

GET VPN Resiliency

The GET VPN Resiliency feature improves the resiliency of Cisco Group Encrypted Transport (GET) VPN so that data traffic disruption is prevented or minimized when errors occur.

- Prerequisites for GET VPN Resiliency, on page 1
- Restrictions for GET VPN Resiliency, on page 1
- Information About GET VPN Resiliency, on page 1
- How to Configure GET VPN Resiliency, on page 3
- Configuration Examples for GET VPN Resiliency, on page 9
- Additional References for GET VPN Resiliency, on page 10
- Feature Information for GET VPN Resiliency, on page 11

Prerequisites for GET VPN Resiliency

All key servers (KSs) and group members (GMs) on which you want to enable this feature must be running GET VPN software version 1.0.4 or higher. You should use this feature only after all devices in the GET VPN network are upgraded to GET VPN software versions that support this feature. This feature provides a command that you use on the KS (or primary KS) to check whether all devices in the network are running versions that support this feature. For more information, see the "*Ensuring That GMs Are Running Software Versions That Support Long SA Lifetime*" section.

Restrictions for GET VPN Resiliency

- All key servers (KSs) and group members (GMs) must be upgraded for Long SA Lifetime.

Information About GET VPN Resiliency

Long SA Lifetime

The long security association (SA) lifetime functionality extends the maximum lifetime of the key encryption key (KEK) and traffic encryption key (TEK) from 24 hours to 30 days. This functionality also lets you configure key servers (KSs) to continue to send periodic reminder rekeys to group members (GMs) that do not respond with an acknowledgment in the last scheduled rekey.

By using a long SA lifetime in combination with periodic reminder rekeys, a KS can effectively synchronize GMs if they miss a scheduled rekey before the keys roll over.



Note For a lifetime longer than 24 hours, the encryption algorithm must be Advanced Encryption Standard-cipher block chaining (AES-CBC) or Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) with an AES key of 128 bits or stronger.

You can use the long SA lifetime functionality along with the GETVPN Suite-B feature to use AES-GSM and Galois Message Authentication Code-Advanced Encryption Standard (GMAC-AES) as traffic encryption key (TEK) policy transforms in a group for packets encapsulated with GCM-AES and GMAC-AES.

Migrating to Long SA Lifetime

When migrating to the long SA lifetime functionality (greater than or equal to one day), the following rules apply:

- When a long SA lifetime is configured on a crypto IPsec profile, GETVPN displays a warning message to not use the IPsec profile for a non- Group Domain of Interpretation (GDOI) group.
- If group members are registered to a key server with short SA lifetime and the key server changes the policy to long SA lifetime, GETVPN checks the software version of all the GMs when the **crypto gdoi ks rekey** command is configured to initiate the policy change. If the GMs registered with the KS do not support long SA lifetime, a message is displayed to discourage the policy change until all GMs are upgraded.
- When the Long SA feature is enabled in KS, it will block registration from GMs running older Cisco IOS releases, which does not support this feature.

Clock Skew Mitigation

Sometimes with longer security association (SA) lifetimes, a group member (GM) may not receive updates from a key server for a longer duration. This may result in group members experiencing clock skew for key encryption key (KEK) lifetime, traffic encryption key (TEK) lifetime, and Time-Based Anti-Replay (TBAR) pseudotime. The refresh rekey and rollover to new outbound IPsec SA helps GMs in mitigating clock skew issues.

Refresh Rekey

If the traffic encryption key (TEK) lifetime is set for a duration greater than two days and Time-Based Anti-Replay (TBAR) is disabled, a key server sends a refresh rekey every 24 hours which updates the key encryption key (KEK) lifetime, TEK lifetime, and TBAR pseudotime on all group members (GMs). In simple terms, a refresh rekey is a retransmission of the current KEK policy, TEK policy, and TBAR pseudotime (if enabled) to all GMs, regardless of the status of receiving a unicast acknowledgment (ACK) for the last rekey. If TBAR is enabled, the refresh rekey is sent every two hours to synchronize the pseudotime, so that an additional refresh rekey is not required.

Rollover to New Outbound IPsec SA

When a long SA lifetime (greater than one day) is configured, the rollover happens when the remaining lifetime of the traffic encryption key (TEK) reaches 1% of the old TEK configured lifetime that has a lower limit of 30 seconds and not 30 seconds of the old TEK's remaining lifetime. This allows a greater clock skew between

the group members (GMs) before discarding traffic from one GM rolling over to the new TEK late (after the other GM has already deleted the old TEK). This mitigates the GM from being “offline” (disconnected from the KS) for a long duration and from being unable to receive the refresh rekeys to mitigate the clock skew.

Periodic Reminder Sync-Up Rekey

The periodic reminder sync-up rekey functionality in the key server (KS) lets you to send periodic reminder rekeys to group members (GMs) who do not respond with an acknowledgment (ACK) in the last scheduled rekey. This functionality in combination with the long SA lifetime functionality is effective for a KS to synchronize with GMs when they miss a scheduled rekey before the keys rollover. In a KS group configuration, a new keyword **periodic** is added to the **rekey retransmit** command when configuring the rekey retransmission.

Each periodic rekey increments the sequence number, similar to rekey retransmissions. The GM is removed from the database on the KS after 3 scheduled rekeys (not retransmissions) for which the GM does not send an ACK.

Pre-Positioned Rekey

The pre-positioned rekey functionality allows the key server (KS) to send a rekey earlier than half the duration of the SA lifetime, when a longer SA lifetime (greater than one day) is configured. The normal behavior of sending the rekey is used for a short SA lifetime. When group members (GMs) receive this early rekey, they continue to use the old TEK as outbound until rolled over to the new TEK as outbound. The pre-positioned rekey feature along with the Long SA Lifetime feature improves key rollover stability. This functionality allows the (KS) sufficient time to recover rekey errors, such as periodic reminder rekeys and synchronize rekeys.

How to Configure GET VPN Resiliency

Ensuring That GMs Are Running Software Versions That Support Long SA Lifetime

You should use the Long SA Lifetime feature only after all devices in the GET VPN network are upgraded to GET VPN software versions that support this feature.

Perform this task on the key server (or primary key server) to ensure that all devices in the network support long SA lifetime.

SUMMARY STEPS

1. **enable**
2. **show crypto gdoi feature long-sa-lifetime**
3. **show crypto gdoi feature long-sa-lifetime | include No**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto gdoi feature long-sa-lifetime** **Example:** `Device# show crypto gdoi feature long-sa-lifetime`	Displays the version of the GET VPN software running on each KS and GM in the GET VPN network and displays whether that device supports long SA lifetime.
Step 3	**show crypto gdoi feature long-sa-lifetime | include No** **Example:** `Device# show crypto gdoi feature long-sa-lifetime | include No`	(Optional) Displays only those devices that do not support long SA lifetime.

Configuring Long SA Lifetime

Configuring Long SA Lifetime for TEK

To configure long SA lifetime for traffic encryption key (TEK), perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **set security-association lifetime days** *days*
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**crypto ipsec profile** *name* **Example:** `Device(config)# crypto ipsec profile gdoi-p`	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec devices and enters crypto IPsec profile configuration mode.
Step 4	**set security-association lifetime days** *days* **Example:** `Device(ipsec-profile)# set security-association lifetime days 15`	Configures the security association (SA) lifetime to over one day. • The maximum number of days is 30.
Step 5	**end** **Example:** `Device(ipsec-profile)# end`	Exits crypto IPsec profile configuration mode and returns to privileged EXEC mode.

Configuring Long SA Lifetime for KEK

To configure long SA lifetime for key encryption key (TEK), perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*
5. **server local**
6. **rekey lifetime days** *days*
7. **end**

DETAILED STEPS

Procedure

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

	Command or Action	Purpose
Step 4	**identity number** *number* **Example:** `Device(config-gdoi-group)# identity number 3333`	Identifies a GDOI group number.
Step 5	**server local** **Example:** `Device(config-gdoi-group)# server local`	Designates a device as a GDOI key server and enters GDOI local server configuration mode.
Step 6	**rekey lifetime days** *days* **Example:** `Device(gdoi-local-server)# rekey lifetime days 20`	Limits the number of days or seconds for a KEK.
Step 7	**end** **Example:** `Device(gdoi-local-server)# end`	Exits GDOI local server configuration mode and returns to privileged EXEC mode.

Configuring the Periodic Reminder Sync-Up Rekey

To configure the periodic reminder sync-up rekey, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*
5. **server local**
6. **rekey retransmit** *number-of-seconds* **periodic**
7. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**crypto gdoi group** *group-name* **Example:** `Device(config)# crypto gdoi group group1`	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	**identity number** *number* **Example:** `Device(config-gdoi-group)# identity number 3333`	Identifies a GDOI group number.
Step 5	**server local** **Example:** `Device(config-gdoi-group)# server local`	Designates a device as a GDOI key server and enters GDOI local server configuration mode.
Step 6	**rekey retransmit** *number-of-seconds* **periodic** **Example:** `Device(gdoi-local-server)# rekey retransmit 10 periodic`	Specifies the number of times the rekey message is periodically retransmitted. • If this command is not configured, there will be no retransmits.
Step 7	**end** **Example:** `Device(gdoi-local-server)# end`	Exits GDOI local server configuration mode and returns to privileged EXEC mode.

Verifying and Troubleshooting GET VPN Resiliency

Verifying and Troubleshooting GET VPN Resiliency on a Key Server

To view the configuration that is running on a key server (KS), use the **show running-config** command and the following commands.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show crypto gdoi** **Example:** `Device# show crypto gdoi`	Displays the current GDOI configuration and the policy that is downloaded from the KS.
Step 3	**show crypto gdoi ks rekey** **Example:** `Device#  show crypto gdoi ks rekey`	Displays information about the rekeys that are sent from the KS.

Verifying and Troubleshooting GET VPN Resiliency on a Group Member

To view the configuration that is running on a group member (GM), use the **show running-config** command and the following commands.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto gdoi ks rekey** **Example:** `Device#  show crypto gdoi ks rekey`	Displays information about the rekeys that are sent from the KS.
Step 3	**show crypto gdoi ks policy** **Example:** `Device# show crypto gdoi ks policy`	Displays the time until the next rekey.

Configuration Examples for GET VPN Resiliency

Example: Ensuring That GMs Are Running Software Versions That Support Long SA Lifetime

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to check whether all the devices in each group support long SA lifetimes:

```
Device# show crypto gdoi feature long-sa-lifetime

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.4          Yes
        10.0.6.2         1.0.4          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.4          Yes
        10.0.3.2         1.0.4          Yes
```

You can also enter the above command on a GM (which will display the information for the GM but not for the KS or other GMs).

The following example shows how to enter the command on the KS (or primary KS) find only those devices in the GET VPN network that do *not* support long SA lifetimes:

```
Device# show crypto gdoi feature long-sa-lifetime | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

Example: Configuring Long SA Lifetime

Example: Configuring Long SA Lifetime for TEK

The following example shows how to configure the long SA lifetime for traffic encryption key (TEK):

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec profile gdoi-p
Device(ipsec-profile)# set security-association lifetime days 15
Device(ipsec-profile)# end
```

Example: Configuring Long SA Lifetime for KEK

The following example shows how to configure the long SA lifetime for key encryption key (KEK):

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey lifetime days 20
Device(gdoi-local-server)# end
```

Example: Configuring the Periodic Reminder Sync-Up Rekey

The following example shows how to configure the periodic reminder sync-up rekey:

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group group1
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey retransmit 10 periodic
Device(gdoi-local-server)# end
```

Additional References for GET VPN Resiliency

Related Documents

Related Topic	Document Title
Cisco IOS security commands	• *Cisco IOS Security Command Reference Commands A to C* • *Cisco IOS Security Command Reference Commands D to L* • *Cisco IOS Security Command Reference Commands M to R* • *Cisco IOS Security Command Reference Commands S to Z*
Basic deployment guidelines for enabling GET VPN in an enterprise network	*Cisco IOS GET VPN Solutions Deployment Guide*
Designing and implementing a GET VPN network	*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*

Standards and RFCs

Standard/RFC	Title
RFC 2401	*Security Architecture for the Internet Protocol*
RFC 6407	*The Group Domain of Interpretation*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for GET VPN Resiliency

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for GET VPN Resiliency

Feature Name	Releases	Feature Information
GET VPN Resiliency		The following commands were introduced or modified: **rekey lifetime, rekey retransmit, set security-association lifetime, show crypto gdoi.**