Deleting Crypto Sessions of Revoked Peer Certificates

The Delete Crypto Sessions of Revoked Peer Certificates on CRL Download feature deletes an active crypto session with a peer if its certificate is found to be revoked when downloading a new CRL.

- Finding Feature Information, on page 1
- Restrictions for Deleting Crypto Sessions of Revoked Peer Certificates, on page 1
- Information About Deleting Crypto Sessions of Revoked Peer Certificates, on page 2
- How to Enable Deletion of Crypto Sessions for Revoked Peer Certificates, on page 2
- Configuration Examples for Deleting Crypto Sessions of Revoked Peer Certificates, on page 4
- Additional References for Deleting Crypto Sessions of Revoked Peers, on page 5
- Feature Information for Deleting Crypto Sessions of Revoked Peer Certificates, on page 6

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

Restrictions for Deleting Crypto Sessions of Revoked Peer Certificates

- If revocation check is turned off and this feature is enabled, the IKE database is not populated with the number of sessions. The show outputs do not display information about the deleted sessions.
- Frequent enabling and disabling of this feature (with active sessions on the device) is not recommended.
- Frequent CRL downloads (in a span of 30 minutes) for the same issuernanme (CA server) is not recommended.
• CRL cache must be enabled. CRL caching cannot be disabled for trustpoint-based prefetch. However, it is possible to disable CRL caching for URL-based prefetch.

• In case of autoenrollment on IKE, the sessions are not deleted until the next IKE rekey, whereas in case of IKEv2, the tunnel must be cleared manually or wait until the certificate expires.

• If IKE has database of “issuer-name” and “SN” populated and receives a notification from PKI about certificate revocation, IKE would act on the PKI notification.

Information About Deleting Crypto Sessions of Revoked Peer Certificates

How a Crypto Session is Deleted

1. When negotiating via certificate authentication, the peer sends the CERT payload to the device, which parses each certificate to store information about serial number and the issuer names. This information forms the list of serial numbers issued by the corresponding CA server and is passed to PKI for revocation check.

2. If the revocation-check crl command is configured for a trustpoint, PKI informs IKE about the revocation check thereby disabling IKE from unnecessarily storing unwanted peer certification information.

3. After a successful CRL download, PKI sends IKE a notification, which contains the “issuer-name.” The CRL signature and content is verified. If there is no change in CRL content, PKI does not notify IKE.

4. If PKI notifies IKE containing the issuer name, IKE prepares a list of serial numbers for an issuer name and passes this list to PKI to verify if the serial numbers in the list are revoked.

5. PKI performs revocation check on the serial number list received from the IKE and checks the list against the downloaded CRL. The revoked serial number list is returned to IKE.

6. On a notification from PKI containing the list of revoked serial numbers, IKE identifies and deletes sessions pertaining to those serial numbers those sessions.

How to Enable Deletion of Crypto Sessions for Revoked Peer Certificates

Enabling Deletion of Crypto Sessions

Perform this task to enable the deletion of crypto sessions for revoked certificates.

SUMMARY STEPS

1. enable
2. clear crypto session
3. configure terminal
4. Do one of the following:
   • crypto isakmp disconnect-revoked-peers
   • crypto ikev2 disconnect-revoked-peers

5. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> clear crypto session</td>
<td>(Optional) Deletes IPsec crypto sessions and IKE and security associations.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# clear crypto session</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> Do one of the following:</td>
<td>Disconnects IKE or IKEv2 crypto sessions with peers having revoked certificates.</td>
</tr>
<tr>
<td>• crypto isakmp disconnect-revoked-peers</td>
<td>For this command to take effect, reconnected the existing sessions.</td>
</tr>
<tr>
<td>• crypto ikev2 disconnect-revoked-peers</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# crypto isakmp disconnect-revoked-peers</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# crypto ikev2 disconnect-revoked-peers</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying the Delete Crypto Session Capability for a Revoked Peer Certificate

Perform this task to verify if the delete crypto session capability is displayed in the show output.

### SUMMARY STEPS

1. enable
2. show crypto isakmp peers
3. show crypto ikev2 session detail

**DETAILED STEPS**

**Step 1**  
**enable**  
**Example:**  
Device> enable  
Enables privileged EXEC mode.  
• Enter your password if prompted.

**Step 2**  
**show crypto isakmp peers**  
**Example:**  
Device# show crypto isakmp peers  
Displays Internet Security Association and Key Management Protocol (ISAKMP) peer descriptions.

**Step 3**  
**show crypto ikev2 session detail**  
**Example:**  
Device# show crypto ikev2 session detail  
Displays the status of active Internet Key Exchange Version 2 (IKEv2) sessions.

---

**Configuration Examples for Deleting Crypto Sessions of Revoked Peer Certificates**

**Example: Enabling Deletion of Crypto Sessions for an IKE Session**

Device> enable  
Device# clear crypto session  
Device# configure terminal  
Device(config)# crypto isakmp disconnect-revoked-peers  
Device# show crypto isakmp peers

Peer: 150.1.1.2 Port: 500 Local: 150.1.1.1  
Phase1 id: 150.1.1.2  
Disconnect Revoked Peer: Enabled

**Example: Enabling Deletion of Crypto Sessions for an IKEv2 Session**

Device> enable  
Device# clear crypto session  
Device# configure terminal  
Device(config)# crypto ikev2 disconnect-revoked-peers  
Device# show crypto ikev2 session detail
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id  Local   Remote  fvr/fvrf   Status
  1   10.0.0.1/500 10.0.0.2/500 (none)/(none) READY
  Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
  Life/Remaining/Active Time: 86400/86157/248 sec
  CE id: 0, Session-id: 1, MIB-id: 1
  Status Description: Negotiation done
  Local spi: 750CBE827434A245 Remote spi: 4353FEDBAEBF24C
  Local id: 10.0.0.1 Remote id: 10.0.0.2
  Local req mess id: 0 Remote req mess id: 0
  Local next mess id: 0 Remote next mess id: 2
  Local req queued: 0 Remote req queued: 0
  Local window: 5 Remote window: 5
  DPD configured for 0 seconds
  NAT-T is not detected
  Disconnect Revoked Peer: Enabled
Child sa: local selector 10.0.0.1/0 - 10.0.0.1/65535
  remote selector 10.0.0.2/0 - 10.0.0.2/65535
  ESP spi in/out: 0x9360A95/0x6C340600
  CPI in/out: 0x9FE5/0xC776
  AH spi in/out: 0x0/0x0
  Encr: AES CBC, keysize: 128, esp_hmac: SHA96
  ah_hmac: Unknown - 0, comp: IPCOMP_LZS, mode tunnel

Additional References for Deleting Crypto Sessions of Revoked Peers

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>
| 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                       |
| Configuring IKE               | Configuring Internet Key Exchange for IPsec VPNs                               |
| Configuring IKEv2             | Configuring Internet Key Exchange Version 2 and FlexVPN Site-to-Site           |
| Recommended cryptographic     | Next Generation Encryption                                                     |
|   algorithms                  |                                                                                |
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for Deleting Crypto Sessions of Revoked Peer Certificates

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete crypto session(s) of revoked peer cert(s) on CRL download</td>
<td>The Delete Crypto Sessions of Revoked Peer Certificates on CRL Download feature deletes an active crypto session with a peer if its certificate is found to be revoked when downloading a new CRL. The following commands were introduced or modified: <code>crypto ikev2 disconnect-revoked-peers</code>, <code>crypto isakmp disconnect-revoked-peers</code>, <code>show crypto isakmp peers</code>, <code>show crypto ikev2 session detail</code>.</td>
<td></td>
</tr>
</tbody>
</table>