

GETVPN CRL Checking

During the Group Encrypted Transport VPN (GET VPN) process, certificates are received from a certificate authority (CA) and used as a proof of identity. Certificates may be revoked for a number of reasons, such as key compromise or certificate loss. Revoked certificates are placed on a certificate revocation list (CRL) that is published periodically to a repository. This list is stored on the repository for the length of time specified by a configured CRL lifetime, and can be anything from a few hours to several days.

- Information About GETVPN CRL Checking, on page 1
- How to Configure GETVPN CRL Checking, on page 2
- Configuration Examples for GETVPN CRL Checking, on page 7
- Additional References for GETVPN CRL Checking, on page 8
- Feature Information for GETVPN CRL Checking, on page 9

Information About GETVPN CRL Checking

In Internet Key Exchange (IKE), certificates are validated when a session is established between two peers. Current sessions are not affected by certificate revocation. However, new sessions will fail to establish and certificates are not validated again unless group members reregister to the key server (KS).

The GETVPN CRL Checking feature enables public key infrastructure (PKI) to notify Group Domain of Interpretation (GDOI) KSs when a new CRL is available for a configured trustpoint. The KS then creates a new Key Encryption Key (KEK) and sends a reauthentication message to the group member devices, which print a syslog message, delete the current KEKs, and reregister to the KS.

Cooperative Key Server Protocol Integration

Cooperative Key Server Protocol (COOP) is a feature of GET VPN that allows you to configure multiple key servers (KSs) in a VPN network. It is used for KS redundancy.

GETVPN CRL checking integrates with COOP by enabling group member (GM) reauthentication on all KSs. However there is always a possibility that a COOP split may occur, where connectivity is temporarily lost among cooperative KSs.

No COOP Split when Reauthentication is Triggered

If no COOP split occurs the primary GM device deletes the Key Encryption Key (KEK) to secondary KSs and sends a reauthentication message to GMs. The secondary KSs then have the current policies synchronized

with the primary policies before the GMs start to reregister. All GMs reregister and reauthenticate to an available KS and receive the new KEK.

COOP Split when Reauthentication is Triggered

If a COOP split occurs before reauthentication is triggered and there are only two primary KSs, they both send out the reauthentication message. Each primary KS creates a new and different KEK. The GM only understands the first reauthentication message it receives as it deletes all the existing KEKs immediately after receiving the message. The GM then reregisters to an available KS and a CRL check takes place. When reregistering, the GM receives either the KEK of the first primary or the KEK of the second primary, depending on which KS the GM reregistered. The GM then installs that KEK and receives further rekeys only from that primary KS. When the COOP merge occurs, the KSs sync up the policies and send rekeys so that all GMs have the current KEK and traffic encryption keys (TEKs).

Avoiding the Creation of Different KEKs

Reauthentication and CRL checking still occurs if reauthentication is triggered during a COOP split. However, triggering the creation of different KEKs in the KSs is avoided by delaying reauthentication. A primary KS only starts the reauthentication if all COOP KSs are reachable (not split). If one COOP KS is not reachable, the primary KS delays sending the reauthentication message until all COOP KSs are reachable.

How to Configure GETVPN CRL Checking

You need to configure several components prior to enabling the GETVPN CRL Checking feature. These include:

- A defined public key infrastructure (PKI) certificate authority (CA) so that group members and key servers are PKI clients and, therefore must enroll to get certificates.
- Key servers (KSs) configured to have certificate revocation list (CRL) checking enabled in PKI.
- KSs configured to download the CRL when it is available on the CA and on a first-needed basis. This means that the KSs download the CRL following the first group member (GM) registration after the new CRL is available. See the “Configuring Key Servers for GETVPN CRL Checking” section.
- CRL checking disabled on the group member devices for PKI. See the “Disabling CRL Checking on Group Members” section.
- Internet Key Exchange (IKE) authentication set to certificates. See the “Setting IKE Authentication to Certificates” section

Configuring Key Servers for GETVPN CRL Checking

To configure key servers (KSs) to download the certificate revocation list (CRL) when the first group member (GM) registration occurs after a new CRL is available on the certificate authority (CA), perform the following steps:

SUMMARY STEPS

1. **ip domain name** *name*
2. **ip http server**

3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **revocation-check** *method*
6. **exit**
7. **crypto identity** *method*
8. **fqdn** *domain*
9. **fqdn** *domain*
10. **exit**
11. **crypto gdoi group** *group-name*
12. **server local**
13. **authorization identity** *name*
14. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**ip domain name** *name* **Example:** `Device(config)# ip domain name cisco.com`	Defines a default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
Step 2	**ip http server** **Example:** `Device(config)# ip http server`	Enables the HTTP server on an IP or IPv6 system.
Step 3	**crypto pki trustpoint** *name* **Example:** `Device(config)# crypto pki trustpoint mycert`	Defines the trustpoint that your device should use and enters CA trustpoint configuration mode.
Step 4	**enrollment url** *url* **Example:** `Device(config-ca-trustpoint)# enrollment url http://10.1.3.1:80`	Specifies the enrollment URL of the CA.
Step 5	**revocation-check** *method* **Example:** `Device(config-ca-trustpoint)# revocation-check crl`	Ensures certificate checking is performed by a CRL.
Step 6	**exit** **Example:**	Exits CA trustpoint configuration mode and returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-ca-trustpoint)# exit`	
Step 7	**crypto identity** *method* **Example:** `Device(config)# crypto identity abcd`	Configures the identity of the device with a given list of distinguished names (DNs) in the certificate of the device and enters crypto identity configuration mode. **Note** You can set restrictions in the device configuration that prevent peers with specific certificates, especially certificates with particular DNs, from having access to selected encrypted interfaces.
Step 8	**fqdn** *domain* **Example:** `Device(config-crypto-identity)# fqdn ut01-unix5.cisco.com`	Derives the name mangler from the remote identity of the fully qualified domain name (FQDN) for a GM.
Step 9	**fqdn** *domain* **Example:** `Device(config-crypto-identity)# fqdn ut01-unix6.cisco.com`	Derives the name mangler from the remote identity of the FQDN for the next GM.
Step 10	**exit** **Example:** `Device(config-crypto-identity)# exit`	Exits crypto identity configuration mode and returns to global configuration mode.
Step 11	**crypto gdoi group** *group-name* **Example:** `Device(config)# crypto gdoi group gdoi-group1`	Creates a Group Domain of Interpretation (GDOI) group and enters GDOI group configuration mode.
Step 12	**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 13	**authorization identity** *name* **Example:** `Device(config-gdoi-local-server)# authorization identity abcd`	Specifies an authorization identity for a GDOI group based on a distinguished name (DN) or FQDN,
Step 14	**end** **Example:**	Exits GDOI local server configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-gdoi-local-server)# end`	

Disabling CRL Checking on Group Members

To disable certificate revocation list (CRL) checking on group members (GMs) for public key infrastructure (PKI), perform the following steps:

SUMMARY STEPS

1. **ip domain name** *name*
2. **ip http server**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **revocation-check** *method*
6. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**ip domain name** *name* **Example:** `Device(config)# ip domain name cisco.com`	Defines a default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
Step 2	**ip http server** **Example:** `Device(config)# ip http server`	Enables the HTTP server on an IP or IPv6 system.
Step 3	**crypto pki trustpoint** *name* **Example:** `Device(config)# crypto pki trustpoint mycert`	Defines the trustpoint that your device should use and enters CA trustpoint configuration mode.
Step 4	**enrollment url** *url* **Example:** `Device(config-ca-trustpoint)# enrollment url http://10.1.3.1:80`	Specifies the enrollment URL of the certificate authority (CA).
Step 5	**revocation-check** *method* **Example:**	Disables certificate checking on the GMs.

	Command or Action	Purpose
	`Device(config-ca-trustpoint)# revocation-check none`	
Step 6	**exit** **Example:** `Device(config-ca-trustpoint)# exit`	Exits CA trustpoint mode and returns to global configuration mode.

Setting IKE Authentication to Certificates

SUMMARY STEPS

1. **crypto isakmp policy** *priority*
2. **no authentication pre-share**
3. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**crypto isakmp policy** *priority* **Example:** `Router(config)# crypto isakmp policy 1`	Defines an internet key exchange (IKE) policy and enters ISAKMP policy configuration mode.
Step 2	**no authentication pre-share** **Example:** `Router(config-isakmp)# no authentication pre-share`	Resets the authentication method within the IKE policy to the default value.
Step 3	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Enabling GETVPN CRL Checking on Key Servers

To configure public key infrastructure (PKI) to notify the Group Domain of Interpretation (GDOI) key server (KS) when a new certificate revocation list (CRL) is available for the configured trustpoint certificate authority (CA), perform the following steps:

SUMMARY STEPS

1. **crypto gdoi group** *group-name*

2. **server local**
3. **registration periodic crl trustpoint** *trustpoint-name*
4. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**crypto gdoi group** *group-name* **Example:** `Device(config)# crypto gdoi group gdoi_group1`	Creates a GDOI group and enters GDOI group configuration mode.
Step 2	**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 3	**registration periodic crl trustpoint** *trustpoint-name* **Example:** `Device(config-gdoi-local-server)# registration periodic crl trustpoint mycert`	Enables periodic registrations for the GDOI KSs when new CRLs become available for the configured PKI trustpoint certificate authority.
Step 4	**end** **Example:** `Device(config-gdoi-local-server)# end`	Exits GDOI local server mode and returns to privileged EXEC mode.

Configuration Examples for GETVPN CRL Checking

Example: Enabling GETVPN CRL Checking

The following examples show how the GETVPN CRL checking feature is enabled, including all required preconfigurations.

Example: Configuring Key Servers for GETVPN CRL Checking

In the following example, thekey servers (KSs)are configured to download the certificate revocation list (CRL) when the first group member registration occurs after a new CRL is available on the trustpoint certificate authority (CA) named mycert:

```
ip domain name cisco.com
ip http server
crypto pki trustpoint mycert
```

```
 enrollment url http://10.1.3.1:80
 revocation-check crl

crypto identity abcd
 fqdn ut01-unix5.cisco.com
 fqdn ut01-unix6.cisco.com

crypto gdoi group gdoi-group1
 server local
 authorization identity abcd
```

Example: Disabling CRL Checking on Group Members

In the following example, CRL checking on Group Members (GM) for public key infrastructure (PKI) is disabled:

```
ip domain name cisco.com
ip http server
crypto pki trustpoint mycert
 enrollment url http://10.1.3.1:80
 revocation-check none
```

Example: Setting IKE Authentication to Certificates

```
crypto isakmp policy 1
 no authentication pre-share
```

Example: Enabling GETVPN CRL Checking on Key Servers

In the following example, PKI is configured to notify the GDOI KS named group1 when a new CRL is available for the trustpoint CA named mycert:

```
Crypto gdoi group gdoi_group1
 Server local
  registration periodic crl trustpoint mycert
```

Additional References for GETVPN CRL Checking

Related Documents

Related Topic	Document Title
Cisco IOS security commands	*Cisco IOS Security Command References*
Basic deployment guidelines for enabling GET VPN in an enterprise network	*Cisco IOS GETVPN Solution 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 GETVPN CRL Checking

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 GETVPN CRL Checking

Feature Name	Releases	Feature Information
GETVPN CRL Checking		Enables public key infrastructure (PKI) to notify Group Domain of Interpretation (GDOI) key servers (KSs) when a new certificate revocation list (CRL) is available for a configured trustpoint. The following command was introduced: **registration periodic crl trustpoint.**