了解IKEv2和AnyConnect重新连接功能

目录

简介

本文档介绍IKEv2自动重新连接功能在适用于AnyConnect的Cisco IOS®和Cisco IOS® XE路由器上如何工作。

先决条件

要求

Cisco 建议您了解以下主题：

- Internet密钥交换版本2(IKEv2)
- 思科安全客户端(CSC)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行版本17.16.01a的Cisco Catalyst 8000V(C8000V)
- 思科安全客户端5.1.8.105版
- 安装了Cisco Secure Client的客户端PC

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

IKEv2和思科安全客户端重新连接功能

Cisco安全客户端中的“自动重新连接”功能可帮助它记住会话一段时间，并在建立安全通道后恢复连接。由于Cisco Secure Client广泛用于互联网密钥交换版本2(IKEv2),IKEv2通过Cisco IOS IKEv2对Secure Client功能的Auto Reconnect功能的支持，扩展了Cisco IOS软件上的Auto Reconnect功能支持。

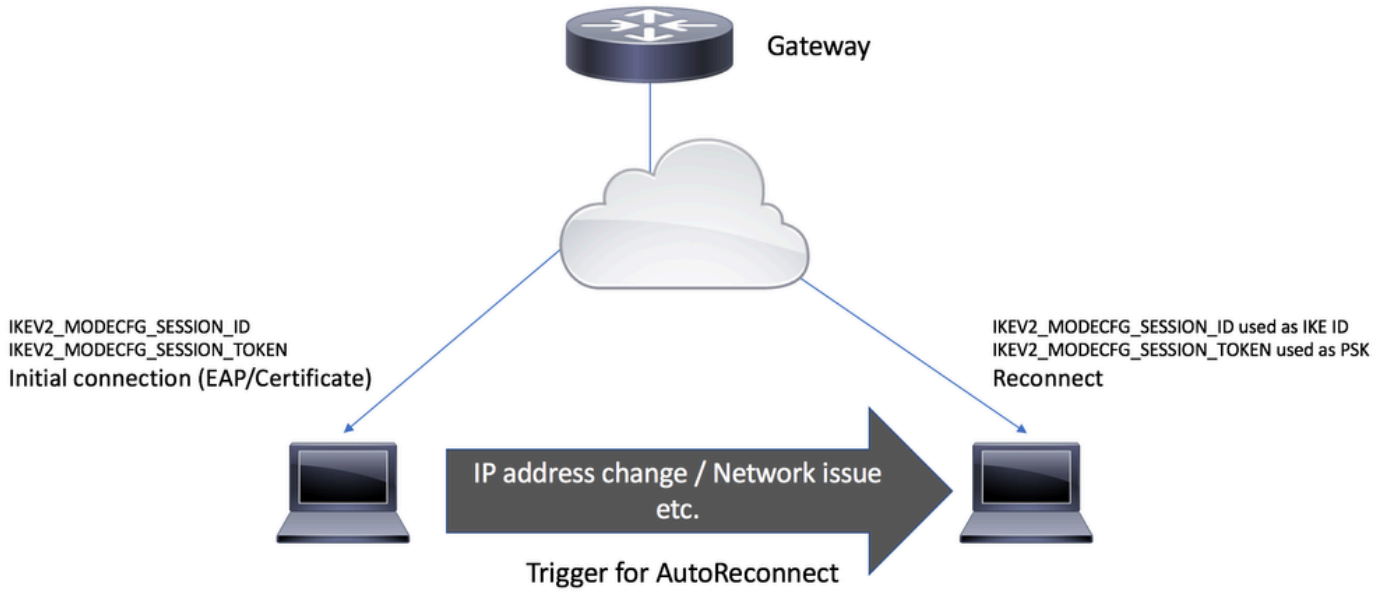
在以下情况下会出现Cisco安全客户端中的自动重新连接：

1. 中间网络已关闭。Cisco Secure Client会在会话启动时尝试恢复会话。
2. Cisco安全客户端设备在网络之间切换。这会导致源端口发生更改，这会导致现有安全关联(SA)断开，因此，Cisco安全客户端会尝试使用自动重新连接功能恢复SA。
3. Cisco安全客户端设备在从睡眠或休眠模式返回后尝试恢复SA。

自动重新连接功能的优点

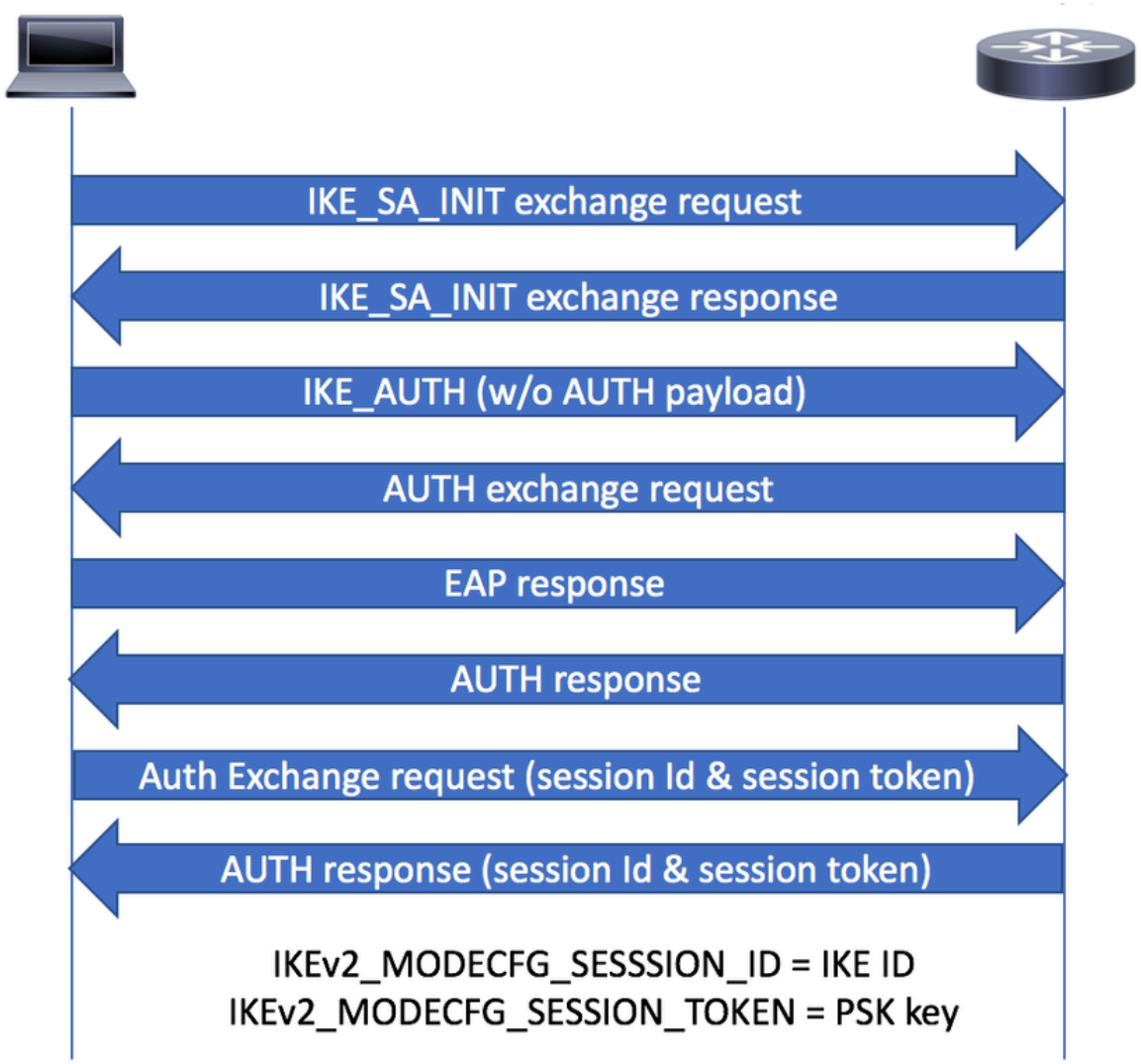
- 原始会话中使用的配置属性无需查询身份验证、授权和记帐(AAA)服务器即可重新使用。
- IKEv2网关无需联系RADIUS服务器即可重新连接到客户端。
- 在恢复会话期间，不需要进行身份验证或授权的用户交互。
- 重新连接会话时，身份验证方法是预共享密钥。与其他身份验证方法相比，此身份验证方法速度较快。
- 预共享密钥身份验证方法有助于以最少的资源在Cisco IOS软件上恢复会话。
- 删除未使用的安全关联(SA)，从而释放加密资源。

自动重新连接连接流

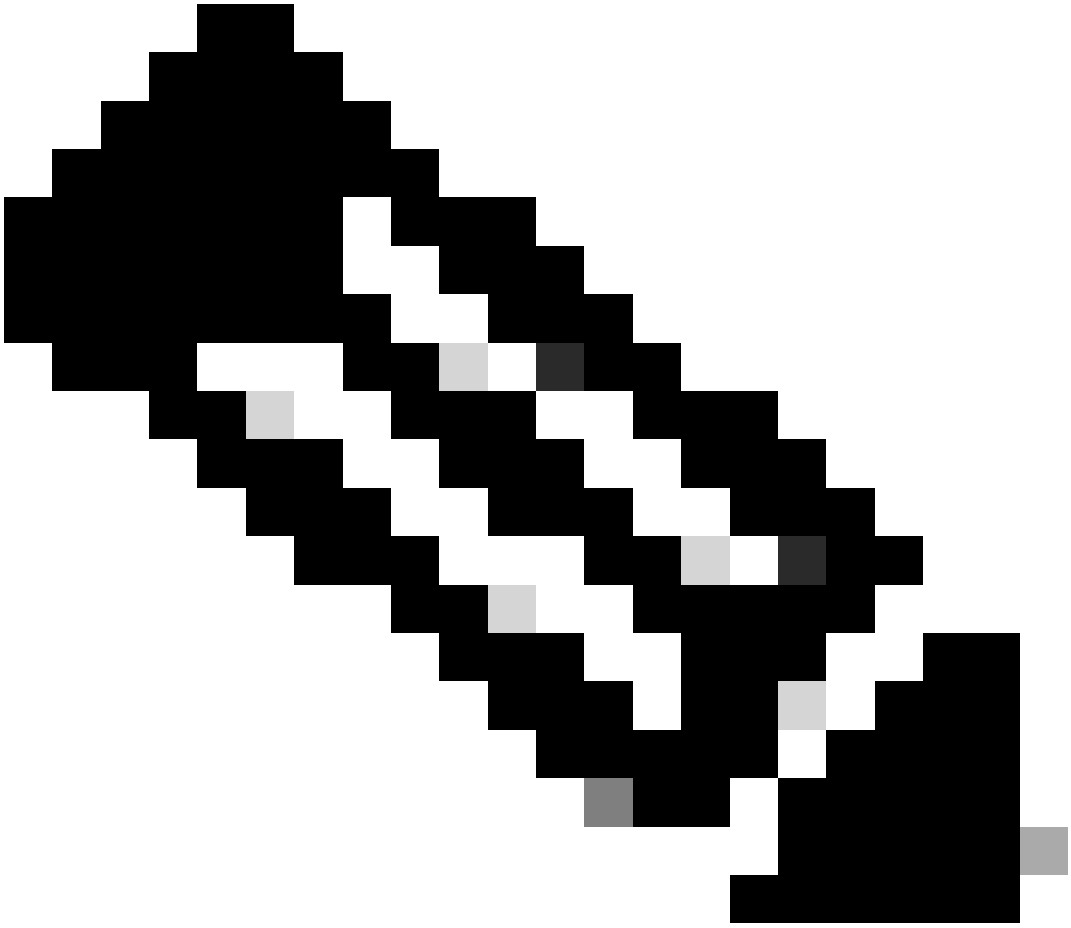


AutoReconnect触发器

1. 在身份验证交换期间，Cisco安全客户端从IKE_AUTH请求的MODECFG_REQ负载中的IKEv2网关请求会话令牌和会话ID属性。
2. IKEv2网关使用reconnect命令检查IKEv2配置文件中是否启用了安全客户端功能的自动重新连接功能的思科IOS IKEv2支持，选择所选IKEv2配置文件的IKEv2策略，并将会话ID和会话令牌属性发送到IKE_AUTH响应的CFGMODE_REPLY负载中的安全客户端。

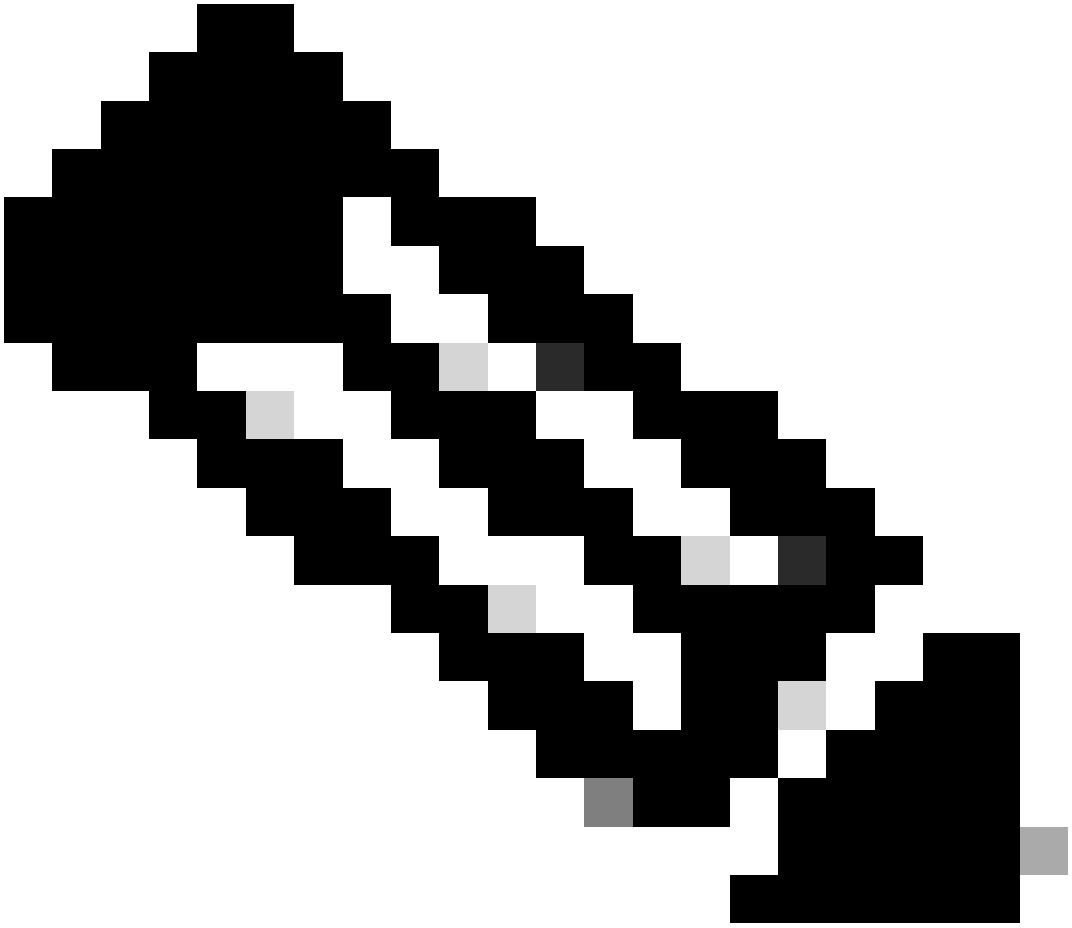

IKE_SA_INIT exchange request
IKE_SA_INIT exchange response
IKE_AUTH (w/o AUTH payload)
AUTH exchange request
EAP response
AUTH response
Auth Exchange request (session Id & session token)
AUTH response (session Id & session token)
IKEv2_MODECFG_SESSSION_ID = IKE ID
IKEv2_MODECFG_SESSION_TOKEN = PSK key

CFGMODE交换

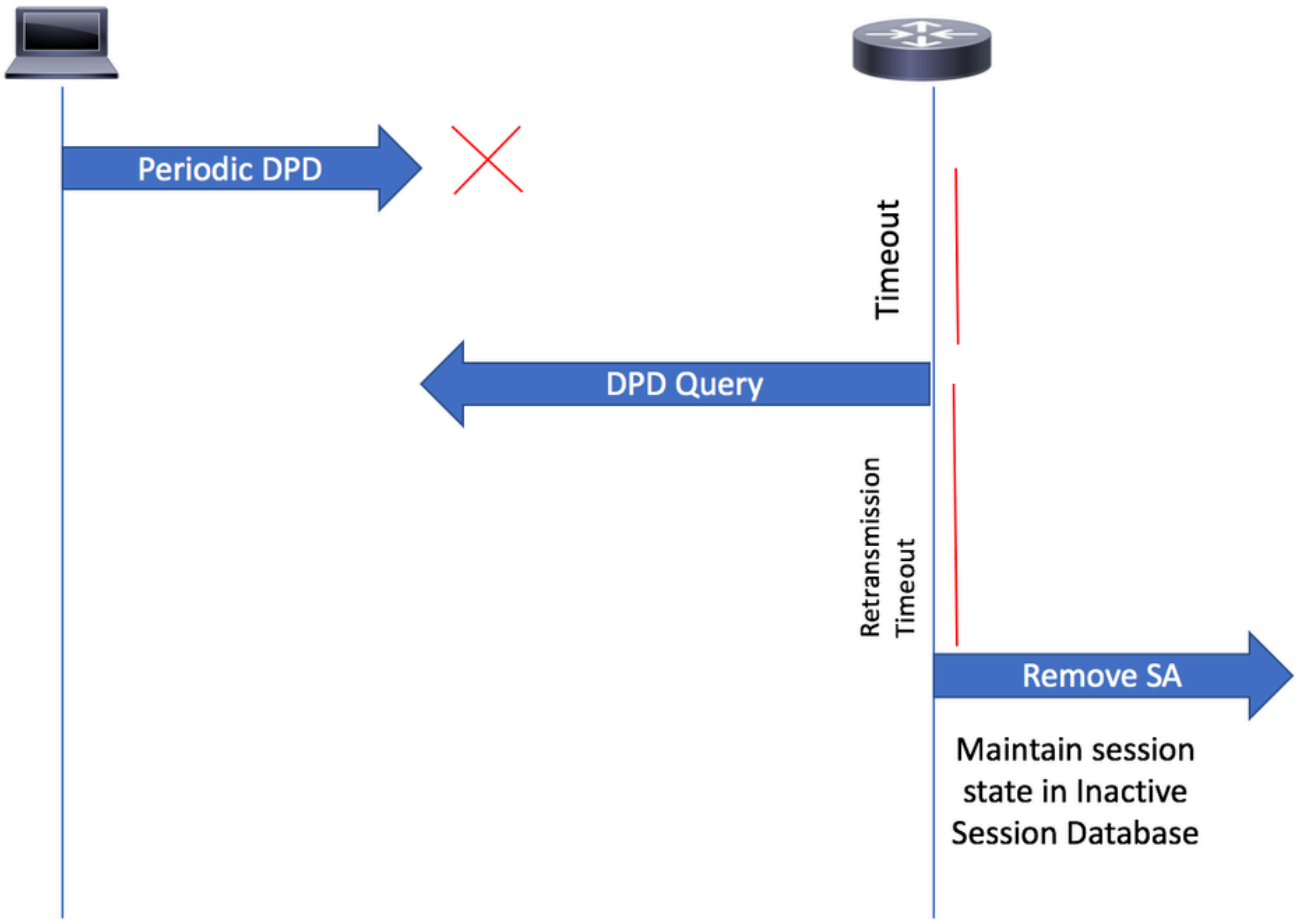


注意：识别无响应客户端的过程基于失效对等体检测(DPD)。 如果在IKEv2配置文件中启用了重新连接功能，则不需要配置DPD，因为DPD在IKEv2中按要求排队

3. Cisco安全客户端定期向网关发送DPD消息。如果DPD按要求排队，网关不会将DPD消息发送到客户端，直到收到来自客户端的DPD。如果在指定的时间段（根据配置的DPD间隔）内没有从安全客户端收到DPD，网关将发送DPD消息。如果未收到来自安全客户端的响应，则会从活动会话数据库中删除SA。



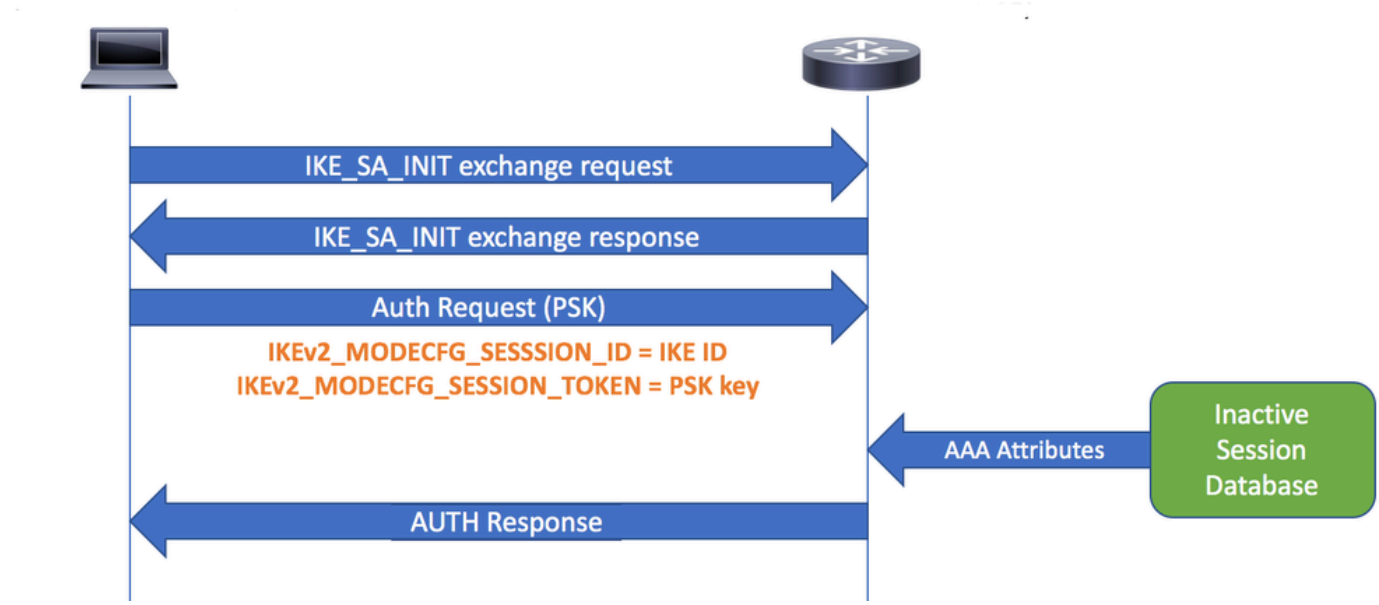
注意：网关仍会在单独的非活动会话数据库中维护会话状态（如AAA属性），以便根据配置的重新连接超时时间允许重新连接。



DPD查询

4.当客户端尝试重新连接时，它会创建新的IKE SA并使用IKE身份(ID)作为会话ID（从MODECFG_REPLY负载接收）。此时，Cisco安全客户端使用IKE PSK身份验证进行重新连接，其中预共享密钥是其之前收到的会话令牌。

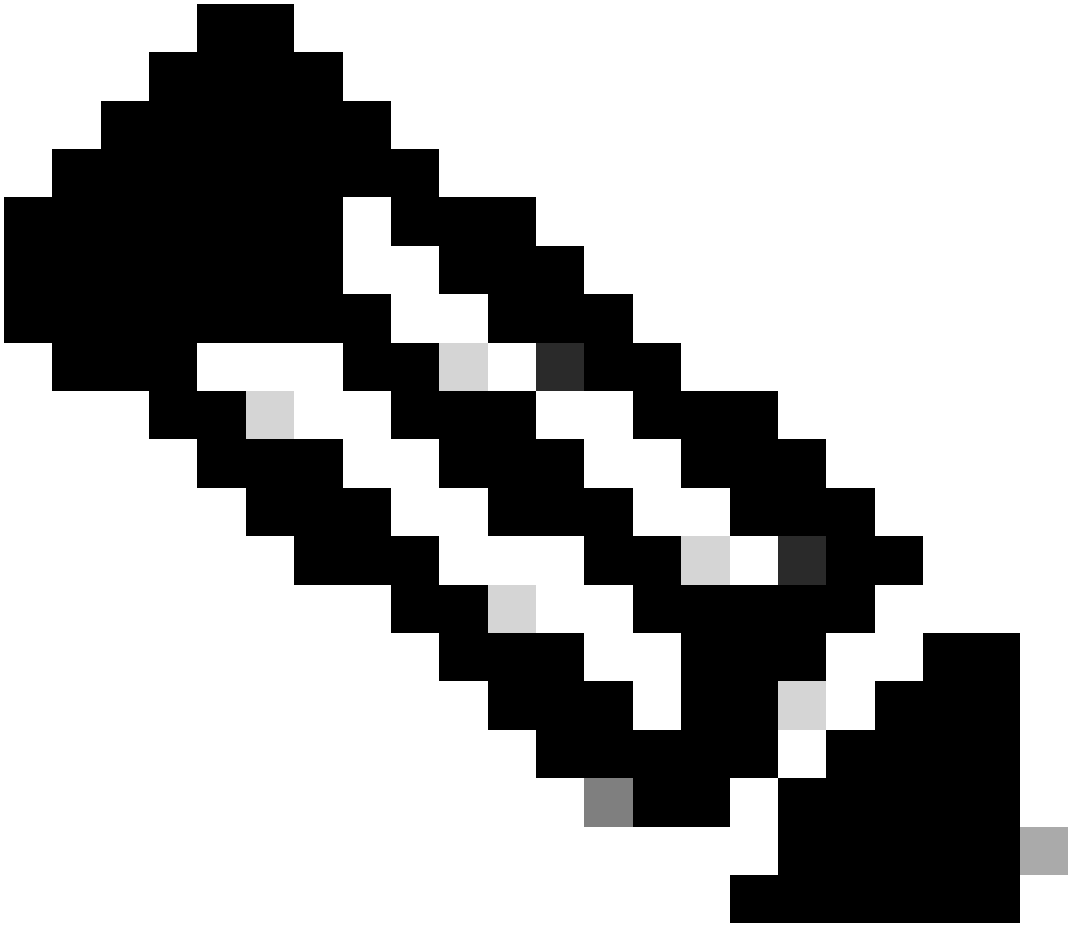
5.当网关收到重新连接请求时，它会在非活动会话数据库中搜索对等IKE ID（充当会话ID）。 在重新连接期间，将从非活动数据库中检索存储的自定义属性并将其应用于新的SA。



重新连接

配置

路由器配置



注意：有关路由器配置，您还可以参阅文档使用本地用户数据库配置安全客户端(AnyConnect)IKEv2远程访问的FlexVPN头端

此配置片段显示了Cisco安全客户端IKEv2远程访问配置的示例，以及如何通过在IKEv2配置文件下配置reconnect来启用AutoReconnect。

<#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
```

思科安全客户端配置文件

<#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>




       true









       ReconnectAfterResume









        <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>
```

配置IKEv2重新连接的限制

1. 无法在Internet密钥交换版本2(IKEv2)配置文件中配置预共享密钥授权方法。这是因为Cisco Secure Client功能的Cisco IOS IKEv2对AutoReconnect功能的支持使用预共享密钥授权方法，并且在同一IKEv2配置文件中配置预共享密钥会导致混乱。
2. 无法在IKEv2配置文件中配置以下命令：

- 身份验证本地预共享
- 身份验证远程预共享
- keyring、aaa authorization group psk
- aaa authorization user psk

验证

<#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
```

此输出显示当前有一个活动会话能够自动重新连接：

```
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
```

重新连接后

当Cisco安全客户端重新连接时，它使用IKEV2_MODECFG_SESSION_ID作为IKE ID。因此，重新连接后，Phase1_id不再是$AnyConnectClient$;而是会话ID，如下所示。此外，请注意，功能现在已设置为R。此处，R表示这是重新连接会话。

<#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
```

重新连接后，身份验证方法现在是PSK（预共享密钥）而不是AnyConnect-EAP，如下所示：

<#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#
```

思科安全客户端DART日志

<#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

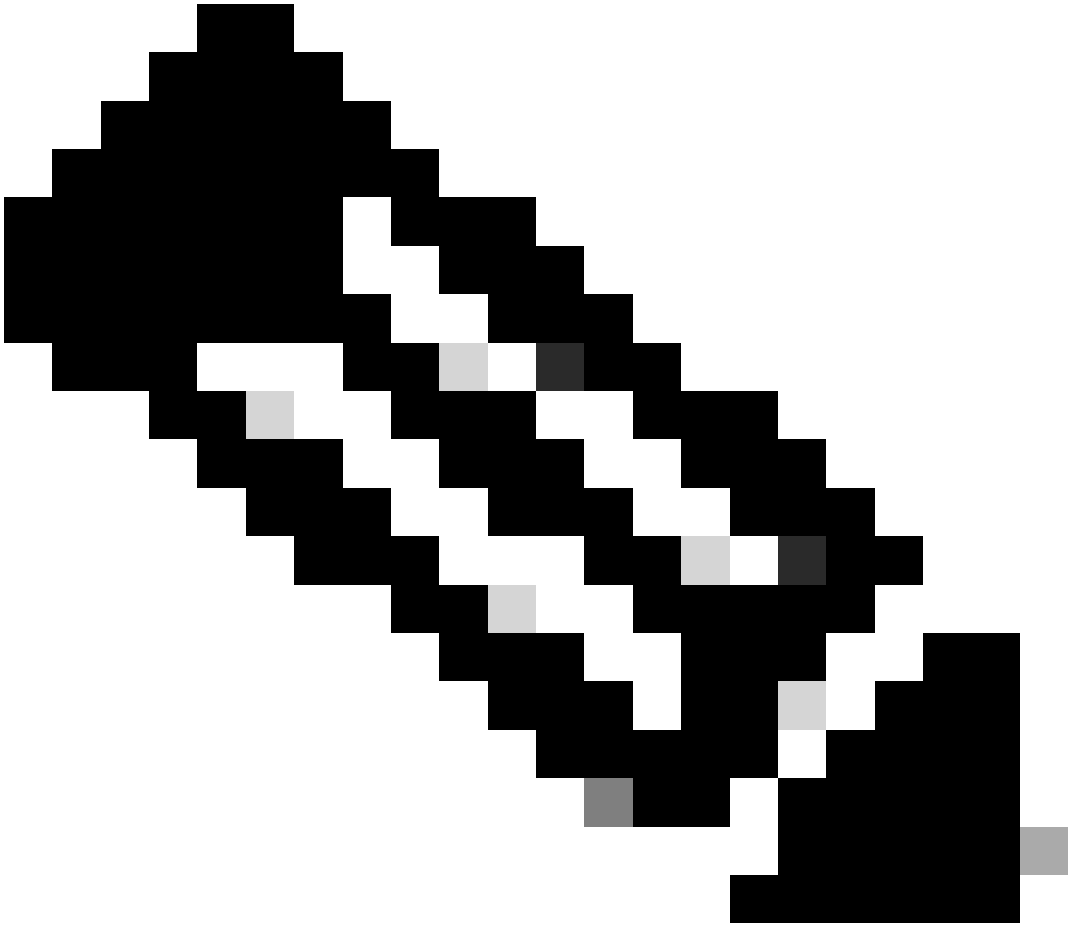
Description : Function: CIPsecProtocol::initiateTunnel
File: IPsecProtocol.cpp
Line: 613

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.



注意：在DART日志中，IKE ID显示为“rIUHKccDRiUtFTATwq”，这是“724955484B6363445269557446544154771”的ASCII表示，在“show crypto session detail”的输出中显示为远程ID。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

IKEv2调试，用于验证网关和客户端之间的协商。

```
Debug crypto condition peer ipv4
```

```
Debug crypto ikev2
Debug crypto ikev2 packet
Debug crypto ikev2 internal
```

```
Debug crypto ikev2 error
```

相关信息

- 安全和VPN配置指南，Cisco IOS XE 17.x
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。