GET VPN Interoperability

The D3P Support on GETVPN Key Server, Activation Time Delay, and GDOI Interop ACK for Cisco GETVPN Key Server features enhance interoperability between key servers and group members.

- Prerequisites for GET VPN Interoperability, on page 1
- Restrictions for GET VPN Interoperability, on page 1
- Information About GET VPN Interoperability, on page 2
- How to Configure GET VPN Interoperability, on page 6
- Configuration Examples for GET VPN Interoperability, on page 12
- Additional References for GET VPN Interoperability, on page 13
- Feature Information for GET VPN Interoperability, on page 14

Prerequisites for GET VPN Interoperability

- To enable the feature for a group, ensure that all the devices in a group are running compatible Cisco IOS software and Group Domain of Interpretation (GDOI) versions.
- Enable the Unicast Rekey functionality on a GDOI group before configuring the Internet-Draft ACK for Cisco GETVPN Key Server and Activation Time Delay features.

Restrictions for GET VPN Interoperability

- The IP-D3P support on GETVPN Key Server feature cannot coexist with the GETVPN Resiliency - GM Error Detection and GET VPN Support of IPsec Inline Tagging for Cisco TrustSec features. The latter features must be disabled before enabling IP-D3P support on a GET VPN key server and the IP-D3P must be disabled before enabling GETVPN Resiliency support on GETVPN Key Server.
- The Activation Time Delay feature supports only on IPsec security association. Multiple IPsec SA must not be configured.
- Cisco-Metdata and IP-D3P cannot coexist. When switching between CMD-feature and IP-D3P, the keyserver must perform **crypto gdoi ks rekey replace** to all the GMs to make sure these two features are not enabled simultaneously.
- ASR1K supports IP-D3P only in GETVPN IPv4 tunnel mode.

Information About GET VPN Interoperability

Overview of IP-Delivery Delay Detection Protocol (IP-D3P)

IP datagrams can be subject to a delivery delay attack, where a host or gateway receives datagrams that are not fresh. A fresh datagram is defined as a “Recently generated; not replayed from some earlier interaction of the protocol.” An IP-D3P datagram consists of a header and an IP payload. The IP-D3P header includes a timestamp that is used by the receivers of the packet to determine if the packet has been recently generated. Receivers compare the timestamp delivered in the IP packet to their local time and thus determine whether the packet should be accepted.

IP-D3P uses the system clock of group members to create and verify the IP-D3P datagram’s timestamp. In most cases, the system clock is set from an external protocol, such as Network Time Protocol (NTP) to synchronize the system clocks of the sender and receiver.

The D3P support on GETVPN Key Server feature enables support for IP-D3P on GET VPN.

IP-D3P Support for Key Server

A new configuration command, **d3p**, in the GDOI local server configuration mode allows you to enable IP-D3P on a key server. After you enable the D3P command, the primary key server issues a rekey to all the group members having a Group Associated Policy (GAP) payload with D3P attributes. The GAP payload includes the following attributes in the rekey message:

- D3P-TYPE—Portable Operating System Interface (POSIX) time, in milliseconds.
- D3P-WINDOWSIZE—IP-D3P window size, in milliseconds.

The **show crypto gkm ks** command displays the IP-D3P parameters that are enabled on a key server.

IP-D3P Support for Cooperative Key Server

If a GET VPN group has more than one key server, IP-D3P must be enabled on all the key servers. The primary key server sends the GAP payload containing the IP-D3P attributes to the secondary key servers through an announcement message, which notifies all cooperative key servers that IP-D3P is now enforced in the group.

On receiving the GAP payload, cooperative key servers check the IP-D3P attributes against their group configuration. If there is a mismatch, cooperative key servers generate a syslog message, warning the network administrator of a misconfiguration or incorrect configuration, as:

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNING: IP-D3P configuration between Primary KS and Secondary
 KS are mismatched
```

IP-D3P Support for Group Member

Group members receive the IP-D3P parameters present in the rekey messages. Group members process the new GAP payload attributes—D3P-TYPE and D3P-WINDOWSIZE. The window-size, which must be used in IP-D3P for a group member, can be overwritten by using the **client d3p** command in the GDOI group configuration. For example, if a key server configuration is **d3p window msec 1000** and a group member configuration is **client d3p window sec 50**, the group member can enable IP-D3P using the following parameters and overriding the parameters received from thekey server:

```
D3P-TYPE = POSIX-TIME-MSEC
D3P-WINDOWSIZE = 50000
```

Use the **show crypto gdoi gm** command to display the IP-D3P configuration of a group member and the IP-D3P errors, if any, that were encountered.

Note IP-D3P cannot be enabled on Cisco ASR 9000 Series Aggregation Services Routers, which use the parameters sent by a key server. Use the **show crypto gdoi group** command to view the parameters sent by the key server on Cisco ASR 9000 Series Aggregation Services Routers.

Activation Time Delay

GET VPN supports the Activation Time Delay (ATD) feature, in which a key server instructs group members to delay the use of new security associations (SAs) for traffic encryption. A key server includes the ATD value in the Group Associated Policy (GAP) payload when sending unicast rekey messages to group members. The time delay value is not user configurable; it is fixed as 30 seconds before SA expiry. The formula for calculating the ATD value is as follows:

ATD = Max((Max(old-SA-remaining-lifetime_sec, 30sec) – 30sec), 1sec)

Note ATD support is limited to group members that are configured on Cisco ASR 9000 Series Aggregation Services Routers and on non-Cisco devices. Therefore, a key server does not send ATD information to devices other than Cisco ASR 9000 Series Aggregation Services Routers and non-Cisco devices

.

Rekey Acknowledgment

When a key server sends a rekey message to group members for updating the keys and policies of a group, it is useful for a key server to know if all group members have received the rekey message and have successfully processed, installed, and responded to the new keys and policies.

Cisco Unicast Rekey Acknowledgment Message

If a unicast rekey is configured, a key server sends rekey messages, for which group members reciprocate by sending an acknowledgment rekey message.

Note There is no acknowledgment message if multicast rekey is configured.

If a key server sends three consecutive unacknowledged unicast rekeys to a group member, and if the unicast rekeys are unacknowledged by that group member, the group member is removed from the group member database in the key server and no further unicast rekeys are sent to that group member.

GDOI I-D Rekey Acknowledgement Message

The GDOI Interop ACK for Cisco Key Server feature implements the standards for rekey acknowledgment messages between non-Cisco group members and a key server, as defined in the RFC-8263, GROUPKEY-PUSH Acknowledgment message.

The GDOI GROUPKEY-PUSH Acknowledgment message, which is referred to as GDOI I-D Rekey ACK, differs from the Cisco unicast rekey acknowledgment message by defining an interoperable method for a group member to send a rekey acknowledgment to any key server in a group.

GDOI I-D Rekey ACK Support for a Key Server

The **rekey acknowledgement** command enables the key server to request group members to acknowledge rekeys depending on the keywords chosen with the command:

- **cisco**—Accepts Cisco-proprietary rekey ACK (encrypted) message.
- **interoperable**—Requests and accepts rekey ACK (unencrypted) message as per the corresponding Internet Draft.
- **any**—Accepts any supported ACK message based on the group key member version.

After enabling the **rekey acknowledgement** command, the key server sends a new policy attribute, **KEK_ACK_REQUESTED**. The new policy attribute in the key encryption key (KEK) SA payload for registration and rekey.

GDOI I-D Rekey ACK Support for Cooperative Key Server

The **rekey acknowledgement** command must be configured on all the key servers if a GET VPN group has multiple key servers. When a primary key server sends an announcement message to a secondary key server, the primary key server also includes the **KEK SA** payload carrying the **KEK_ACK_REQUESTED** attribute. This notifies all the cooperative key servers to send the **KEK_ACK_REQUESTED** attribute to the group members registered under them.

Upon receiving the **KEK SA** payload with the **KEK_ACK_REQUESTED** attribute, cooperative key servers check their group configuration. If there is a mismatch, cooperative key servers generate a message, warning the network administrator of a misconfiguration or incorrect configuration, as shown here:

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNING: Interoperable Rekey ACK configuration between Primary
 KS and Secondary KS are mismatched
```

Note Rekey acknowledgments are sent only to a primary key server because it is the primary key server that sends rekey messages. A rekey acknowledgment is sent to a cooperative server only when a cooperative key server is promoted as a primary key server, and if the old primary key server did not create a key encryption key (KEK) or traffic encryption key (TEK) policy.

GDOI I-D Rekey Support for Group Member

A group member is said to support the Internet-Draft ACK for Cisco GETVPN Key Server feature if the group member receives the rekey message containing the KEK_ACK_REQUESTED attribute in the KEK SA payload and sends the GDOI I-D Rekey ACK to the key server through an acknowledgment message.

Key Server and Group Member Communication

When a key server sends the KEK_ACK_REQUESTED attribute in the KEK SA payload, a group member must respond to subsequent rekey messages with the GDOI I-D Rekey ACK unless notified otherwise by the corresponding key server. The communication between a key server and group members are as follows:

1. For every GROUPKEY-PUSH message sent by a key server, the group member must respond with the GROUP-PUSH-KEY ACK message.
2. The key server verifies and validates the message for format and payload. If validation fails, the message is dropped.
3. If validation is successful, the key server processes the SEQ and ID payloads to record the latest acknowledged sequence number for the group member associated with the ID. The sequence number must be the same as the last sent sequence number; otherwise, the SEQ and ID payload will not be recorded.

Note In case of a Cisco key server, a group member is removed from the database if a group member does not send an acknowledgment for three consecutive rekey messages. If a group member is configured with the unicast rekey feature and the KEK_ACK_REQUESTED attribute is not sent for a given KEK Security Parameter Index (SPI), the group members must send the Cisco Unicast Rekey ACK message to the key server.

The following table explains the attributes sent in the KEK SA payload along with the values sent for each acknowledgment option configured on a key server:

Table 1: KEK SA Payload for Each Acknowledgment Option

Acknowledgement Option	New Cisco Group Member	Cisco ASR 9000 Group Member	Non-Cisco Group Member
Cisco	No Attribute	No Attribute	No Attribute
Interoperable	K E K _ A C K _ R E Q REKEY_ACK_KEK_SHA256	KEK_ACK_REQ REKEY_ACK_KEK_SHA256	KEK_ACK_REQ REKEY_ACK_KEK_SHA256
Any	No Attribute	KEK_ACK_REQ REKEY_ACK_KEK_SHA256	KEK_ACK_REQ REKEY_ACK_KEK_SHA256

Note When the **no rekey acknowledgement** command is used to set the rekey acknowledgment to the default value ‘Cisco’, the key server does not include the KEK_ACK_REQUESTED attribute in the KEK SA payload.

The following table explains the acknowledgment methodology for each acknowledgment type configured via the keywords in the **rekey acknowledgement** command on a key server:

Table 2: Acknowledgment Methodology

Acknowledgement Option	Key Server Accepts I-D ACK	Key Server Accepts Cisco ACK
Cisco	No (results in error)	Yes
Interoperable	Yes	No (results in error)
Any	Yes	Yes

How to Configure GET VPN Interoperability

Ensuring the Correct GDOI Version on a Key Server

SUMMARY STEPS

1. **enable**
2. **show crypto gkm feature** *feature name*
3. **show crypto gkm feature** *feature-name* | **include no**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

```
Device> enable
```

Step 2 **show crypto gkm feature** *feature name*

Displays the GDOI version running on each key server and group member in the network and information about whether the device supports GET VPN interoperability features, namely, D3P support on GETVPN Key Server and Internet-Draft ACK for Cisco GETVPN Key Server.

Example:

```
Device# show crypto gkm feature ip-d3p
Group Name: GET VPN1
    Key Server ID       Version   Feature Supported
        10.0.8.1         1.0.11         Yes
        10.0.9.1         1.0.10         No
    Group Member ID     Version   Feature Supported
        10.0.3.1         1.0.11         Yes
        10.65.9.2        1.0.10         No
```

Example:

```
Device# show crypto gkm feature gdoi-interop-ack
Group Name: GET VPN2
    Key Server ID       Version   Feature Supported
        10.0.8.1         1.0.11         Yes
        10.0.9.1         1.0.10         No
    Group Member ID     Version   Feature Supported
        10.0.3.1         1.0.11         Yes
        10.65.9.2        1.0.10         No
```

Step 3 **show crypto gkm feature** *feature-name* | **include no**

(Optional) Finds devices that do not support a feature.

Example:

```
Device# show crypto gkm feature gdoi-interop-ack | include no
```

Ensuring the Correct GDOI Version on a Group Member

SUMMARY STEPS

1. **enable**
2. **show crypto gkm feature** *feature name*

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show crypto gkm feature** *feature name*

Displays the GDOI version running on a group member in the network and information about whether the device supports GET VPN interoperability features, namely, D3P support on GETVPN Key Server and Internet-Draft ACK for Cisco GETVPN Key Server.

Example:

```
Device# show crypto gkm feature ip-d3p
       Version    Feature Supported
        1.0.11           Yes
```

Example:

```
Device# show crypto gkm feature gdoi-interop-ack
       Version    Feature Supported
        1.0.10           No
```

Enabling IP-D3P on a Key Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gkm group GETVPN**
4. **server local**
5. **sa d3p window** {**sec** *seconds* | **msec** *milliseconds*}
6. **exit**
7. **show crypto gkm ks replay**

DETAILED STEPS

	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 gkm group GETVPN** **Example:** `Device(config)# crypto gkm group GETVPN`	Configures a group key management (GKM) group and enters GKM group configuration mode.
Step 4	**server local** **Example:** `Device(config-gkm-group)# server local`	Designates the device as a key server and enters GDOI local server configuration mode.
Step 5	**sa d3p window** {**sec** *seconds* | **msec** *milliseconds*} **Example:** `Device(gdoi-local-server)# sa d3p window msec 5000`	Enables IP delivery delay detection protocol (IP-D3P) on all security associations in the group. • **sec** *seconds*—Window size, in seconds. The range is from1 to 100. • **msec** *milliseconds*—Window size, in milliseconds. The range is from 100 to 10000.
Step 6	**exit** **Example:** `Device(gdoi-local-server)# exit`	Exits GDOI local server configuration mode and returns to privileged EXEC mode.
Step 7	**show crypto gkm ks replay** **Example:** `Device# show crypto gkm ks replay`	Displays key server group information for time-based anti-replay.

Example

The following is a sample output from the **show crypto gkm ks replay** command:

```
Device# show crypto gkm ks replay
Anti-replay Information For Group GETVPN:
    IP-D3P: Type = POSIX-TIME-MSEC, Window-size = 5000 msec
```

Enabling IP-D3P on a Group Member

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gkm group GET**
4. **client d3p window** {**sec** *seconds* | **msec** *milliseconds*}
5. **exit**
6. **show crypto gkm gm replay**

DETAILED STEPS

	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 gkm group GET** **Example:** `Device(config)# crypto gkm group GETVPN`	Configures a group key management (GKM) group and enters GKM group configuration mode.
Step 4	**client d3p window** {**sec** *seconds* | **msec** *milliseconds*} **Example:** `Device(config-gkm-group)# client d3p window sec 50`	Enables client-acceptable IP delivery delay detection protocol (IP-D3P). • **sec** *seconds*—Window size, in seconds. The range is from1 to 100. • **msec** *milliseconds*—Window size, in milliseconds. The range is from 100 to 10000.
Step 5	**exit** **Example:** `Device(gdoi-local-server)# exit`	Exits GDOI local server configuration mode and returns to privileged EXEC mode.
Step 6	**show crypto gkm gm replay** **Example:** `Device# show crypto gkm gm replay`	Displays group member information for time-based anti-replay.

Example

The following is a sample output from the **show crypto gkm gm replay** command:

```
Device# show crypto gkm gm replay
Anti-replay Information For Group GET:
   IP-D3P:
     Posix-time-msec           : 502764.17
     Input Packets            : 5        Output Packets           : 5
     Input Error Packets      : 5        Output Error Packets     : 0

IP-D3P Error History (sampled at 10pak/min):
     xx:xx:xx.xxx PST Tue Feb 25 2014: src=5.0.0.2; my_time=502729.95; peer_time=33.46;
win=10
     yy:yy:yy.yyy PST Tue Feb 25 2014: src=5.0.0.2; my_time=502723.95; peer_time=27.45;
win=10
```

Enabling Rekey Acknowledgment

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gkm group GET**
4. **server local**
5. **rekey acknowledgement**{**cisco** | **interoperable** | **any**}
6. **exit**
7. **show crypto gkm ks replay**

DETAILED STEPS

	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 gkm group GET** **Example:** `Device(config)# crypto gkm group GET`	Configures a group key management (GKM) group and enters GKM group configuration mode.
Step 4	**server local** **Example:** `Device(config-gkm-group)# server local`	Designates the device as a key server and enters GDOI local server configuration mode.
Step 5	**rekey acknowledgement**{**cisco** | **interoperable** | **any**} **Example:** `Device(gdoi-local-server)# rekey acknowledgment interoperable`	Enables group members to acknowledge rekeys. • **cisco**—Accepts Cisco Rekey ACK (encrypted) message.

	Command or Action	Purpose
		• **interoperable**—Requests and accepts interoperable rekey ACK (unencrypted) message. • **any**—Accepts a supported ACK message based on group key member version.
Step 6	**exit** **Example:** `Device(gdoi-local-server)# exit`	Exits GDOI local server configuration mode and returns to privileged EXEC mode.
Step 7	**show crypto gkm ks replay** **Example:** `Device# show crypto gkm ks replay`	Displays rekey acknowledgment configuration on the key server.

Example

The following is a sample output from **show** commands displaying the rekey acknowledgment configuration:

```
Device# show crypto gkm

GROUP INFORMATION
    Group Name               : GETVPN (Unicast)
 .
 .
 .
    Group Rekey Lifetime     : 86400 secs
    Group Rekey
        Remaining Lifetime   : 44710 secs
        Time to Rekey        : 44485 secs
        Acknowledgement Cfg  : {Cisco|Interoperable|Any}
 .
 .
 .

Device# show crypto gkm ks

Total group members registered to this box: 0
Key Server Information For Group GETVPN:
    Group Name               : GETVPN
Group Name               : GETVPN (Unicast)
 .
 .
 .
    Group Members            : 0
      GDOI Group Members     : 0
      G-IKEv2 Group Members  : 0
    Rekey Acknowledgement Cfg: {Cisco|Interoperable|Any}
    IPSec SA Direction       : Both
 .
 .
 .
Device# show crypto gkm ks rekey

Group GETVPN (Unicast)
```

```
    Acknowledgement Type In-Use         : {Cisco|Interoperable|Any}
    Number of Rekeys sent               : 20
 .
 .
 .
Device# show crypto gkm ks rekey

Group GETVPN (Multicast)
    Acknowledgement Type In-Use         : None
    Number of Rekeys sent               : 20
 .
 .
 .
Device# show crypto gkm ks policy

Key Server Policy:
For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):
  # of teks : 2  Seq num : 7
  KEK POLICY (transport type : Unicast)
    spi : 0x7D32D2052B87CEFE14060B58B0176129
    management alg     : disabled    encrypt alg       : AES
    crypto iv length   : 16          key size          : 16
    orig life(sec): 86400       remaining life(sec): 44699
    time to rekey (sec): 44474
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : mykeys
    acknowledgement    : {cisco|interoperable|any}

Device# show crypto gkm ks policy

Key Server Policy:
For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):
  # of teks : 2  Seq num : 7
  KEK POLICY (transport type : Multicast)
    spi : 0x7D32D2052B87CEFE14060B58B0176129
    management alg     : disabled    encrypt alg       : AES
    crypto iv length   : 16          key size          : 16
    orig life(sec): 86400       remaining life(sec): 44699
    time to rekey (sec): 44474
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : mykeys
    acknowledgement    : none
```

Configuration Examples for GET VPN Interoperability

Example: Enabling IP-D3P on a Key Server

```
Device> enable
Device# configure terminal
Device(config)# crypto gkm group GETVPN
Device(config-gkm-group)# server local
Device(gdoi-local-server)# sa d3p window msec 5000
Device(gdoi-local-server)# exit
```

Example: Enabling IP-D3P on a Group Member

```
Device> enable
Device# configure terminal
Device(config-gkm-group)# client d3p window sec 50
Device(gdoi-local-server)# exit
```

Example: Enabling Rekey Acknowledgement

```
Device> enable
Device# configure terminal
Device(config)# crypto gkm group GET
Device(config-gkm-group)# server local
Device(gdoi-local-server)# rekey acknowledgment interoperable
Device(gdoi-local-server)# exit
```

Additional References for GET VPN Interoperability

Related Documents

Related Topic	Document Title
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
GET VPN configuration	*Cisco Group Encrypted Transport VPN*
Unicast rekey	"Unicast Rekeying" section in the *GET VPN* module

Standards and RFCs

Standard/RFC	Title
draft-weis-delay-detection-00	*IP Delivery Delay Detection Protocol*
draft-weis-gdoi-rekey-ack-01	*GDOI GROUPKEY-PUSH Acknowledgement Message*
RFC 5374- Section 5.4 - Group Associated Policy	*Multicast Extensions to the Security Architecture for the Internet Protocol*
RFC 6407 - Section 4.2.1 - Activation Time Delay	*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 Interoperability

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 https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 3: Feature Information for GET VPN Interoperability

Feature Name	Releases	Feature Information
D3P support on GETVPN Key Server		The D3P support on GETVPN Key Server feature enables support for IP-D3P on a GET VPN network. The following commands were introduced or modified: **client d3p**, **sa d3p**, **show crypto gkm gm replay**, **show crypto gkm ks replay**.
Internet-Draft ACK for Cisco GETVPN Key Server		The Internet-Draft ACK for Cisco GETVPN Key Server implements the standard for rekey acknowledgment message between non-Cisco group members and key server as defined in the GDOI GROUPKEY-PUSH Acknowledgment Message draft. The following commands were introduced or modified: **rekey acknowledgement**, **show crypto gkm**.
RFC 8263 ID Ack implementation		The Group Domain of Interpretation (GDOI) includes the ability of key server to provide a set of current devices with additional security associations. For example, to rekey expiring security associations. This feature adds the ability of a key server to request that the group devices return an acknowledgement of receipt of its rekey message and specifies the acknowledgement method.