages and enable full encryption after you verify each member device.

Tip Passive SA mode on group members requires Cisco IOS Software release 12.4(22)T+ or 15.0+, or Release 2.3 (12.2(33)XNC)+ on ASRs.

The following procedure shows an example of the end-to-end migration process you might follow to convert to GET VPN using these passive mode features.

Related Topics

- Understanding Group Encrypted Transport (GET) VPNs, page 29-2
- Configuring GET VPN, page 29-12

Step 1 Create the new GET VPN topology in Security Manager using the Create VPN wizard. When you are in the wizard, ensure that you make these selections:

- When selecting devices, choose the key servers for the topology, but for group members, select the first set of group members that will be migrated. For more information, see Selecting Devices for Your VPN Topology, page 25-32.
- When configuring the group encryption settings, select **Receive Only**. This enables the SA receive-only feature for the entire topology. For more information, see Defining GET VPN Group Encryption, page 25-54.

For information about creating VPNs, see Creating or Editing VPN Topologies, page 25-28.

Step 2 Deploy the configurations to all devices in the VPN. The group members should now be able to receive encrypted traffic but not send it. For information on the deployment process, see the following topics based on the Workflow mode you are using:

- Deploying Configurations in Non-Workflow Mode, page 8-28
- Deploying Configurations in Workflow Mode, page 8-34

Step 3 Outside of Security Manager, verify that all of the group members are functioning properly.

For example, you can test whether the group members are able to send and receive encrypted packets using some CLI commands on the group member devices:

- On group member 1, configure the following command, where “groupexample” is the name of the GDOI group for the VPN. This command sets the device to accept encrypted or clear text, but to send only clear text.

  crypto gdoi gm group groupexample ipsec direction inbound only

- On group member 2, configure the following command. This command sets the device to accept encrypted or clear text, but to send encrypted text.

  crypto gdoi gm group groupexample ipsec direction inbound optional

- Ping group member 1 from group member 2. Group member 2 should encrypt the packet before sending it, and group member 1 should accept it and decrypt it. If you ping member 2 from member 1, the ping should be sent in clear text and accepted by member 2. Ensure that your ACLs allow pings.

Step 4 In Security Manager, select **Manage > Site-to-Site VPNs** (see Site-to-Site VPN Manager Window, page 25-18).

Select the GET VPN topology, then select **Group Members**.

Add the remaining group members that you want to add to the topology (click the **Add Group Member (+)** button, select the devices, and click **OK**).

If you want to use passive mode to test the new group members before enabling full encryption, ensure that you select **Enable Passive SA Mode** when configuring the group members:

- To configure an individual group member, select it and click the **Edit Group Member (pencil)** button.
- To enable passive mode on more than one device at a time, use Shift+click or Ctrl+click to select multiple devices, then right-click and select **Edit Passive SA Mode**. You can then select the option and click **OK**.

For more information on configuring group members, see Configuring GET VPN Group Members, page 29-20.

Step 5 Deploy the configuration changes to all devices in the VPN. All devices should be operating in passive mode at this point.

Step 6 In the Site-to-Site VPN Manager, select the GET VPN topology, then select **Group Encryption Policy**.

Deselect **Receive Only**. This turns off SA receive-only mode at the topology level.

Step 7 Deploy the configuration changes to all devices in the VPN. Now the GET VPN should be operating in fully encrypted mode for the original group members that you tested. Any new members that you added with passive SA mode enabled should be receiving encrypted traffic and sending clear text traffic.

Step 8 Use the following process to verify the new devices and to turn off passive mode. You can follow this process for all new devices at once, or you can do smaller groups of them at a time. You can also use this process for new group members as you extend your network. Iterate the following steps as appropriate:

a. Verify that the new group members are functioning properly using the same techniques that you used to verify the original group members.

b. When you are ready to move a set of group members to fully-encrypted mode, in the Site-to-Site VPN Manager, select the GET VPN topology and select **Group Members**.

c. Select all passive mode group members that should use full encryption, right-click and select **Edit Passive SA Mode**. Deselect the **Enable Passive SA Mode** option and click **OK**.

d. Deploy configurations to all devices in the VPN, not just the ones whose passive mode you changed. Normally, you should not deploy to less than all devices in a VPN.

Troubleshooting GET VPN Configurations

If after provisioning and deploying GET VPN using Security Manager, the GET VPN is not working, check the following:

- Ensure that the RSA key is synchronized among all cooperative key servers (that is, the RSA key is the same). For information on how to synchronize keys, see Generating and Synchronizing RSA Keys, page 29-13.
- If desired traffic is not being encrypted, make sure the key server security policy ACL (security association) has a permit ACE for the desired traffic. For asymmetric ACEs (where the source and destination addresses are different), ensure that there is a mirrored ACE (with the source and destination addresses reversed). For more information, see Understanding the GET VPN Security Policy and Security Associations, page 29-10.
- For multicast rekey, make sure that the network is multicast enabled and that all key servers and most group members are configured to enable multicast. You must enable multicast on the devices directly; Security Manager does not provision the commands required to enable multicast. For more information, see Choosing the Rekey Transport Mechanism, page 29-6.
- When using multicast rekey, check whether there is a deny ACE in the key server security ACL for the multicast group address to prevent encryption of multicast rekey messages.
- Check that the local security ACL on the group member has only deny ACEs. If you include a permit statement in an attempt to identify traffic that should be encrypted, the matching traffic is actually dropped because there is no corresponding IPsec SA. Because the permit entry is defined in the group member, the key server is not aware of it and cannot generate the required IPsec SA. For more information, see Understanding the GET VPN Security Policy and Security Associations, page 29-10.
- For group member authorization using certificates, check that the ISAKMP authentication uses certificates and that a PKI policy is configured. ISAKMP identity on the group member and key server should be set to use the distinguished name (dn).

- Normally, network address translation (NAT) is not used in the type of WAN environments where GET VPN is deployed. However, if you use NAT, ensure that the security policy ACL has permit statements for the translated addresses. Also, if you are using Network Address Translation-Traversal (NAT-T), the GDOI protocol port changes to 4500.
- A control plane replay protection mechanism was added to Cisco IOS Software releases 12.4(15)T10, 12.4(22)T3, 12.4(24)T2, 15.0(1)M, and 12.2(33)XNE. This mechanism is not backward-compatible, so if any GET VPN group member in the network is running any of these (or later) releases, you must also upgrade all key servers to one of these (or newer) releases. Otherwise, network disruption might occur because of a failed rekey, which causes one of the following system logging (syslog) messages to appear:
  - %GDOI-3-GDOI_REKEY_SEQ_FAILURE: Failed to process rekey seq # 2 in seq payload for group get-group, last seq # 6
  - %GDOI-3-PSEUDO_TIME_TOO_OLD: Rekey received in group get-group is too old and failed PST check: my_pst is 184 sec, peer_pst is 25 sec, allowable_skew is 10 sec

Tip For additional troubleshooting tips from the CLI configuration perspective, including information about valuable **show** commands, see *Cisco Group Encrypted Transport VPN* on Cisco.com.

Related Topics

- Understanding Group Encrypted Transport (GET) VPNs, page 29-2
- Configuring GET VPN, page 29-12