Configuring the FlexVPN Server

This module describes FlexVPN server features, IKEv2 commands required to configure the FlexVPN server, remote access clients, and the supported RADIUS attributes.

Security threats, as well as cryptographic technologies to help protect against such threats, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

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 the FlexVPN Server

Dual-Stack Tunnel Interface and VRF-Aware IPsec

When configuring a dual-stack tunnel interface in a VPN routing and forwarding (VRF)-aware IPsec scenario, you cannot use the ip vrf forwarding command to configure an Inside VPN routing and forwarding (IVRF) instance because this is not a valid configuration. Use the vrf forwarding vrf-name command to define the
IVRF of the tunnel interface, where the `vrf-name` argument is defined using the `vrf definition` command with IPv4 and IPv6 address families inside the definition.

**SSO Restrictions**

- The Cisco ASR 1000 Series Routers support stateful IPsec sessions on Embedded Services Processor (ESP) switchover. During ESP switchover, all IPsec sessions will stay up and no user intervention is needed to maintain IPsec sessions.

- For an ESP reload (no standby ESP), the SA sequence number restarts from 0. The peer router drops packets that do not have the expected sequence number. You may need to explicitly reestablish IPsec sessions to work around this issue for systems that have a single ESP after an ESP reload. Traffic disruption might happen over the IPsec sessions in such cases for the duration of the reload.

- The Cisco ASR 1000 Series Router currently does not support Stateful Switchover (SSO) IPsec sessions on Route Processors (RPs). The IPsec sessions will go down on initiation of the switchover, but will come back up when the new RP becomes active. No user intervention is needed. Traffic disruption might happen over the IPsec sessions for the duration of the switchover, until the sessions are back up.

- The Cisco ASR 1000 Series Router does not support stateful ISSU for IPsec sessions. Before performing an ISSU, you must explicitly terminate all existing IPsec sessions or tunnels prior to the operation and reestablish them post ISSU. Specifically, ensure that there are no half-open or half-established IPsec tunnels present before performing ISSU. To do this, we recommend a interface shutdown in the case of interfaces that may initiate a tunnel setup, such as a routing protocol initiating a tunnel setup, or interfaces that have keepalive enabled, or where there is an auto trigger for an IPsec session. Traffic disruption over the IPsec sessions during ISSU is obvious in this case.

**Restrictions for AnyConnect Profile Download**

- The FlexVPN AnyConnect Profile Download feature supports Cisco IOS XE devices as headend and Cisco AnyConnect Secure Mobility client.

- The Cisco AnyConnect profile information can be stored on bootflash only. You cannot load the profile from a remote location, for example, on a TFTP boot server.

- This feature works only with Anyconnect EAP option as a remote authentication method.

**Information About the FlexVPN Server**

**Peer Authentication Using EAP**

The FlexVPN server supports peer authentication using the Extensible Authentication protocol (EAP) and acts as a pass-through authenticator relaying EAP messages between the client and the backend EAP server. The backend EAP server is typically a RADIUS server that supports EAP authentication.

---

**Note**

While a FlexVPN client authenticates the FlexVPN client using EAP, the FlexVPN server must authenticated by using certificates.
The FlexVPN server is configured to authenticate FlexVPN clients that use EAP by configuring the `authentication remote eap` command in IKEv2 profile configuration mode. FlexVPN clients authenticate using EAP by skipping the AUTH payload in the IKE_AUTH request.

If the `query-identity` keyword is configured, the FlexVPN server queries the EAP identity from the client; otherwise, the FlexVPN client’s IKEv2 identity is used as the EAP identity. However, if the `query-identity` keyword is not configured and the FlexVPN client’s IKEv2 identity is an IPv4 or IPv6 address, the session is terminated because IP addresses cannot be used as the EAP identity.

The FlexVPN server starts the EAP authentication by passing the FlexVPN client’s EAP identity to the EAP server; the FlexVPN server then relays EAP messages between the remote access (RA) client and the EAP server until the authentication is complete. If the authentication succeeds, the EAP server is expected to return the authenticated EAP identity to the FlexVPN server in the EAP success message.

After EAP authentication, the EAP identity used for the IKEv2 configuration is obtained from the following sources in the given order:

- The EAP identity provided by the EAP server with the EAP success message.
- The EAP identity queried from the client when the `query-identity` keyword is configured.
- The FlexVPN client IKEv2 identity used as the EAP identity.

The figure below shows IKEv2 exchange for EAP authentication without the `query-identity` keyword.
The figure below shows the IKEv2 exchange for EAP authentication with the `query-identity` keyword.

<table>
<thead>
<tr>
<th>IKEv2 RA client</th>
<th>IKEv2 RA server</th>
<th>RADIUS-EAP server</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDR, SAi1, KEi, Ni</td>
<td>HDR, SAi1, KEi, Nr, [CERTREQ]</td>
<td>HDR, SK {IDr, [CERT], [IDr]} SAI2, TSi, TSr</td>
</tr>
<tr>
<td>HDR, SK {IDi, [CERTREQ], [IDr]} SAI2, TSi, TSr</td>
<td>RADIUS Access-Request/EAP-Message/EAP-Response/EAP-ID(IKEv2-ID)</td>
<td>HDR, SK {IDr, [CERT], AUTH, EAP/EAP-Request/EAP-method})</td>
</tr>
<tr>
<td>HDR, SK {EAP/EAP-Response/EAP-method}</td>
<td>RADIUS Access-Request/EAP-Message/EAP-Response/EAP-method</td>
<td>HDR, SK {EAP (success)}</td>
</tr>
</tbody>
</table>
IKEv2 RA client  | IKEv2 RA server  | RADIUS-EAP server  
---|---|---
HDR, SA11, KEi, N1   |   |   
HDR, SK {IDr,  
[CERTREQ],  
[IDr] SA2, TSI, T Sr}   | HDR, SK {IDr,  
[CERTREQ],  
[IDr] KEr, Nr,  
[CERTREQ]}   |   
HDR, SK {EAP(EAP-  
Response(Identity))}   | RADIUS Access-Request/  
EAP-Message/EAP-  
Response (EAP-ID)   | HDR, SK {EAP(EAP-  
Response (EAP-method))}   
 HDR, SK {EAP(EAP-  
Response (EAP-method))}   | RADIUS Access-Request/  
EAP-Message/EAP-  
Response (EAP-method)   | HDR, SK {EAP (success)}   
HDR, SK {AUTH}   | HDR, SK {AUTH,  
SA2, TSI, T Sr}   

**IKEv2 Configuration Mode**

IKEv2 configuration mode allows IKE peers to exchange configuration information such as IP addresses and routes. The configuration information is obtained from IKEv2 authorization. Both pull and push models are supported. The pull model involves the exchange of configuration requests and replies; the push model involves the exchange of configuration sets and acknowledgements.

The following table describes the conditions when the initiator and the responder send different configuration payload types:
Table 1: Configuration Payload Types

<table>
<thead>
<tr>
<th>Configuration Payload Type</th>
<th>Sent By...</th>
<th>When...</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG_REQUEST</td>
<td>Initiator</td>
<td>The initiator is the FlexVPN client or if the config-exchange request command is enabled in the IKEv2 profile.</td>
</tr>
<tr>
<td>CFG_REPLY</td>
<td>Responder</td>
<td>The responder receives the CFG_REQUEST.</td>
</tr>
</tbody>
</table>
| CFG_SET                   | Initiator and responder | Initiator—The config-exchange set send command is enabled in the IKEv2 profile. 
Respond—The CFG_REQUEST is not received, the configuration data is available, and the config-exchange set send command is enabled in the IKEv2 profile. |
| CFG_ACK                   | Initiator and responder | Initiator—The config-exchange set accept command is enabled in the IKEv2 profile. 
Respond—The config-exchange set accept command is enabled in the IKEv2 profile. |

The commands to send configuration requests and configuration set payloads are enabled by default.

Depending on your release, the IKEv2 initiator can trigger a configuration mode when the initiator is a FlexVPN client, or any static tunnel interface initiating IKEv2 can trigger configuration mode by enabling the config-mode command in the IKEv2 profile.

The IKEv2 FlexVPN server supports the following standard IPv4 configuration attributes:

- INTERNAL_IP4_ADDRESS
- INTERNAL_IP4_NETMASK
- INTERNAL_IP4_DNS
- INTERNAL_IP4_NBNS
- INTERNAL_IP4_SUBNET

The IKEv2 FlexVPN server supports the following standard IPv6 configuration attributes:

- INTERNAL_IP6_ADDRESS
- INTERNAL_IP6_DNS
- INTERNAL_IP6_SUBNET

IPv6 configuration attributes are only supported by the Microsoft Windows IKEv2 client.
The INTERNAL_IP4_SUBNET and INTERNAL_IP6_SUBNET configuration attributes, controlled by the `route set` and `aaa attribute list` commands in the IKEv2 authorization policy, are not supported when you configure a static virtual tunnel interface (SVTI)-to-SVTI tunnel. In such cases, static routing or dynamic routing must be used instead of the IKEv2-based route exchange.

The IKEv2 FlexVPN server supports the following standard common configuration attribute:

- APPLICATION_VERSION

Note: This attribute is only sent for Cisco Anyconnect and FlexVPN clients.

The IKEv2 FlexVPN server supports the following Cisco Unity configuration attributes:

- MODECFG_BANNER
- MODECFG_DEFDOMAIN
- MODECFG_SPLITDNS_NAME
- MODECFG_BACKUPSERVERS
- MODECFG_PFS
- MODECFG_SMARTCARD_REMOVAL_DISCONNECT

Note: The Cisco Unity attributes are sent only for Cisco Anyconnect and FlexVPN clients.

The IKEv2 FlexVPN server supports the following Cisco FlexVPN configuration attributes:

- MODECFG_CONFIG_URL
- MODECFG_CONFIG_VERSION

Note: The Cisco FlexVPN attributes are sent only for Cisco FlexVPN clients.

The INTERNAL_IP4_ADDRESS attribute value is derived from the following sources in the given order:

- The Framed-IP-Address attribute received in AAA user authorization.
- The local IP address pool.
- The DHCP server.

The DHCP server, if configured, allocates addresses only if the local IP address pool is not configured. However, if an error occurs when allocating IP addresses from the local pool, the next address source DHCP server is not used for allocating the addresses.

The value for INTERNAL_IP4_NETMASK attribute is derived as follows:

- If the IP address is obtained from the DHCP server, the netmask is also obtained from the DHCP server.
• If the IP address is obtained from either the Framed-IP-Address attribute in AAA user authorization or the local IP address pool, the netmask is derived from the IPv4 netmask attribute received in the user or group authorization. If the netmask is not available, the INTERNAL_IP4_NETMASK attribute is not included in the configuration reply. If the netmask is available, the INTERNAL_IP4_NETMASK attribute is included only if the INTERNAL_IP4_ADDRESS attribute is included in the configuration reply.

An IPv4 address is allocated and included in the reply only if the client requests an address. If the client requests multiple IPv4 addresses, only one IPv4 address is sent in the reply. If available, the remaining attributes are included in the reply even though the client does not request them. If the client requests an IPv4 address and the FlexVPN server is unable to assign an address, an INTERNAL_ADDRESS_FAILURE message is returned to the client.

It is always recommended that the prefix length should be used as 128 on ipv6 local pool configuration.

For example, if clients are 4, `ipv6 local pool pool1 afe0::/126 128` needed to be configured for the prefix length. If clients are 16, `ipv6 local pool pool1 afe0::/124 128` needed to be configured for the prefix length.

**IKEv2 Authorization**

IKEv2 authorization provides a policy for an authenticated session by using the AAA. The policy can be defined locally or on the RADIUS server, and contains local and/or remote attributes. The username for authorization can either be derived from the peer identity using the `name-mangler` keyword or be directly specified in the command. IKEv2 authorization is mandatory only if the peer requests an IP address via configuration mode.

IKEv2 authorization types are as follows:

• User authorization—Use the `aaa authorization user` command in the IKEv2 profile to enable user authorization. User authorization is based on the user-specific portion of the peer IKE identity such as fqdn-hostname. The attributes from user authorization are called user attributes.

• Group authorization—Use the `aaa authorization group` command in the IKEv2 profile to enable group authorization. Group authorization is based on the generic portion of the peer IKE identity such as fqdn-domain. The attributes from group authorization are called group attributes.

• Implicit user authorization—Use the `aaa authorization user cached` command in the IKEv2 profile to enable implicit user authorization. Implicit authorization is performed as part of EAP authentication or when obtaining the AAA preshared key. The attributes from implicit user authorization are called cached attributes.

**Note**

Depending on your release, the `aaa authorization user cached` command may or may not be available. Explicit user authorization is performed only when implicit user authorization does not return any attributes or does not have the Framed-IP-Address attribute.

**Merging and Overriding Attributes**

Attributes from different sources are merged before they are used. The precedence of merging attributes is as follows:

• When merging duplicate attributes, the source of the attribute has a higher precedence.

• When merging user and cached attributes, user attributes have higher precedence.
• When merging merged-user-attributes and group attributes, merged-user attributes have a higher precedence, by default. However, this precedence can be reversed using the **aaa author group override** command.

### IKEv2 Authorization Policy

An IKEv2 authorization policy defines the local authorization policy and contains local and/or remote attributes. Local attributes, such as VPN routing and forwarding (VRF) and the QoS policy, are applied locally. Remote attributes, such as routes, are pushed to the peer via the configuration mode. Use the **crypto ikev2 authorization policy** command to define the local policy. The IKEv2 authorization policy is referred from the IKEv2 profile via the **aaa authorization** command.

### IKEv2 Name Mangler

The IKEv2 name mangler is used to derive the username for IKEv2 authorization and obtain the AAA preshared key from the peer IKE identity.

### IKEv2 Multi-SA

The IKEv2 Multi-SA feature allows an IKEv2 Dynamic Virtual Tunnel Interface (DVTI) session on the IKEv2 responder to support multiple IPsec Security Associations (SA). The maximum number of IPsec SAs per DVTI session is either obtained from AAA authorization or configured on the IPsec profile. The value from AAA has a higher priority. Any change to the `max-flow-limit` argument in the IPsec profile is not applied to the current session but is applied to subsequent sessions. The IKEv2 Multi-SA feature makes the configuration of the IKEv2 profile in the IPsec profile optional. This optional configuration allows IPsec DVTI sessions using the same virtual template to have different IKEv2 profiles, thus saving the number of virtual template configurations.

**Note**
The IKEv2 Multi-SA feature allows multiple IPsec SAs that have non-any-any proxies. However, when the IPsec SA proxies are any-any, a single IPsec SA is allowed.

For more information, see the “Multi-SA Support for Dynamic Virtual Tunnel Interfaces for IKEv2” module in the Security for VPNs with IPsec Configuration Guide.

### IKEv2 Dynamic Routing

With IKEv2 static routing, route information is exchanged during initial session bring up. The IKEv2 Dynamic Routing Support feature enables exchange of route information even after a session is established. Changes in routing information such as new routes, addition or deletion of routes can be propagated from FlexVPN client to FlexVPN server. The route information is included in the IKEv2 information exchange messages.

The IKEv2 Dynamic Routing Support feature is supported with SVTI, FlexVPN Client and FlexVPN Spoke. For more information, refer to the “IKEv2 Dynamic Routing” section in the Configuring the FlexVPN Client module of FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T. The software release on FlexVPN server must be Cisco IOS XE Everest 16.5.1 and later for this feature to work with FlexVPN client.
Only redistribution of connected routes from FlexVPN client is supported.

AnyConnect Profile Download

The FlexVPN AnyConnect Profile Download feature enables a device running Cisco IOS XE software to connect and push the profile information in IKEv2 protocol to Cisco AnyConnect Secure Mobility client. Cisco AnyConnect Secure Mobility client contains profiles used for configuring the settings for VPN. These profiles can be manually configured or can be downloaded from a headend. The headend can be configured to deploy profiles globally for all Cisco AnyConnect Secure Mobility client users.

Use the `anyconnect profile` command to match a VPN profile against an IKEv2 profile.

Note: Crypto SSL profile is not mandatory to configure AnyConnect Profile Download feature.

Supported RADIUS Attributes

The following tables list the RADIUS attributes supported by the IKEv2 FlexVPN server:

- The Scope field defines the direction of the attribute and the usage on the FlexVPN server or client.
  - Inbound—FlexVPN server to RADIUS
  - Outbound—RADIUStotheFlexVPN server
  - Local—Used locally by the FlexVPN server
  - Remote—Pushed to the client by the FlexVPN server

- The “Local configuration” field specifies the IKEv2 authorization policy command that is used to configure the attribute locally on the FlexVPN server.

- Cisco AV Pair is a Cisco Vendor Specific Attribute (VSA) with vendor-id 9 and vendor-type 1. The VSAs are encapsulated in the Radius IETF attribute 26 Vendor-Specific. The Cisco AV pair is specified as a string of format “protocol:attribute=value”.

Example:

```
cisco-avpair = “ipsec:ipv6-addr-pool=v6-pool”
```

The following example shows the Cisco AV pair for a standard access-list.

```
cisco-avpair = “ipsec:route-set-access-list 99”
```

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name</td>
<td>Inbound and outbound (bidirectional)</td>
</tr>
<tr>
<td>User-Password</td>
<td>Inbound</td>
</tr>
<tr>
<td>Attribute</td>
<td>Scope</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Calling-Station-Id</td>
<td>Inbound</td>
</tr>
<tr>
<td>Service-Type</td>
<td>Inbound</td>
</tr>
<tr>
<td>EAP-Message</td>
<td>Bidirectional</td>
</tr>
<tr>
<td>Message-Authenticator</td>
<td>Bidirectional</td>
</tr>
</tbody>
</table>

Table 3: Outbound IETF and Cisco AV Pair RADIUS Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Scope</th>
<th>Local configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel-Type</td>
<td>IETF</td>
<td>Local</td>
<td>N/A</td>
</tr>
<tr>
<td>Tunnel-Medium-Type</td>
<td>IETF</td>
<td>Local</td>
<td>N/A</td>
</tr>
<tr>
<td>Tunnel-Password</td>
<td>IETF</td>
<td>Local</td>
<td>N/A</td>
</tr>
<tr>
<td>ipsec:ikev2-password-local</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>N/A</td>
</tr>
<tr>
<td>ipsec:ikev2-password-remote</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>N/A</td>
</tr>
<tr>
<td>ipsec:addr-pool</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>pool</td>
</tr>
<tr>
<td>ipsec:group-dhcp-server</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>dhcp server</td>
</tr>
<tr>
<td>ipsec:dhcp-giaddr</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>dhcp giaddr</td>
</tr>
<tr>
<td>ipsec:dhcp-timeout</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>dhcp timeout</td>
</tr>
<tr>
<td>ipsec:ipv6-addr-pool</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>ipv6 pool</td>
</tr>
<tr>
<td>ipsec:route-set=interface</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>route set interface</td>
</tr>
<tr>
<td>ipsec:route-set=prefix</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>N/A</td>
</tr>
<tr>
<td>ipsec:route-accept</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>route accept any</td>
</tr>
<tr>
<td>ip:interface-config</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>aaa attribute list</td>
</tr>
<tr>
<td>ipsec:ipsec-flow-limit</td>
<td>Cisco AV Pair</td>
<td>Local</td>
<td>ipsec flow-limit</td>
</tr>
<tr>
<td>Framed-IP-Address</td>
<td>IETF</td>
<td>Remote</td>
<td>N/A</td>
</tr>
<tr>
<td>Framed-IP-Netmask</td>
<td>IETF</td>
<td>Remote</td>
<td>netmask</td>
</tr>
<tr>
<td>ipsec:dns-servers</td>
<td>Cisco AV Pair</td>
<td>Remote</td>
<td>DNS</td>
</tr>
<tr>
<td>ipsec:wins-servers</td>
<td>Cisco AV Pair</td>
<td>Remote</td>
<td>wins</td>
</tr>
<tr>
<td>ipsec:route-set=access-list</td>
<td>Cisco AV Pair</td>
<td>Remote</td>
<td>route set access-list</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(See Note 1.)</td>
</tr>
</tbody>
</table>
### Supported Remote Access Clients

The FlexVPN server interoperates with the Microsoft Windows 7 IKEv2 client, Cisco IKEv2 AnyConnect client, and Cisco FlexVPN client.

#### Microsoft Windows 7 IKEv2 Client

The Microsoft Windows 7 IKEv2 client sends an IP address as the Internet Key Exchange (IKE) identity that prevents the Cisco IKEv2 FlexVPN server from segregating remote users based on the IKE identity. To allow the Windows 7 IKEv2 client to send the email address (user@domain) as the IKE identity, apply the hotfix documented in KB975488 ([http://support.microsoft.com/kb/975488](http://support.microsoft.com/kb/975488)) on Microsoft Windows 7 and specify the email address string in either the Username field when prompted or the CommonName field in the certificate depending on the authentication method.

For certificate-based authentication, the FlexVPN server and Microsoft Windows 7 client certificates must have an Extended Key Usage (EKU) field as follows:

- For the client certificate, EKU field = client authentication certificate.
- For the server certificate, EKU field = server authentication certificate
The certificates can be obtained from the Microsoft Certificate Server or the IOS CA server.

For EAP authentication, the Microsoft Windows 7 IKEv2 client expects an EAP identity request before any other EAP requests. Ensure that you configure the `query-identity` keyword in the IKEv2 profile on the IKEv2 FlexVPN server to send an EAP identity request to the client.

**Cisco IKEv2 AnyConnect Client**

For certificate-based authentication, the FlexVPN server and the AnyConnect client certificates must have an Extended Key Usage (EKU) field as follows:

- For the client certificate, EKU field = client authentication certificate
- For the server certificate, EKU field = server authentication certificate

If the FlexVPN server authenticates to AnyConnect client using certificates, a SubjectAltName extension is required in the FlexVPN server certificate that contains the server’s IP address or fully qualified domain name (FQDN). Additionally, HTTP certified URLs must be disabled on the FlexVPN server using the `no crypto ikev2 http-url cert` command.

The following example displays the XML tags specific to EAP-MD5 authentication of IKEv2 sessions in the AnyConnect client profile:

```xml
<PrimaryProtocol>IPsec
    <StandardAuthenticationOnly>true
        <AuthMethodDuringIKENegotiation>
            EAP-MD5
        </AuthMethodDuringIKENegotiation>
    </StandardAuthenticationOnly>
</PrimaryProtocol>
```


**How to Configure the FlexVPN Server**

**Configuring the IKEv2 Profile for the FlexVPN Server**

This task describes the IKEv2 profile commands required for configuring the FlexVPN server in addition to the basic IKEv2 profile commands. Refer to the “Configuring IKEv2 Profile (Basic)” task in the *Configuring Internet Key Exchange Version 2 (IKEv2)* feature module for information about configuring the basic IKEv2 profile.

Perform this task to configure the IKEv2 profile for the FlexVPN Server:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `crypto ikev2 profile profile-name`
4. `aaa authentication eap list-name`
5. **authentication** {local {rsa-sig | pre-share [key {0 | 6} password] | ecdsa-sig | eap [gtc | md5 | ms-chapv2] [username username] [password {0 | 6} password]} | remote {eap [query-identity | timeout seconds] | rsa-sig | pre-share [key {0 | 6} password] | ecdsa-sig}}

6. Execute both or one of the following:
   - **aaa authorization user** {eap | psk} {cached | list aaa-listname [aaa-username | name-mangler mangler-name]}
   - **aaa authorization user cert list** aaa-listname {aaa-username | name-mangler mangler-name}

7. Execute both or one of the following:
   - **aaa authorization group** [override] {eap | psk} list aaa-listname [aaa-username | name-mangler mangler-name]
   - **aaa authorization group** [override] cert list aaa-listname {aaa-username | name-mangler mangler-name}

8. **crypto vpn anyconnect profile** profile-name flash:file-name
9. anyconnect profile profile-name
10. **config-exchange** {request | set {accept | send}}
11. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>crypto ikev2 profile profile-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# crypto ikev2 profile profile1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>aaa authentication eap list-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ikev2-profile)# aaa authentication eap list1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>authentication {local {rsa-sig</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Device(config-ikev2-profile)# authentication local ecdsa-sig

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ecdsa-sig — Specifies ECDSA-sig as the authentication method.</td>
<td></td>
</tr>
<tr>
<td>• eap — Specifies EAP as the remote authentication method.</td>
<td></td>
</tr>
<tr>
<td>• query-identity — Queries the EAP identity from the peer.</td>
<td></td>
</tr>
<tr>
<td>• timeout seconds — Specifies the duration, in seconds, to wait for the next IKE_AUTH request after sending the first IKE_AUTH response.</td>
<td></td>
</tr>
</tbody>
</table>

Note: You can specify only one local authentication method but multiple remote authentication methods.

Step 6

Execute both or one of the following:

- **aaa authorization user {eap | psk} {cached | list aaa-listname [aaa-username | name-mangler mangler-name]}**
- **aaa authorization user cert list aaa-listname {aaa-username | name-mangler mangler-name}**

Example:

Device(config-ikev2-profile)# aaa authorization user eap cached

Example:

Device(config-ikev2-profile)# aaa authorization user cert list list1 name-mangler mangler1

Specifies the AAA method list and username for user authorization.

- **user** — Specifies user authorization.
- **cert** — Specifies that the peers must be authenticated using certificates.
- **eap** — Specifies that the peers must be authenticated using EAP.
- **psk** — Specifies that the peers must be authenticated using preshared keys.
- **cached** — Specifies that the attributes received during EAP authentication or obtained from the AAA preshared key must be cached.
- **aaa-listname** — AAA method list name.
- **aaa-username** — Specifies the username that must be used in the AAA authorization request.
- **name-mangler** — Specifies the name mangler that derives the AAA authorization username from the peer identity.
- **mangler-name** — Name mangler to be used.
For psk and eap authentication methods, specifying the aaa-username argument or the name-mangler keyword is optional and if not specified, the peer identity is used as the username.

For psk and eap authentication methods, you can simultaneously configure two variants for user authorization with the cached and list keyword respectively.

Specifying the aaa-username argument or the name-mangler keyword is mandatory for cert authentication, as the peer identity of type distinguished name (DN) cannot be used.

### Step 7

Execute both or one of the following:

- **aaa authorization group** [override] {eap | psk} list
  
  aaa-listname [aaa-username | name-mangler
  
  mangler-name]

- **aaa authorization group** [override] cert list
  
  aaa-listname {aaa-username | name-mangler
  
  mangler-name}

**Example:**

Device(config-ikev2-profile)# aaa authorization

  group override psk list list1

**Example:**

Device(config-ikev2-profile)# aaa authorization

  group cert list list1 name-mangler mangler1

### Purpose

- Specifies the AAA method list and username for group authorization.
  
  - **group**—Specifies group authorization.
  
  - **override**—(Optional) Specifies that attributes from group authorization should take precedence while merging attributes. By default, user attributes take precedence.
  
  - **cert**— Specifies that peers must be authenticated using certificates.
  
  - **eap**— Specifies that peers must be authenticated using EAP.
  
  - **psk**— Specifies that peers must be authenticated using preshared keys.
  
  - **aaa-listname**—AAA method list name.
  
  - **aaa-username**—Username that must be used in the AAA authorization request.
  
  - **name-mangler**— Specifies the name mangler that derives the AAA authorization username from the peer identity.
  
  - **mangler-name**—Name mangler to be used.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Note** | - For **psk** and **eap** authentication methods, specifying the **aaa-username** argument or the **name-mangler** keyword is optional and if not specified, the peer identity is used as the username.  
- For **psk** and **eap** authentication methods, you can simultaneously configure two variants for user authorization with the **cached** and **list** keyword respectively.  
- Specifying the **aaa-username** argument or the **name-mangler** keyword is mandatory for **cert** authentication, as the peer identity of type distinguished name (DN) cannot be used. |

**Step 8**  
*crypto vpn anyconnect profile* *profile-name*  
*flash:file-name*  
**Example:**  
Device(config-ikev2-profile)# crypto vpn anyconnect profile vpn-profile flash:test1.xml  
**Note**  
Defines an AnyConnect profile.

**Step 9**  
*anyconnect profile* *profile-name*  
**Example:**  
Device(config-ikev2-profile)# anyconnect profile vpn-profile  
**Note**  
The profile name mentioned in this step must reference to Cisco AnyConnect profile in the *crypto vpn anyconnect profile* *profile-name*  
*flash:file-name* command.

**Step 10**  
*config-exchange* *{request | set} {accept | send}*  
**Example:**  
Device(config-ikev2-profile)# config-exchange set accept  
**(Optional)** Enables configuration exchange options.  
- **request**—Enables the configuration exchange request.  
- **set**—Enables the configuration exchange request set options.  
- **accept**—Accepts the configuration exchange request set.  
- **send**—Enables sending of the configuration exchange set.  
**Note**  
The request and set options are enabled by default.

**Step 11**  
*end*  
**Example:**  
Device(config-ikev2-profile)# end  
**Note**  
Exits IKEv2 profile configuration mode and returns to privileged EXEC mode.
Configuring the IKEv2 Name Mangler

Perform this task to specify the IKEv2 name mangler, which is used to derive a name for authorization requests and obtain AAA preshared keys. The name is derived from specified portions of different forms of remote IKE identities or the EAP identity. The name mangler specified here is referred to in the IKEv2 profile.

SUMMARY STEPS

1. enable
2. configure terminal
3. crypto ikev2 name-mangler mangler-name
4. dn {common-name | country | domain | locality | organization | organization-unit | state}
5. eap {all | dn {common-name | country | domain | locality | organization | organization-unit | state} | prefix | suffix {delimiter {. | @ | \}}}
6. email {all | domain | username}
7. fqdn {all | domain | hostname}
8. 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>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</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 3</strong> crypto ikev2 name-mangler mangler-name</td>
<td>Defines a name mangler and enters IKEv2 name mangler configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# crypto ikev2 name-mangler mangler1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> dn {common-name</td>
<td>country</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ikev2-name-mangler)# dn state</td>
<td>• common-name</td>
</tr>
<tr>
<td></td>
<td>• country</td>
</tr>
<tr>
<td></td>
<td>• domain</td>
</tr>
<tr>
<td></td>
<td>• locality</td>
</tr>
<tr>
<td></td>
<td>• organization</td>
</tr>
<tr>
<td></td>
<td>• organization-unit</td>
</tr>
<tr>
<td></td>
<td>• state</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Derives the name from the remote identity of type EAP (Extensible Authentication Protocol).</td>
</tr>
<tr>
<td>eap {all</td>
<td>dn {common-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-ikev2-name-mangler)# eap prefix delimiter @</td>
<td>• all—Derives the name from the entire EAP identity.</td>
</tr>
<tr>
<td></td>
<td>• dn—Derives the name from any of the following fields in the remote EAP identity of type DN:</td>
</tr>
<tr>
<td></td>
<td>• common-name</td>
</tr>
<tr>
<td></td>
<td>• country</td>
</tr>
<tr>
<td></td>
<td>• domain</td>
</tr>
<tr>
<td></td>
<td>• locality</td>
</tr>
<tr>
<td></td>
<td>• organization</td>
</tr>
<tr>
<td></td>
<td>• organization-unit</td>
</tr>
<tr>
<td></td>
<td>• state</td>
</tr>
<tr>
<td></td>
<td>• prefix—Derives the name from the prefix in the EAP identity.</td>
</tr>
<tr>
<td></td>
<td>• suffix—Derives the name from the suffix in the EAP identity.</td>
</tr>
<tr>
<td></td>
<td>• delimiter {</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Derives the name from the remote identity of type e-mail.</th>
</tr>
</thead>
<tbody>
<tr>
<td>email {all</td>
<td>domain</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-ikev2-name-mangler)# email username</td>
<td>• all—Derives the name from the entire remote IKE identity of type e-mail.</td>
</tr>
<tr>
<td></td>
<td>• domain—Derives the name from the domain part of the remote IKE identity.</td>
</tr>
<tr>
<td></td>
<td>• username—Derives the name from the username part of the remote IKE identity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Derives the name from the remote identity of type FQDN (Fully Qualified Domain Name).</th>
</tr>
</thead>
<tbody>
<tr>
<td>fqdn {all</td>
<td>domain</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-ikev2-name-mangler)# fqdn domain</td>
<td>• all—Derives the name from the entire remote IKE identity of type FQDN.</td>
</tr>
<tr>
<td></td>
<td>• domain—Derives the name from the domain part of the remote IKE identity.</td>
</tr>
<tr>
<td></td>
<td>• hostname—Derives the name from the hostname part of the remote IKE identity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Exits IKEv2 name mangler configuration mode and returns to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-ikev2-name-mangler)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring the IKEv2 Authorization Policy

Perform this task to configure the IKEv2 authorization policy.

SUMMARY STEPS

1. enable
2. configure terminal
3. crypto ikev2 authorization policy policy-name
4. aaa attribute list list-name
5. backup-gateway string
6. banner banner-text
7. configuration url url
8. configuration version version
9. def-domain domain-name
10. dhcp {giaddr ip-address | server {ip-address | hostname} | timeout seconds}
11. [ipv6] dns primary-server [secondary-server]
12. include-local-lan
13. ipsec flow-limit number
14. netmask mask
15. pfs
16. [ipv6] pool name
17. route set {interface interface | access-list {access-list-name | access-list-number | ipv6 access-list-name}}
18. route accept any [tag value] [distance value]
19. route redistribute protocol [route-map map-name]
20. route set remote {ipv4 ip-address mask | ipv6 ip-address/mask}
21. smartcard-removal-disconnect
22. split-dns string
23. session-lifetime seconds
24. route set access-list {acl-number | [ipv6] acl-name}
25. wins primary-server [secondary-server]
26. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>3</td>
<td>crypto ikev2 authorization policy <em>policy-name</em></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config)# crypto ikev2 authorization policy policy1</td>
</tr>
<tr>
<td>4</td>
<td>aaa attribute list <em>list-name</em></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-ikev2-author-policy)# aaa attribute list list1</td>
</tr>
<tr>
<td>5</td>
<td>backup-gateway <em>string</em></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-ikev2-author-policy)# backup-gateway gateway1</td>
</tr>
<tr>
<td>6</td>
<td>banner <em>banner-text</em></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-ikev2-author-policy)# banner This is IKEv2</td>
</tr>
<tr>
<td>7</td>
<td>configuration url <em>url</em></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-ikev2-author-policy)# configuration url <a href="http://www.cisco.com">http://www.cisco.com</a></td>
</tr>
<tr>
<td>8</td>
<td>configuration version <em>version</em></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-ikev2-author-policy)# configuration version 2.4</td>
</tr>
<tr>
<td>9</td>
<td>def-domain <em>domain-name</em></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-ikev2-author-policy)# def-domain cisco</td>
</tr>
<tr>
<td>10</td>
<td>dhcp {giaddr <em>ip-address</em></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>server <em>ip-address</em></td>
</tr>
<tr>
<td></td>
<td>hostname}</td>
</tr>
<tr>
<td></td>
<td><strong>timeout seconds</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Device(config-ikev2-author-policy)# dhcp giaddr 192.0.2.1</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>• giaddr <em>ip-address</em>—Specifies the gateway IP address (giaddr).</td>
</tr>
<tr>
<td></td>
<td>• server <em>ip-address</em></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>hostname}—Specifies the IP address or hostname of the DHCP server. The hostname is resolved during configuration.</td>
</tr>
<tr>
<td></td>
<td>• timeout seconds—Specifies the wait time in seconds for the response from the DHCP server.</td>
</tr>
</tbody>
</table>
### Configuring the IKEv2 Authorization Policy

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>Note</strong> You can specify only one DHCP server. It is assumed that the DHCP server can be reached via the global routing table, and therefore, the DHCP packets are forwarded to the global routing table.</td>
</tr>
<tr>
<td><strong>[ipv6] dns primary-server [secondary-server]</strong></td>
<td>Specifies the IP addresses of primary and secondary Domain Name Service (DNS) servers that are sent to the client in the configuration reply.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>ipv6</strong> — (Optional) Specifies an IPv6 address for the DNS server. To specify an IPv4 address, execute the command without this keyword.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>primary-server</strong> — IP address of the primary DNS server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>secondary-server</strong> — (Optional) IP address of the secondary DNS server.</td>
</tr>
<tr>
<td><strong>include-local-lan</strong></td>
<td>Includes local LAN. This parameter is sent to the client via the nonstandard Cisco Unity configuration attribute.</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>ipsec flow-limit number</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Specifies the maximum number of IPsec SAs that an IKEv2 dVTI session on the IKEv2 responder can have. The range is from 0 to 50000.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>By default, the command is disabled, and there is no limit on the number of IPsec flows per dVTI session. A value of 0 will not allow any IPsec SAs.</td>
</tr>
<tr>
<td><strong>netmask mask</strong></td>
<td>Specifies the netmask of the subnet from which the IP address is assigned to the client.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>mask</strong> — Subnet mask address.</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td><strong>pfs</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enables Password Forward Secrecy (PFS). This parameter is sent to the client via the nonstandard Cisco Unity configuration attribute. This parameter specifies whether the client should use PFS.</td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td><strong>[ipv6] pool name</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Defines a local IP address pool for assigning IP addresses to the remote access client.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>ipv6</strong> — (Optional) Specifies an IPv6 address pool. To specify an IPv4 address, execute the command without this keyword.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>name</strong> — Name of the local IP address pool.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 17</strong> route set {interface interface</td>
<td>access-list {access-list-name</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Specifies the route set parameters to the peer via configuration mode and allows running routing protocols such as Border Gateway Protocol (BGP) over VPN.</td>
</tr>
<tr>
<td></td>
<td>• <code>interface</code>—Specifies the route interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>access-list</code>—Specifies the route access list.</td>
</tr>
<tr>
<td></td>
<td>• <code>access-list-name</code>—Access list name.</td>
</tr>
<tr>
<td></td>
<td>• <code>access-list-number</code>—Standard access list number.</td>
</tr>
<tr>
<td></td>
<td>• <code>ipv6</code>—Specifies an IPv6 access list.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ikev2-author-policy)# route set interface</td>
<td></td>
</tr>
<tr>
<td><strong>Step 18</strong> route accept any [tag value] [distance value]</td>
<td>Filters the routes received from the peer and specify the tag and metric values to install these routes.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ikev2-author-policy)# route accept any tag 10</td>
<td>• <code>any</code>—Accepts all routes received from the peer.</td>
</tr>
<tr>
<td></td>
<td>• <code>tag value</code>—(Optional) Specifies the tag ID for the static routes added by IKEv2. The range is from 1 to 497777.</td>
</tr>
<tr>
<td></td>
<td>• <code>distance value</code>—(Optional) Specifies the distance for the static routes added by IKEv2. The range is from 1 to 255.</td>
</tr>
<tr>
<td><strong>Step 19</strong> route redistribute protocol [route-map map-name]</td>
<td>Filters the routes received from the peer and specify the tag and metric values to install these routes.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ikev2-author-policy)# route redistribute connected</td>
<td>• <code>protocol</code>—Source protocol from which routes are redistributed. It can be one of the following keywords: connected or static.</td>
</tr>
<tr>
<td></td>
<td>• <code>route-map map-name</code>—(Optional) Route map that should be filtered to import routes from one source routing protocol to another routing protocol. If a map name is not specified, all routes are redistributed.</td>
</tr>
<tr>
<td><strong>Step 20</strong> route set remote {ipv4 ip-address mask</td>
<td>ipv6 ip-address</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ikev2-author-policy)# route set remote ipv6 2001:DB8::1/32</td>
<td></td>
</tr>
<tr>
<td><strong>Step 21</strong> smartcard-removal-disconnect</td>
<td>Enables smartcard removal disconnect. This parameter is sent to the client via the nonstandard Cisco Unity configuration attribute. This parameter specifies that the client should terminate the session when the smart card is removed.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ikev2-author-policy)# smartcard-removal-disconnect</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 22 | `split-dns string` | Allows you to specify up to ten split domain names. This parameter is sent to the client via the nonstandard Cisco Unity configuration attribute. This parameter specifies the domain names that the client should use for private networks. **Example:**
```
Device(config-ikev2-author-policy)# split-dns abc1
```
| Step 23 | `session-lifetime seconds` | Specifies the IKEv2 session lifetime. **Example:**
```
Device(config-ikev2-author-policy)# session-lifetime 1000
```
  - `seconds seconds` — The range is from 120 to 25920000, which converts to two minutes to 300 days.
| Step 24 | `route set access-list {acl-number | [ipv6] acl-name}` | Specifies the subnets that are pushed to the remote peer via configuration mode. **Example:**
```
Device(config-ikev2-client-config-group)# route set access-list 110
```
  - `acl-number` — Access list number (ACL). The ACL number can only be specified for an IPv4 ACL.
  - `ipv6` — (Optional) Specifies an IPv6 access control list (ACL). To specify an IPv4 attribute, execute the command without this keyword.
  - `acl-name` — Access list name.
| Step 25 | `wins primary-server [secondary-server]` | Specifies the internal Windows Internet Naming Service (WINS) server addresses that are sent to the client in the configuration reply. **Example:**
```
Device(config-ikev2-author-policy)# wins 203.0.113.1 203.0.113.115
```
  - `primary-server` — IP address of the primary WINS server.
  - `secondary-server` — (Optional) IP address of the secondary WINS server.
| Step 26 | `end` | Exits IKEv2 authorization policy configuration mode and returns to privileged EXEC mode. **Example:**
```
Device(config-ikev2-author-policy)# end
```

## Configuration Examples for the FlexVPN Server

### Example: Configuring the FlexVPN Server

**Example: Configuring the FlexVPN Server to Authenticate Peers Using EAP**

This example shows how to configure the FlexVPN server to authenticate peers using EAP.
aaa new-model
!
aaa group server radius eap-server
    server 192.168.2.1
!
aaa authentication login eap-list group eap-server
!
crypto pki trustpoint trustpoint1
    enrollment url http://192.168.3.1:80
    revocation-check crl
!
crypto ikev2 profile ikev2-profile1
    match identity remote address 0.0.0.0
    authentication local rsa-sig
    authentication remote eap query-identity
    pki trustpoint trustpoint1
    aaa authentication eap eap-list
    virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
    set transform-set trans transform1
    set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
    ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
    ip unnumbered Ethernet0/0
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile ipsec-profile1
!
radius-server host 192.168.2.1 key key1
!

Example: Configuring the FlexVPN Server for Group Authorization (External AAA)

The following example shows how to configure the FlexVPN server for group authentication through an external AAA, which would be the RADIUS or TACACS server.

aaa new-model
!
aaa group server radius cisco-acs
    server 192.168.2.2
!
aaa authorization network group=author-list group cisco-acs
!
crypto pki trustpoint trustpoint1
    enrollment url http://192.168.3.1:80
    revocation-check crl
!
crypto pki certificate map certmap1 1
    subject-name co cisco
!
crypto ikev2 name-mangler group=author-mangler
    dn domain
!
crypto ikev2 profile ikev2-profile1
    match certificate certmap1
    authentication local rsa-sig
    authentication remote rsa-sig
Example: Configuring the FlexVPN Server for Group Authorization (Local AAA)

The following example shows how to configure the FlexVPN server for group authorization through the local AAA using the IKEv2 authorization policy. The authorization policy specifies standard IPv4 and IPv6 attributes, and Cisco Unity, and FlexVPN attributes to be sent to the client through configuration mode. The authorization policy also specifies per user attributes through `aaa attribute list` command for local use.

```plaintext
aaa new-model

aaa authorization network local-group-author-list local

aaa attribute list attr-list1
  attribute type interface-config "ip mtu 1100"
  attribute type interface-config "tunnel key 10"

crypto pki trustpoint trustpoint1
  enrollment url http://192.168.3.1:80
  revocation-check crl

crypto pki certificate map certmap1 1
  subject-name co cisco

crypto ikev2 authorization policy author-policy1
  pool pool1
  dhcp server 192.168.4.1
  dhcp timeout 10
  dhcp giaddr 192.168.1.1
  dns 10.1.1.1 10.1.1.2
  route set access-list acl1
  wins 192.168.1.2 192.168.1.3
  netmask 255.0.0.0
  banner ^C flexvpn server ^C
  configuration url http://www.abc.com
  configuration version 10
  def-domain abc.com
  split-dns dns1
  split-dns dns2
  split-dns dns3
  backup-gateway gw1
```
Example: Configuring the FlexVPN Server for User Authorization

The following example shows how to configure the FlexVPN server for user authentication.

```
aaa new-model
!
aaa group server radius cisco-acs
    server 192.168.2.2
!
aaa authorization network user-author-list group cisco-acs
!
crypto pki trustpoint trustpoint1
    enrollment url http://192.168.3.1:80
    revocation-check crl
!
crypto pki certificate map certmap1
    subject-name co cisco
!
crypto ikev2 name-mangler user-author-mangler
    dn common-name
!
crypto ikev2 profile ikev2-profile1
    match certificate certmap1
    authentication local rsa-sig
    authentication remote rsa-sig
    pki trustpoint trustpoint1
    aaa authorization user cert list user-author-list name-mangler user-author-mangler
```

```
Example: Configuring the FlexVPN Server for IPv6 Session with IPv6 Configuration Attributes

The following example shows how to configure the FlexVPN server for an IPv6 dynamic Virtual Tunnel Interfaces (dVTI) session. The example uses local AAA group authorization using the IKEv2 authorization policy. The IPv6 configuration attributes are configured under the IKEv2 authorization policy.

```
avirtual-template 1
! crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
! crypto ipsec profile ipsec-profile1
  set transform-set trans transform1
  set ikev2-profile ikev2-profile1
! interface Ethernet0/0
  ip address 192.168.1.1 255.255.255.0
! interface Virtual-Template1 type tunnel
  ip unnumbered Ethernet0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile ipsec-profile1
! radius-server host 192.168.2.2 key key2
```

```
Example: Configuring the FlexVPN Server for IPv6 Session with IPv6 Configuration Attributes

aaa new-model
!
aaa authorization network local-group-author-list local
!
crypto pki trustpoint trustpoint1
  enrollment url http://192.168.3.1:80
  revocation-check crl
!
crypto pki certificate map certmap1 1
  subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
  ipv6 pool v6-pool
  ipv6 dns 2001:DB8:1::11 2001:DB8:1::12
  ipv6 subnet-acl v6-acl
!
crypto ikev2 profile ikev2-profile1
  match certificate certmap1
  authentication local rsa-sig
  authentication remote rsa-sig
  pki trustpoint trustpoint1
  aaa authorization group cert list local-group-author-list author-policy1
  virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
  set transform-set trans transform1
  set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
  ipv6 address 2001:DB8:1::1/32
!
interface Virtual-Template1 type tunnel
  ipv6 unnumbered Ethernet0/0
  tunnel mode ipsec ipv6
  tunnel protection ipsec profile ipsec-profile1
```

Configuring the FlexVPN Server
Example: Configuring AnyConnect Profile Download

The following example shows how to configure the FlexVPN AnyConnect Profile Download feature:

```
no ip http secure-server
crypto ssl policy ssl-policy
  pki trustpoint CA1 sign
  ip address local 10.0.0.1 port 443
no shutdown
crypto ssl profile ssl_prof
  match policy ssl-policy
crypto vpn anyconnect profile ANY-PROF bootflash:profile.xml
crypto ikev2 profile ikev2_profile
  anyconnect profile ANY-PROF
```

Additional References for Configuring the FlexVPN Server

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Security commands</td>
<td>• Cisco IOS Security Command Reference Commands A to C</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference Commands D to L</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference Commands M to R</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference Commands S to Z</td>
</tr>
<tr>
<td>IPsec configuration</td>
<td>Configuring Security for VPNs with IPsec</td>
</tr>
<tr>
<td>Recommended cryptographic algorithms</td>
<td>Next Generation Encryption</td>
</tr>
</tbody>
</table>
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 Configuring the FlexVPN Server

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 4: Feature Information for Configuring the FlexVPN Server

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlexVPN AnyConnect Profile Download</td>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>The FlexVPN AnyConnect Profile Download feature enables a device running Cisco IOS XE software to connect and push the profile information in IKEv2 protocol to Cisco AnyConnect Secure Mobility client. The following commands were introduced: anyconnect profile, crypto vpn anyconnect profile.</td>
</tr>
<tr>
<td>IKEv2 headend support for remote access clients</td>
<td>Cisco IOS XE Release 3.5S</td>
<td>This feature provides IKEv2 support for Anyconnect 3.0, FlexVPN hardware client, and multi SA support for VTI. The following commands were introduced or modified: aaa attribute list, backup-gateway, banner, config-mode set, configuration url, configuration version, def-domain, dhcp, dns, include-local-lan, max flow limit, pfs, pool, route accept, route set interface, smartcard-removal-disconnect, split-dns, subnet-acl.</td>
</tr>
</tbody>
</table>