Understand IKEv2 and AnyConnect Reconnect Feature

Contents

Introduction

This document describes how IKEv2 Auto Reconnect feature works on Cisco IOS® and Cisco IOS® XE routers for AnyConnect.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Internet Key Exchange version 2 (IKEv2)
- Cisco Secure Client (CSC)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Catalyst 8000V (C8000V) running version 17.16.01a

- Cisco Secure Client version 5.1.8.105
- Client PC with Cisco Secure Client installed

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

IKEv2 and Cisco Secure Client Reconnect Feature

The Auto Reconnect feature in the Cisco Secure Client helps it to remember the session for a period of time and to resume the connection after establishing the secure channel. As the Cisco Secure Client is extensively used with Internet Key Exchange Version 2 (IKEv2), IKEv2 extends the Auto Reconnect feature support on Cisco IOS software through the Cisco IOS IKEv2 support for Auto Reconnect feature of Secure Client feature.

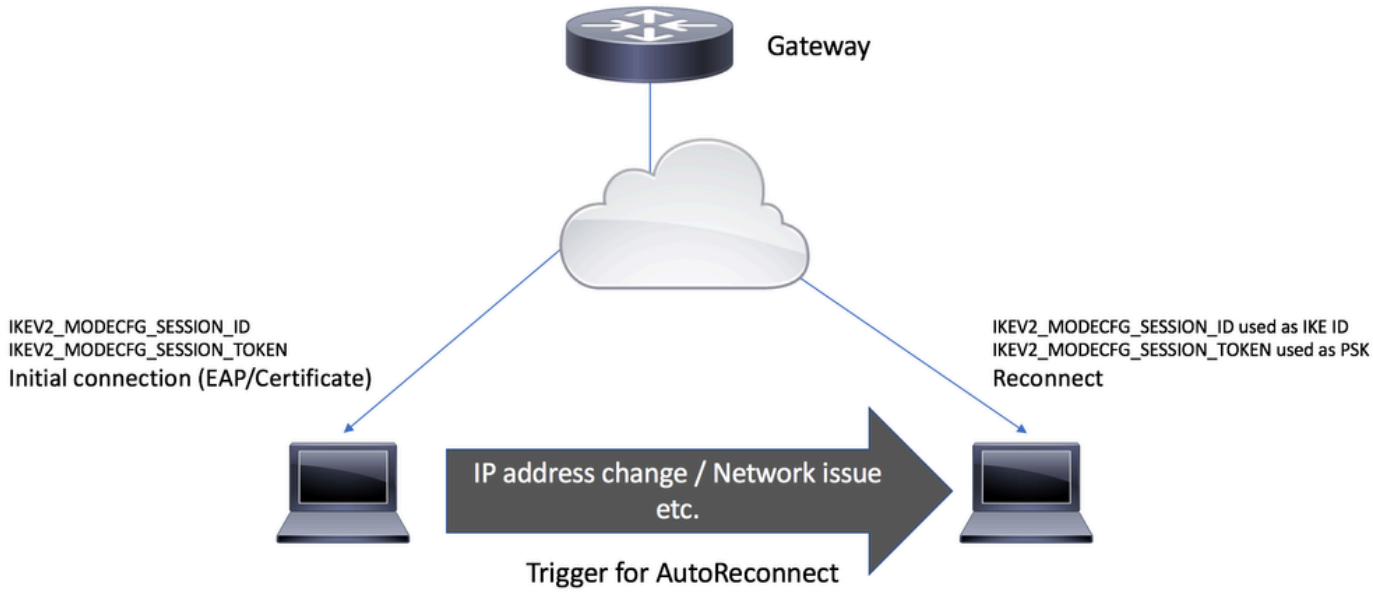
Auto Reconnect in the Cisco Secure Client occurs in the these scenarios:

1. The intermediate network is down. The Cisco Secure Client tries to resume the session when it is up.
2. The Cisco Secure Client device switches between networks. This results in source port change, which brings down the existing security association (SA) and, hence, the Cisco Secure Client tries to resume the SA using the Auto Reconnect feature.
3. The Cisco Secure Client device tries to resume SA after returning from sleep or hibernate mode.

Advantages of Auto Reconnect Feature

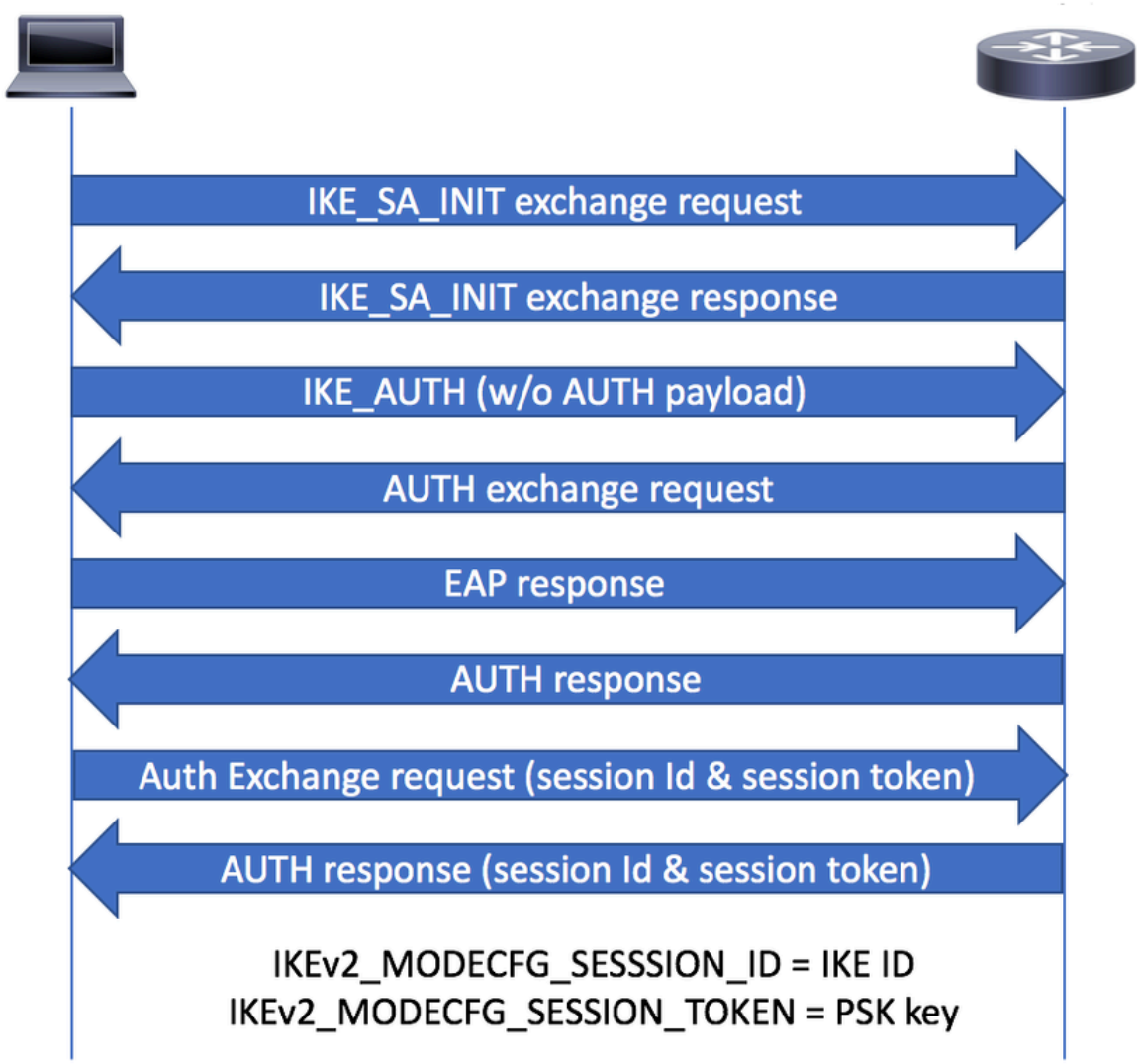
- The config attributes used in the original session are reused without querying the authentication, authorization, and accounting (AAA) server.
- The IKEv2 gateway does not have to contact the RADIUS server for reconnecting to the client.
- No user interaction for authentication or authorization is needed during resuming the session.
- The authentication method is the preshared key when reconnecting a session. This authentication method is quick compared to other authentication methods.
- The preshared key authentication method helps in resuming a session on the Cisco IOS software with minimal resources.
- The unused security associations (SAs) are removed thereby freeing the crypto resources.

Auto Reconnect Connection Flow

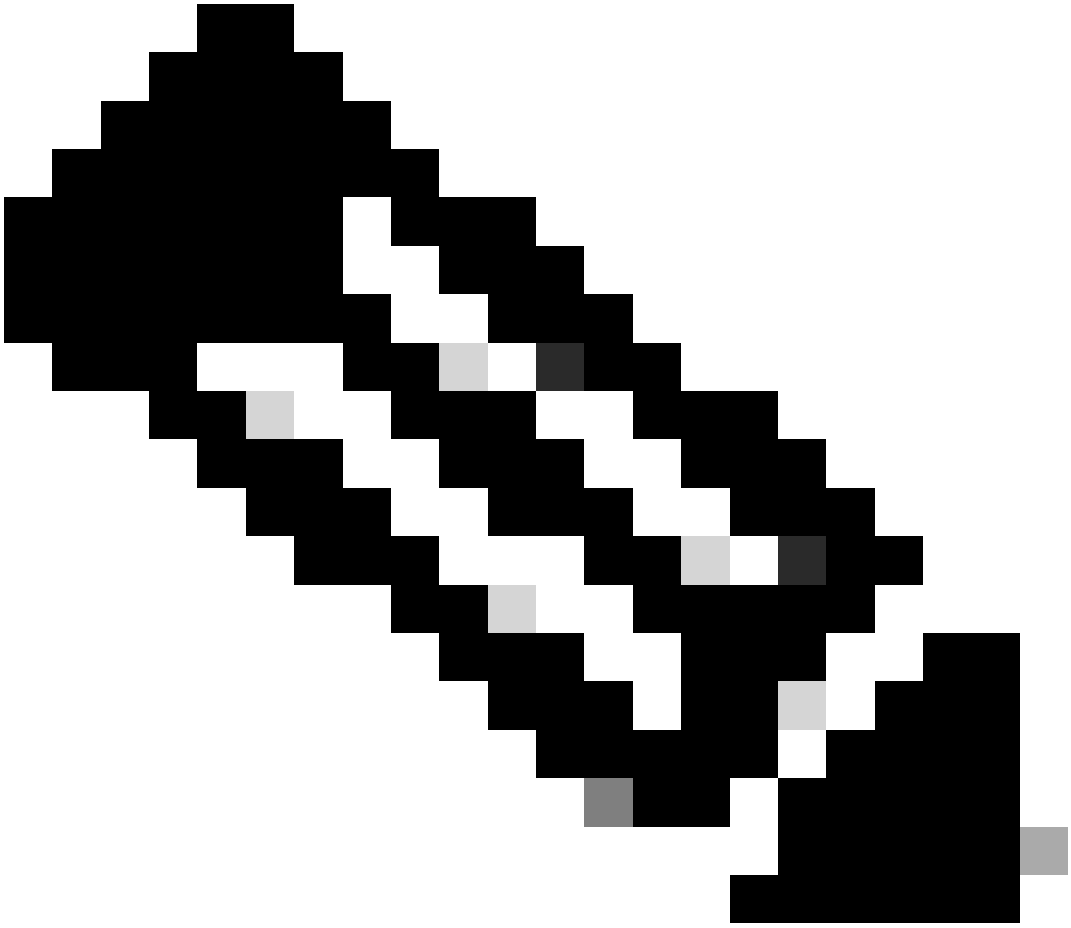


Trigger for AutoReconnect

1. During the AUTH exchange, Cisco Secure Client requests for the Session-token and Session-id attribute from IKEv2 Gateway in MODECFG_REQ payload of IKE_AUTH Request.
2. IKEv2 Gateway checks if the Cisco IOS IKEv2 support for the Auto Reconnect feature of Secure Client feature is enabled in the IKEv2 profile using the reconnect command, selects the IKEv2 policy of the chosen IKEv2 profile, and sends the session ID and the session token attributes to the Secure Client in CFGMODE_REPLY payload of the IKE_AUTH response.

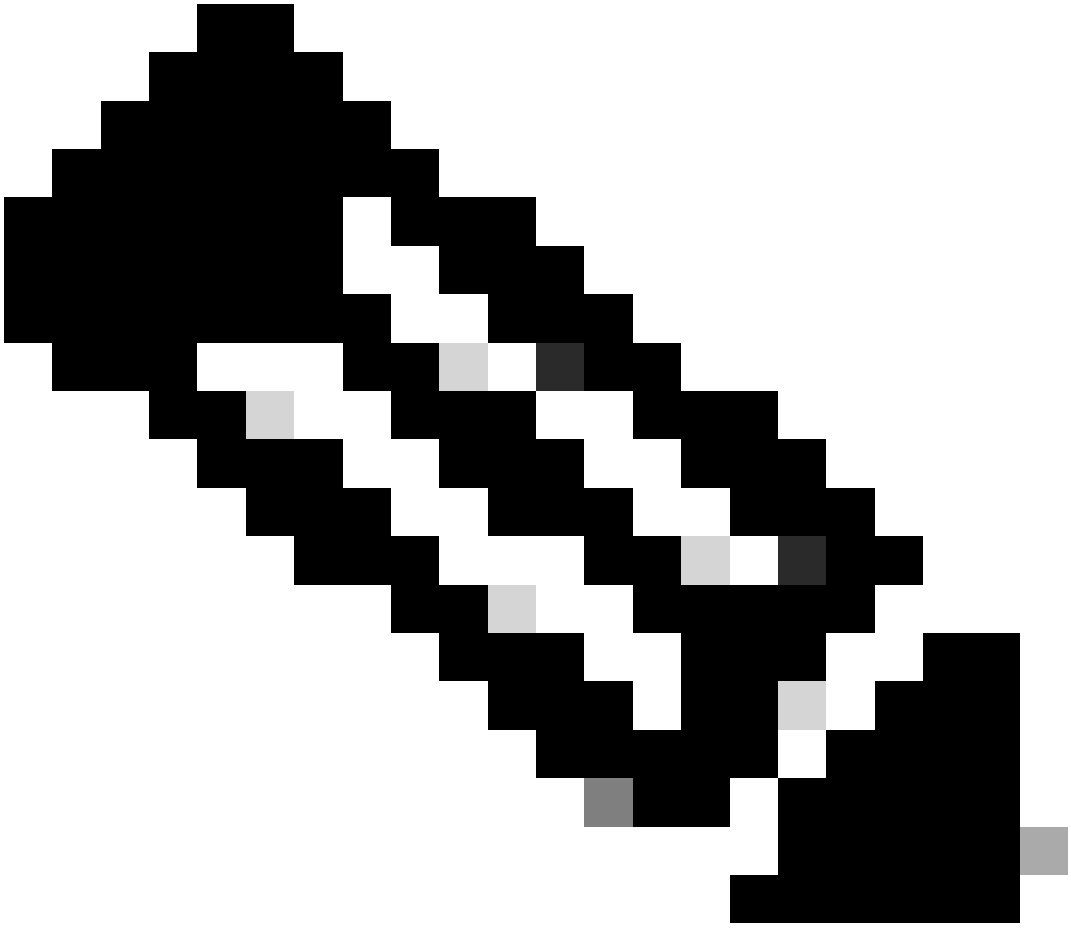


CFGMODE Exchange

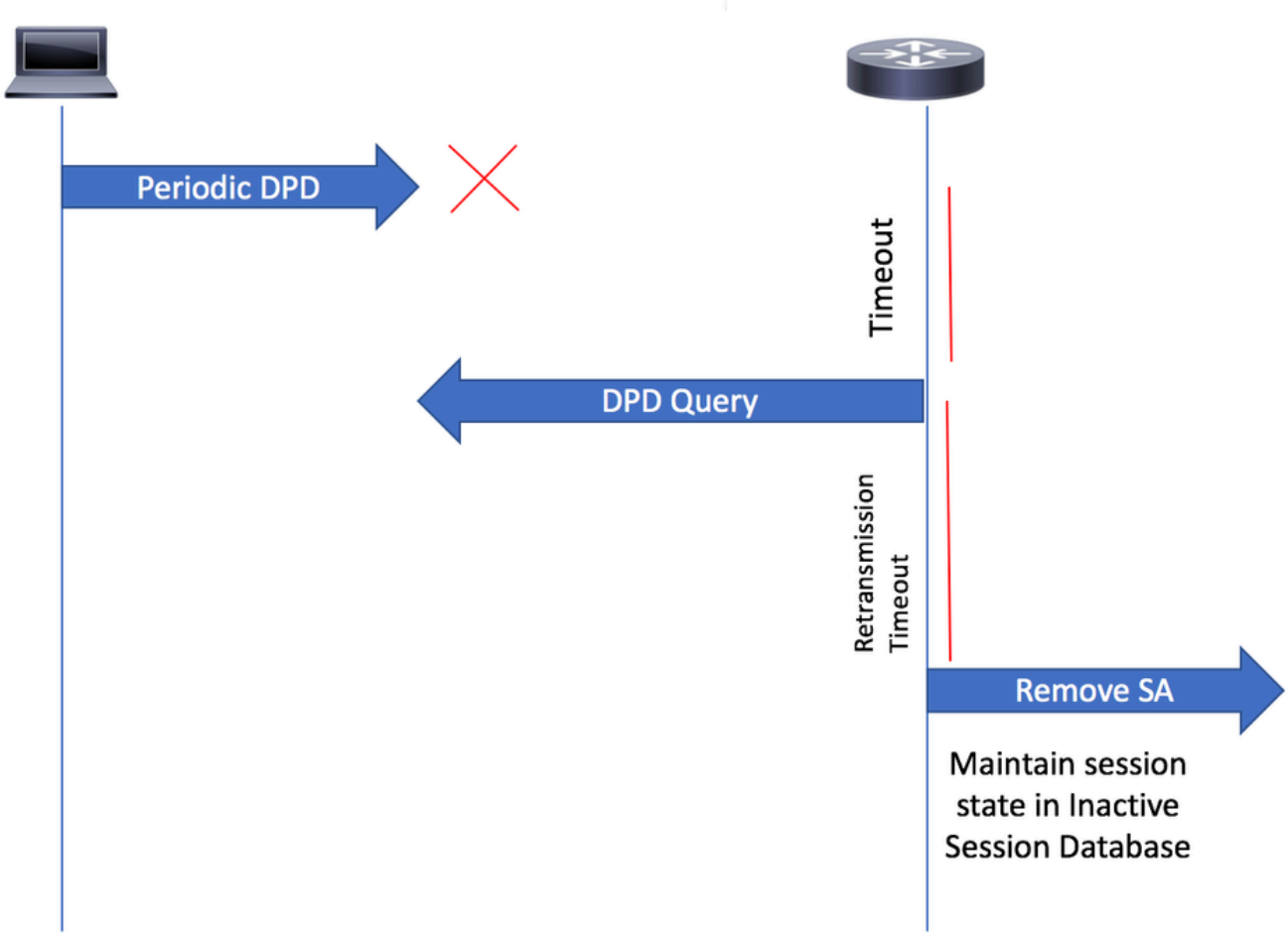


Note: The process of identifying non-responding client is based on Dead Peer Detection (DPD). If the reconnect feature is enabled in the IKEv2 profile, you do not need to configure DPD, as DPD is queued as on-demand in IKEv2

3. The Cisco Secure Client periodically sends DPD messages to the gateway. If DPD is queued as on-demand, the gateway does not send DPD messages to the client until it receives DPD from the client. If DPD is not received from Secure Client within the specified time period (as per configured DPD interval), the gateway sends a DPD message. If no response is received from the Secure Client, the SA is deleted from the active session database.



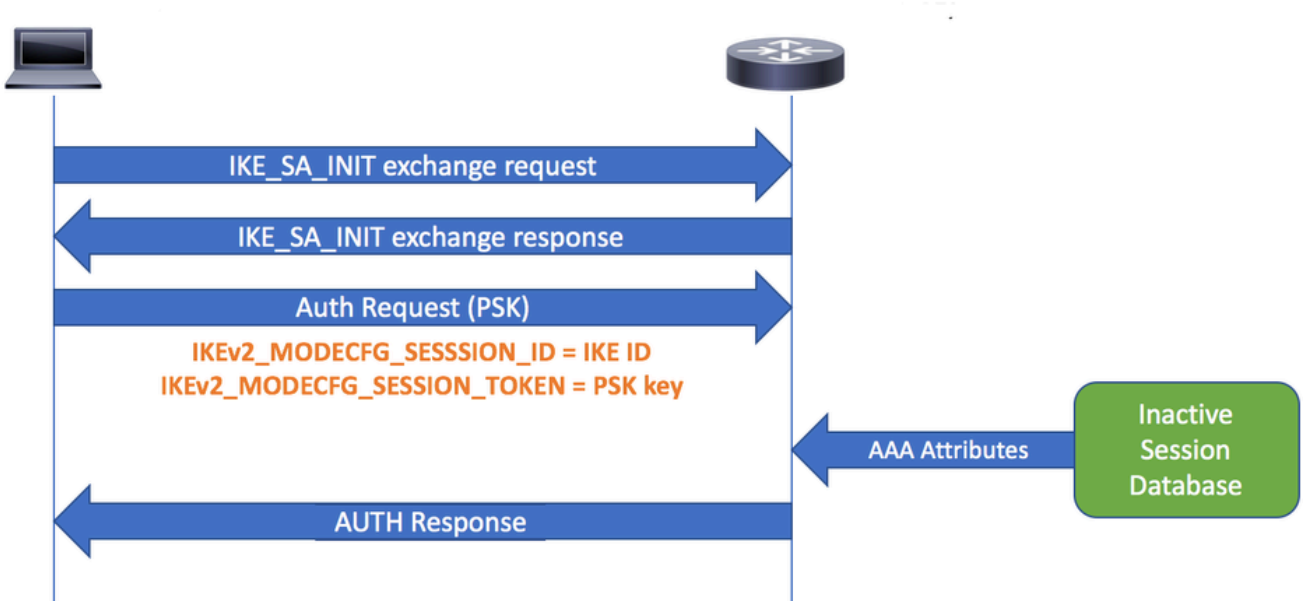
Note: The Gateway still maintains the session state (such as AAA Attributes) in a separate inactive session database to allow the reconnection as per configured reconnect timeout period.



DPD Query

4. When the client tries to reconnect, it creates a new IKE SA and uses the IKE identity (ID) as the Session ID, which it received from the MODECFG_REPLY payload. At this point, Cisco Secure Client uses IKE PSK authentication for the reconnection, with the pre-shared key being the session token it received earlier.

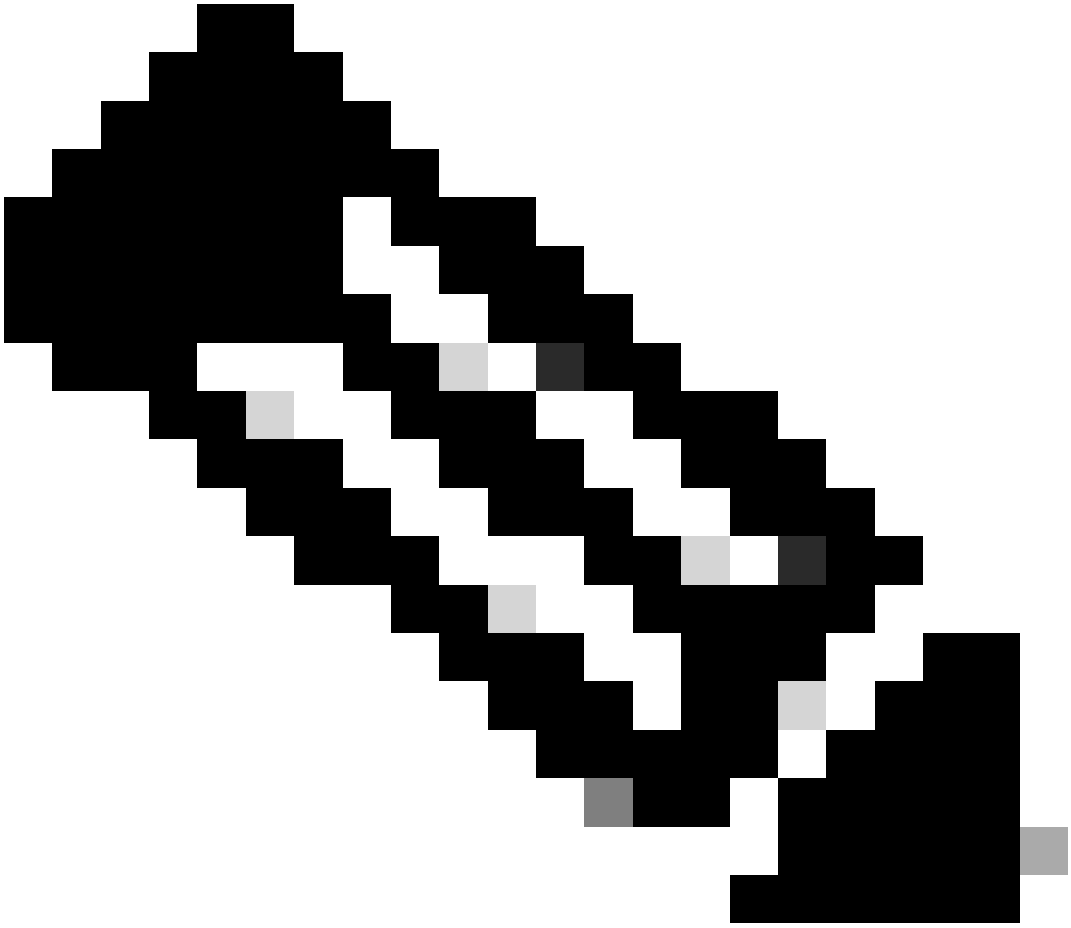
5. When the gateway receives a reconnect request, it searches the Inactive Session Database for the peer IKE ID (which serves as the session ID). During reconnection, the stored custom attributes from the Inactive Database are retrieved and applied to the new SA.



Reconnect

Configure

Router Configuration



Note: For router configuration you can also refer to the document Configure FlexVPN Headend for Secure Client (AnyConnect) IKEv2 Remote Access Using Local User Database

This configuration snippet shows an example of Cisco Secure Client IKEv2 Remote Access configuration and how AutoReconnect is enabled by configuring **reconnect** under the IKEv2 profile.

<#root>

```
aaa new-model
!
!
aaa authentication login a-eap-authen-local local
aaa authorization network a-eap-author-grp local
!
username test password 0 cisco
!
ip local pool ACPOOL 192.168.20.5 192.168.20.10
!
ip access-list standard split_tunnel
10 permit 192.168.10.0 0.0.0.255
!
```

```
crypto ikev2 authorization policy ikev2-auth-policy
 pool ACPOOL
 def-domain example.com
 route set access-list split_tunnel
!
crypto ikev2 proposal default
encryption aes-cbc-256
integrity sha512 sha384
group 19 14 21
!
crypto ikev2 policy default
match fvrf any
proposal default
!
!
```

crypto ikev2 profile AnyConnect-EAP

match identity remote key-id *$AnyConnectClient$*

```
authentication local rsa-sig
authentication remote anyconnect-eap aggregate
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 10
anyconnect profile acvpn
```

reconnect timeout 900

```
!
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
!
crypto vpn anyconnect bootflash:cisco-secure-client-win-5.1.8.105-webdeploy-k9.pkg sequence
crypto vpn anyconnect profile acvpn bootflash:acvpn.xml
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha384-hmac
mode tunnel
!
!
crypto ipsec profile AnyConnect-EAP
set transform-set TSET
set ikev2-profile AnyConnect-EAP
!
interface Virtual-Template10 type tunnel
 ip unnumbered GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile AnyConnect-EAP
```

Cisco Secure Client Profile

<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSc
    <ClientInitialization>
        <UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
        <AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
        <ShowPreConnectMessage>false</ShowPreConnectMessage>
        <CertificateStore>All</CertificateStore>
        <CertificateStoreOverride>false</CertificateStoreOverride>
        <ProxySettings>Native</ProxySettings>
        <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
        <AuthenticationTimeout>12</AuthenticationTimeout>
        <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
        <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
        <LocalLanAccess UserControllable="true">false</LocalLanAccess>
        <ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
        <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>


<AutoReconnect UserControllable="false">true



            <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>



        </AutoReconnect>


        <AutoUpdate UserControllable="false">true</AutoUpdate>
        <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
        <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
        <WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
        <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
        <PPPExclusion UserControllable="false">Disable
            <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
        </PPPExclusion>
        <EnableScripting UserControllable="false">false</EnableScripting>
        <EnableAutomaticServerSelection UserControllable="false">false
            <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
            <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
        </EnableAutomaticServerSelection>
        <RetainVpnOnLogoff>false
        </RetainVpnOnLogoff>
        <AllowManualHostInput>true</AllowManualHostInput>
    </ClientInitialization>
    <ServerList>
        <HostEntry>
            <HostName>IKEv2_Gateway</HostName>
            <HostAddress>flexvpn-c8kv.example.com</HostAddress>
            <PrimaryProtocol>

IPsec


                <StandardAuthenticationOnly>true
                    <AuthMethodDuringIKENegotiation>

EAP-AnyConnect

</AuthMethodDuringIKENegotiation>
                </StandardAuthenticationOnly>
            </PrimaryProtocol>
        </HostEntry>
    </ServerList>
```

```
</AnyConnectProfile>
```

Restrictions for Configuring IKEv2 Reconnect

1. The preshared key authorization method cannot be configured on the Internet Key Exchange Version 2 (IKEv2) profile. This is because the Cisco IOS IKEv2 support for AutoReconnect feature of Cisco Secure Client feature uses the preshared key authorization method and configuring the preshared key on the same IKEv2 profile can lead to confusion.
2. These commands cannot be configured on the IKEv2 profile:

- **authentication local pre-share**
- **authentication remote pre-share**
- **keyring, aaa authorization group psk**
- **aaa authorization user psk**

Verify

<#root>

```
sal_c8kv#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect

Interface: Virtual-Access1
Profile: AnyConnect-EAP
Uptime: 00:00:15
Session status: UP-ACTIVE
Peer: 10.106.69.69 port 63516 fvrf: (none) ivrf: (none)


Phase1_id: *$AnyConnectClient$*


      Desc: (none)
  Session ID: 16
  IKEv2 SA: local 10.106.45.225/4500 remote 10.106.69.69/63516 Active


Capabilities:DN

 connid:1 lifetime:23:59:45
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.20.5
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 15 drop 0 life (KB/Sec) 4607998/3585
        Outbound: #pkts enc'ed 15 drop 0 life (KB/Sec) 4608000/3585
```

<#root>

```
sal_c8kv#show crypto ikev2 session detailed
 IPv4 Crypto IKEv2 Session
```

```
Session-id:16, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.106.45.225/4500    10.106.69.69/63516    none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify:
```

AnyConnect-EAP

```
      Life/Active Time: 86400/620 sec
      CE id: 1016, Session-id: 16
      Status Description: Negotiation done
      Local spi: 67C3394ED1EAADE7        Remote spi: EBFE2587F20EA7C2
      Local id: 10.106.45.225
```

Remote id: *$AnyConnectClient$*

```
      Remote EAP id: user1
      Local req msg id:  0              Remote req msg id:  26
      Local next msg id: 0              Remote next msg id: 26
      Local req queued:  0              Remote req queued:  26
      Local window:      5              Remote window:      1
      DPD configured for 45 seconds, retry 2
      Fragmentation not  configured.
      Extended Authentication not configured.
      NAT-T is detected  outside
      Cisco Trust Security SGT is disabled
      Assigned host addr: 192.168.20.5
      Initiator of SA : No
      PEER TYPE: AnyConnect
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 192.168.20.5/0 - 192.168.20.5/65535
          ESP spi in/out: 0x2E14CBAF/0xD5590D3
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 256, esp_hmac: SHA384
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

This output shows that currently there is 1 active session which is capable of auto reconnect:

```
sal_c8kv#show crypto ikev2 stats reconnect
Total incoming reconnect connection: 0
Success reconnect connection: 0
Failed reconnect connection: 0
Reconnect capable active session count: 1
Reconnect capable inactive session count: 0
```

After Reconnect

When the Cisco Secure Client reconnects, it uses the IKEV2_MODECFG_SESSION_ID as the IKE ID. Therefore, after reconnection, the Phase1_id is no longer $AnyConnectClient$; instead, it is the session ID, as shown. Additionally, note that the capabilities now have **R** set. Here, **R** indicates that this is a reconnect session.

<#root>

```
sal_c8kv#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect

Interface: Virtual-Access2
Profile: AnyConnect-EAP
Uptime: 00:00:03
Session status: UP-ACTIVE
Peer: 10.106.69.69 port 54626 fvrf: (none) ivrf: (none)
```

Phase1_id: 724955484B6363445269557446544154771

```
      Desc: (none)
  Session ID: 17
  IKEv2 SA: local 10.106.45.225/4500 remote 10.106.69.69/54626 Active
```

Capabilities:DNR

```
 connid:1 lifetime:23:59:57
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.10.10.1
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 22 drop 0 life (KB/Sec) 4608000/3596
        Outbound: #pkts enc'ed 22 drop 0 life (KB/Sec) 4608000/3596
```

After reconnect, the authentication method is now PSK (pre-shared key) instead of AnyConnect-EAP as shown:

<#root>

```
sal_c8kv#show crypto ikev2 session detail
 IPv4 Crypto IKEv2 Session

Session-id:39, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.106.45.225/4500   10.106.69.69/54626     none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA,
```

Auth verify: PSK

```
      Life/Active Time: 86400/202 sec
      CE id: 1017, Session-id: 17
      Status Description: Negotiation done
      Local spi: 33F57D418CFAFEBD Remote spi: F2586DF08F2A8308
      Local id: 10.106.45.225
```

Remote id: 724955484B6363445269557446544154771

```
      Local req msg id:  0              Remote req msg id:  8
```

```
      Local next msg id: 0              Remote next msg id: 8
      Local req queued:  0              Remote req queued:  8
      Local window:      5              Remote window:      1
      DPD configured for 45 seconds, retry 2
      Fragmentation not  configured.
      Extended Authentication not configured.
      NAT-T is detected  outside
      Cisco Trust Security SGT is disabled
      Assigned host addr: 192.168.20.5
      Initiator of SA : No
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 192.168.20.5/0 - 192.168.20.5/65535
          ESP spi in/out: 0x38ADBE12/0xE3E00C0E
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 256, esp_hmac: SHA384
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

<#root>

```
sal_c8kv#show crypto ikev2 stats reconnect

Total incoming reconnect connection:        1


Success reconnect connection:               1


Failed reconnect connection:                0
Reconnect capable active session count:     1
Reconnect capable inactive session count:   0
IKEv2_Gateway#
```

Cisco Secure Client DART logs

<#root>

```
Date        : 03/13/2025
Time        : 01:27:35
Type        : Information
Source      : acvpnagent

Description :

The IPsec connection to the secure gateway has been established.


.
.
Date        : 03/13/2025
Time        : 01:29:05
Type        : Information
Source      : acvpnagent

Description : Current Preference Settings:
ServiceDisable: false
```

CertificateStoreOverride: false
CertificateStore: All
ShowPreConnectMessage: false
AutoConnectOnStart: false
MinimizeOnConnect: false
LocalLanAccess: false
DisableCaptivePortalDetection: false

AutoReconnect: true

AutoReconnectBehavior: ReconnectAfterResume

UseStartBeforeLogon: true
AutoUpdate: true
<snip>
IPProtocolSupport: IPv4,IPv6
AllowManualHostInput: true
BlockUntrustedServers: false
PublicProxyServerAddress:
.
.
Date : 03/13/2025
Time : 01:29:21
Type : Information
Source : acvpnui

Description : Message type information sent to the user:
Connected to IKEv2_Gateway.
.
.

!! Now system is put to sleep and resumes back.

Date : 03/13/2025
Time : 03:08:44
Type : Information
Source : acvpnagent

Description : ..

Client Agent continuing from system suspend.

Date : 03/13/2025
Time : 03:08:44
Type : Warning
Source : acvpnagent

Description : Session level reconnect reason code 9:

System resume from suspend mode (Sleep, Stand-by, Hibernate, etc).

Originates from session level

Date   : 03/13/2025
Time   : 03:08:44
Type   : Information
Source   : acvpnui

Description : Message type information sent to the user:
Reconnecting to IKEv2_Gateway...
.
.
Date   : 03/13/2025
Time   : 03:10:34
Type   : Information
Source   : acvpnagent

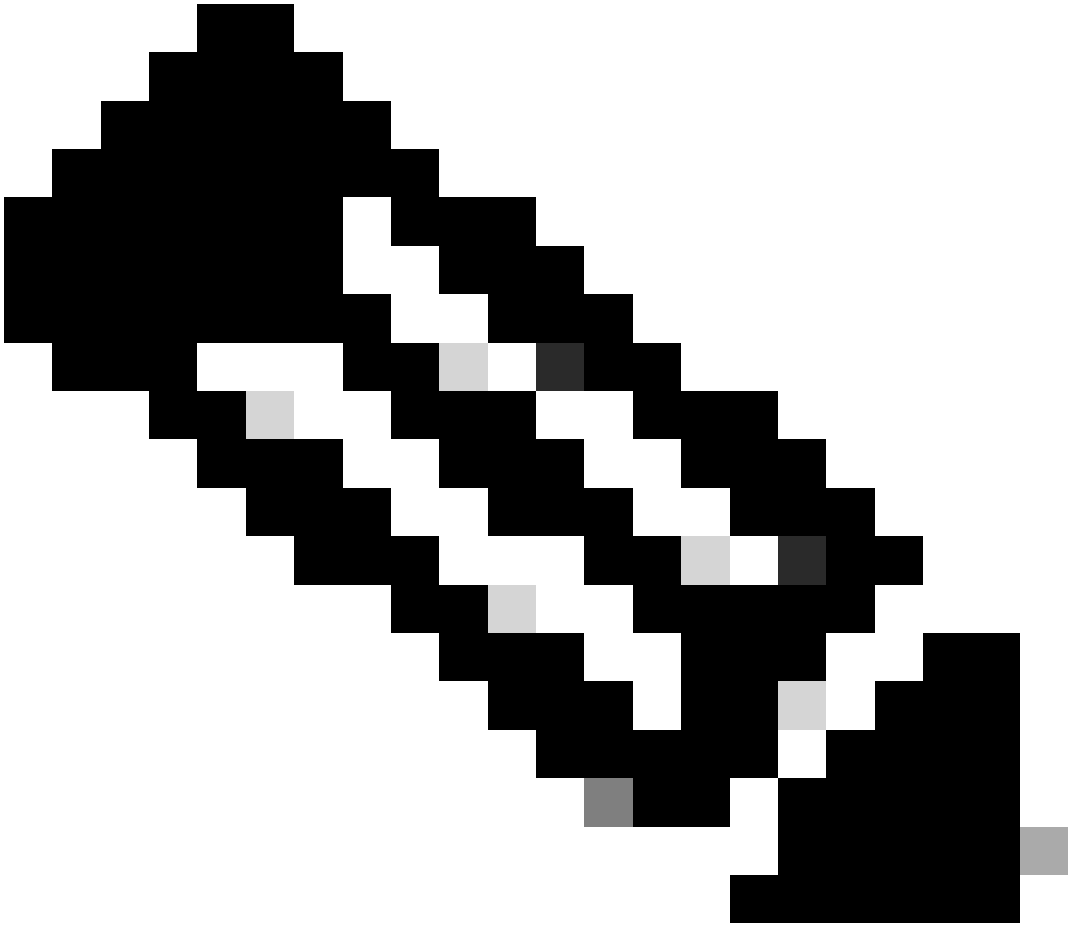
Description : Function: CIPsecProtocol::initiateTunnel
File: IPsecProtocol.cpp
Line: 613

Using IKE ID 'rIUHKccDRiUtFTATwq' for reconnect

.
.
Date   : 03/13/2025
Time   : 03:11:44
Type   : Information
Source   : acvpnui

Description : Message type information sent to the user:

Connected to IKEv2_Gateway.



Note: In DART logs, IKE ID is shown as 'rIUHKccDRiUtFTATwq' which is the ASCII representation of '724955484B6363445269557446544154771', shown as Remote ID in the output of "show crypto session detail".

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

IKEv2 debugs to verify the negotiation between the gateway and the client.

```
Debug crypto condition peer ipv4 <ipaddress>
Debug crypto ikev2
Debug crypto ikev2 packet
Debug crypto ikev2 internal
Debug crypto ikev2 error
```

Related Information

- Security and VPN Configuration Guide, Cisco IOS XE 17.x
- Technical Support & Documentation - Cisco Systems