Perfect Forward Secrecy for GETVPN

If a Group Member (GM) is compromised, an attacker may access saved long-term keys and messages. With Perfect Forward Secrecy (PFS) for GETVPN, the attacker cannot use the keys and messages to obtain the keys of past or future sessions. Thus, the attacker may use the compromised Traffic Encryption Key (TEK) to decrypt the communication of the current session, but cannot decrypt recorded or future communication.

Feature Information for PFS for GETVPN

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 PFS for GETVPN

Feature Name	Releases	Feature Information
Perfect Forward Secrecy for GETVPN	Cisco IOS XE Gibraltar 16.12.1	The following commands are introduced or modified: **show crypto gkm feature pfs**, **pfs**, **show crypto gdoi**, and **client pfs**.

Information About PFS for GETVPN

Overview of PFS for GETVPN

Suppose a device is compromised and an attacker accesses the long-terms keys saved on it. For Perfect Forward Secrecy (PFS), the attacker must not be able to use the long-term keys to obtain keys and decrypt recorded communication of past sessions. A related security measure is called Perfect Backward Secrecy (PBS). For PBS, the attacker must not be able to use the long-term keys to obtain keys and decrypt communication of future sessions.

If a GM is compromised, an attacker may access saved long-term keys and messages. The attacker may so obtain the Diffie Hellman (DH) result and the registration message or the Key Encryption Key (KEK) and past rekey messages. With PFS for GETVPN, the attacker cannot use the keys and messages to obtain TEKs of past sessions. In addition, the attacker cannot use the KEK to decrypt future rekey messages, and so, cannot obtain TEKs of future sessions. Thus, the attacker has access only to the TEK of the current session. Despite the compromised keys, any recorded or future communication remains secure.

PFS for GETVPN comprises the following changes:

- A modified rekey process; the GM registration mechanism is unchanged.
- If you enable PFS for GETVPN, the default lifetime of the GM-KS IKEv2 channel changes from 1 day to 600 seconds.

  However, if you have configured customized lifetime, the lifetime does not change after you enable PFS for GETVPN.
- Key Servers (KSs) and Group Members (GMs) that support PFS for GETVPN have new version numbers. The version numbers support backward compatibility and interactions with third-party GMs.

Restrictions for PFS for GETVPN

- A Key Server (KS) and a Group Member (GM) must communicate using the IKEv2 protocol. PFS for GETVPN is not supported when KS and GM communicate using the IKEv1 protocol.
- Enable PFS on all the KSs in a COOP. On a GM, PFS is enabled by default.
- Both scheduled rekey and manually triggered rekey cause a GM to reregister with a KS. The reregistration may cause a noticeable overhead at the KS, especially at scale.
- Force rekey can cause traffic loss because of a key mismatch between GMs.
- When the RSA key size is 4096, because of the large size of the key, the Crypto Engine takes considerable time for a rekey signing. During a rekey signing, if too many registration requests are received, the Crypto Engine may be overloaded. An overloaded Crypto Engine logs the following error message:

  ```
  %ACE-3-TRANSERR: IOSXE-ESG(9): IKEA trans 0x11A8; opcode 0x23; param 0x0; error 0xC;
  retry cnt 0
  ```

  You may see this error message more frequently in a GETVPN deployment that uses an RSA key size of 4096, has more than 100 GMs, and has PFS enabled. The increased frequency is because when PFS is enabled, every rekey triggers a re-registration, and with more than a 100 GMs, the Crypto Engine is more likely to receive several registration requests during a rekey signing and may be overloaded.

  Similarly, you may see this error message more frequently in such a deployment if you run the **crypto gdoi ks rekey replace-now** command repeatedly due to the registration requests triggered by this command.

  In a GETVPN deployment with PFS enabled, we recommend that you use an RSA key size of 2048. Using an RSA key size of 4096 is not necessary because the rekey message does not contain TEK/KEK keys.

Modified Rekey Process

PFS for GETVPN ensures that an attacker cannot use the KEK from a compromised GM to decrypt past or future rekey messages. Thus, the attacker cannot obtain past or future KEKs or TEKs. For this purpose, PFS for GETVPN modifies the rekey mechanism so that rekey messages do not include KEKs or TEKs. The contents of the rekey message depend on the type of rekey.

Scheduled Rekey

1. When the rekey timer for KEK or TEK expires, KS generates a new KEK or TEK, respectively.
2. KS sets a private attribute in the GSA payload of the rekey message and encrypts the message with the current KEK. The rekey message does not include the new KEK or TEK. KS sends the rekey message to the GM.
3. GM receives the rekey message and decrypts the message using the current KEK. GM identifies the scheduled rekey and starts a reregistration timer for a random time interval in the 0–6 seconds range.
4. When the reregistration timer expires, GM initiates reregistration with the KS.
5. After reregistration, KS sends the KEK or TEK to the GM over the IKEv2 channel.
6. On receiving a new KEK, GM replaces the old KEK with the new KEK.
7. On receiving a new TEK, GM checks the Activation Time Delay (ATD) for the TEK. If the ATD is non-zero, GM starts a timer to enforce ATD before installing the TEK in the data plane.

   ATD is calculated on the KS as follows:

   a. If Long SA lifetime is configured, the ATD timer is initialized to a value in seconds computed as follows:
   ATD = (remaining lifetime of old TEK) - (1% of remaining lifetime of old TEK) - 75

      The new TEK rolls over at (1% of remaining lifetime of old TEK).

   b. If Long SA lifetime is not configured, the ATD timer is initialized to a value is seconds computed as follows:
   ATD = (remaining lifetime of old TEK) - 75

      The new TEK rolls over 30 seconds before the expiry of the old TEK.

Sync-up Rekey

1. KS sends a GM a rekey message that includes only the pseudoTimeStamp (PST) value.

   The message does not contain KEK or TEK.
2. On receiving the rekey message, GM updates its pseudotime value and does not trigger any reregistration. Depending on the pseudoTimeStamp value received from the KS and the TimeBased Anti Replay (TBAR) window configured on the GM, GM may generate syslog messages.

Manually Triggered Key

1. When you trigger a rekey operation using **crypto gdoi ks** or **clear crypto gdoi ks members**, KS sends the GAP/DELETE payload based on the rekey type.

   • Rekey message without policy change

Table 2: GAP/DELETE Payload for a Rekey Message Without Policy Change

Type	KEK	TEK	Private Attribute for Rekey	KD	GAP	DELETE
`crypto gdoi ks rekey`	No	No	No	No	No	No
`crypto gdoi ks rekey replace-now`	No	No	Yes	No	ATD 1 sec	No
`clear crypto gdoi ks members`	No	No	No	No	ATD 5% of TEK	Yes
`clear crypto gdoi ks members now`	No	No	Yes	No	ATD 1 sec	Yes

   • Rekey message with policy change

Table 3: GAP/DELETE Payload for a Rekey Message with Policy Change

Type	KEK	TEK	Private Attribute for Rekey	KD	GAP	DELETE
`crypto gdoi ks rekey`	No	No	Yes	No	ATD 5% of TEK	No
`crypto gdoi ks rekey replace-now`	No	No	Yes	No	ATD 1 sec	No
`clear crypto gdoi ks members`	No	No	No	No	ATD 5% of TEK	Yes
`clear crypto gdoi ks members now`	No	No	Yes	No	ATD 1 sec	Yes

2. On receiving the rekey message, GM initiates reregistration with the KS.
3. As part of GM reregistration, KS sends the KEK or TEK to the GM over the IKEv2 channel.
4. GM sets the lifetime of the old key to the Activation Time Delay (ATD) value sent by the KS. After the ATD, GM deletes the old key and installs the new key.

Suite-B Support

During the first registration of a GM, KS assigns a unique Sender Identifier (SID) and Initialization Vector (IV) range to the GM. When a GM re-registers with a KS in response to a rekey message, the GM provides the SID that the KS assigned during registration. KS does not assign new a SID or Initialization Vector (IV) range to the GM.

KS and GM Versions for PFS for GETVPN

If Cisco IOS XE Gibraltar 16.12.1 or a later release is installed on a GM, PFS for GETVPN is enabled by default. You can disable PFS for GETVPN using the command-line interface. The GM version varies based on whether PFS is enabled or not as summarized in the following table.

	Without Suite-B Support	With Suite-B Support	ASR 1000 Series
PFS disabled	16	17	19
PFS enabled	21	22	20

If Cisco IOS XE Gibraltar 16.12.1 or a later release is installed on a KS, PFS for GETVPN is disabled by default and the KS version is 1.0.18. You can enable PFS for GETVPN via the CLI. With PFS for GETVPN enabled, the KS version is 1.0.23. Enable PFS for GETVPN on all the cooperative KSs.

KS sends rekey messages to GMs based on the GM version:

- To GMs that have PFS for GETVPN disabled and send a version number such as 1.0.17 or 1.0.19, KS sends rekey messages that have the KEK or TEK.

  KS sends rekey messages that have the KEK or TEK to GMs that have PFS for GETVPN disabled and to non-Cisco GMs. GMs that have PFS for GETVPN disabled send a version number such as 1.0.17 or 1.0.19 to the KS. Non-Cisco GMs send an unknown version number to the KS.

- KS sends modified rekey messages that do not have KEK or TEK to GMs that have PFS for GETVPN enabled. GMs that have PFS for GETVPN enabled send a version number such as 1.0.20 or 1.0.22

Upgrading KS and GM for PFS for GETVPN

For PFS for GETVPN to be effective, enable PFS on every KS and GM in the network. If you do not enable PFS for GETVPN on a GM and the GM is breached, compromised keys can hamper the security of the entire network.

Upgrade the KSs in the network as follows:

Note We recommend that you upgrade KSs while there is sufficient time for the expiry of KEK and TEKs.

1. Upgrade a Secondary KS and wait for the COOP election to complete.
2. Repeat Step 1 for each Secondary KS in the COOP.

   The Secondary KSs reboot and synchronize with the Primary KS and assume the role of Secondary KSs.

3. Upgrade the Primary KS.

   One of the Secondary KSs is elected as the new Primary KS. The upgraded KS reboots and assumes the role of a Secondary KS.

4. Enable PFS on all the KSs.

After the upgrade, KS sends rekey messages based on the version number that GMs send. Based on the GM version number, KS sends rekey messages that contain KEK or TEK, or modified rekey messages without KEK or TEK.