瞭解IKEv2和AnyConnect重新連線功能

目錄

簡介

本文檔介紹IKEv2自動重新連線功能在適用於AnyConnect的Cisco IOS®和Cisco IOS® XE路由器上如何工作。

必要條件

需求

思科建議您瞭解以下主題：

- 網際網路金鑰交換版本2(IKEv2)
- 思科安全使用者端(CSC)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行版本17.16.01a的Cisco Catalyst 8000V(C8000V)
- 思科安全使用者端版本5.1.8.105
- 安裝了Cisco Secure Client的客戶端PC

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

IKEv2和思科安全客戶端重新連線功能

思科安全客戶端中的「自動重新連線」功能有助於它記住會話一段時間，並在建立安全通道後恢復連線。由於Cisco Secure Client與Internet Key Exchange Version 2(IKEv2)結合使用，IKEv2通過安全客戶端功能的Cisco IOS IKEv2自動重新連線功能擴展了Cisco IOS軟體上的「自動重新連線」功能支援。

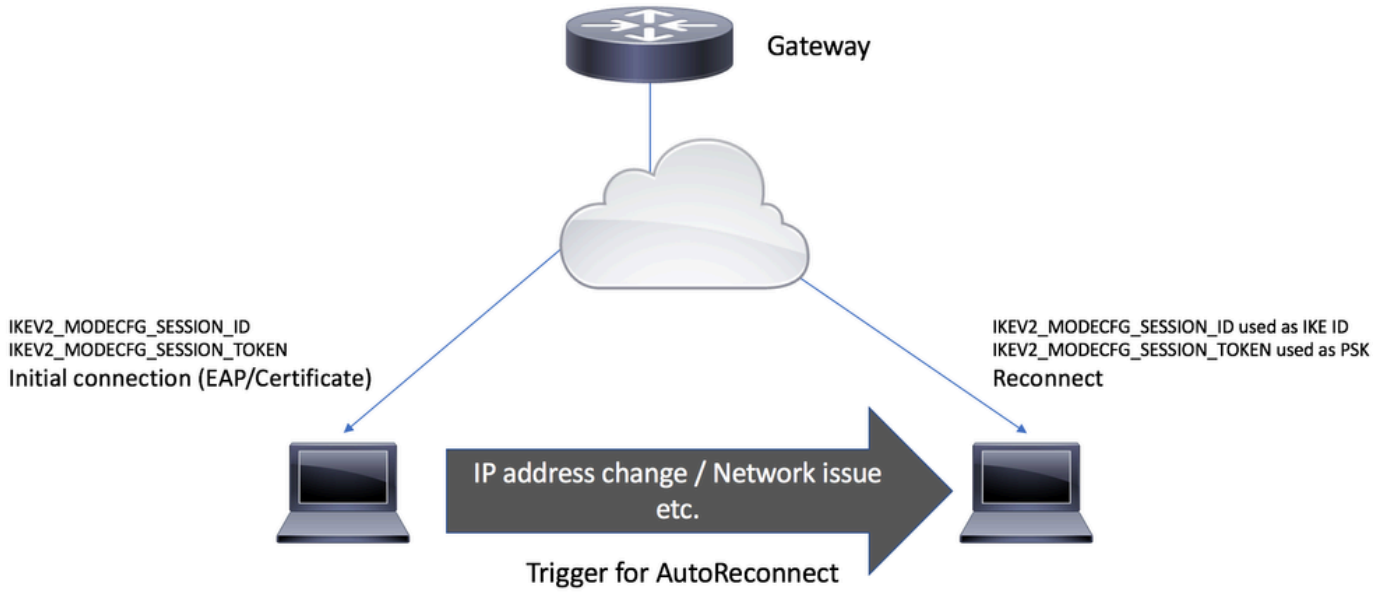
在下列情況下會發生思科安全客戶端中的自動重新連線：

1. 中間網路已關閉。Cisco Secure Client會在會話啟動時嘗試恢復會話。
2. Cisco Secure Client裝置在網路之間切換。這會導致來源連線埠變更，這會關閉現有的安全關聯(SA)，因此Cisco安全使用者端會嘗試使用自動重新連線功能恢復SA。
3. 在從休眠模式或休眠模式返回後，思科安全客戶端裝置會嘗試恢復SA。

自動重新連線功能的優點

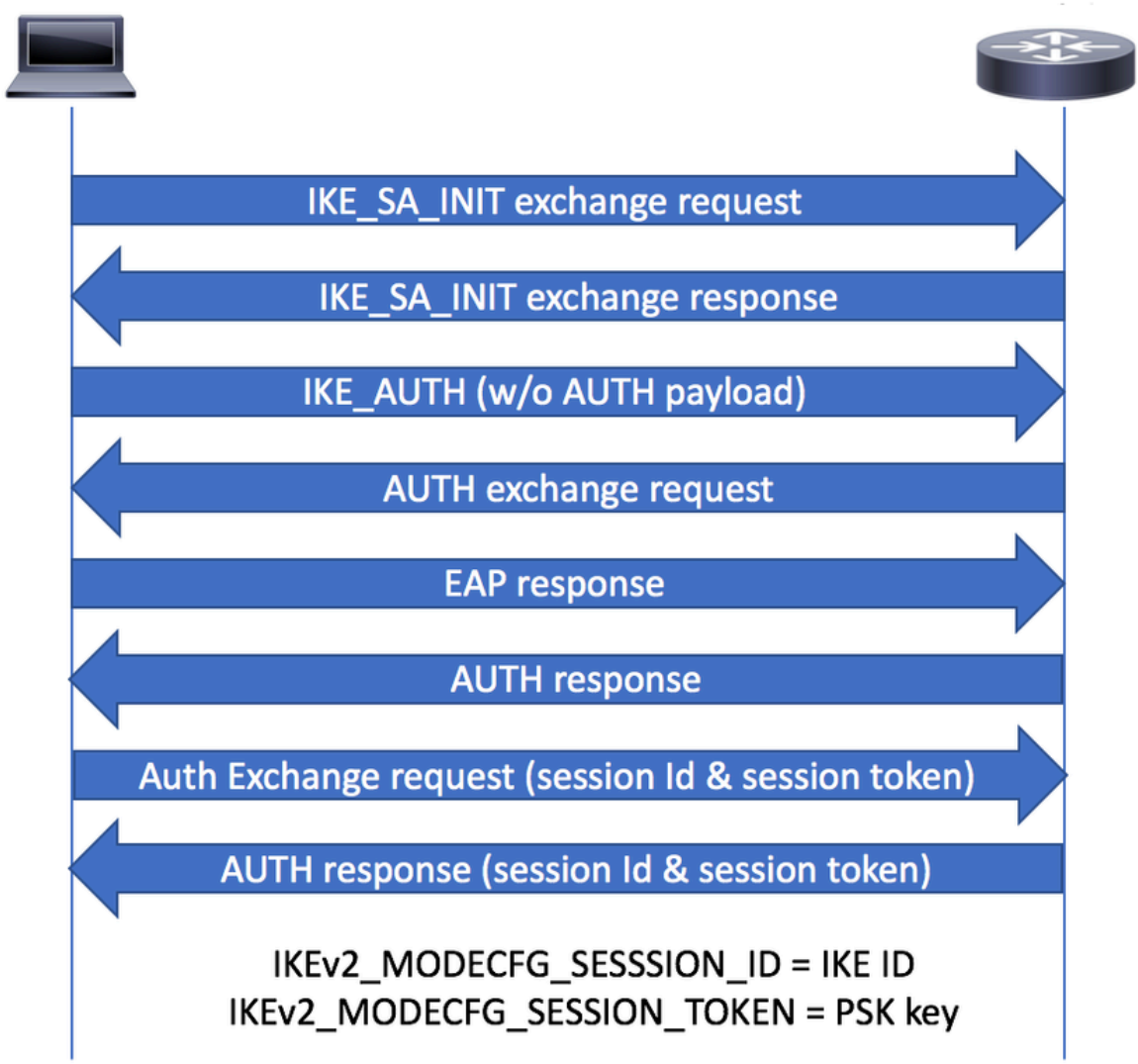
- 原始會話中使用的配置屬性無需查詢身份驗證、授權和記帳(AAA)伺服器即可重新使用。
- IKEv2網關無需聯絡RADIUS伺服器即可重新連線到客戶端。
- 在恢復會話期間，不需要進行身份驗證或授權的使用者互動。
- 驗證方法是重新連線會話時的預共用金鑰。與其它驗證方法相比，這種驗證方法快速。
- 預共用金鑰身份驗證方法有助於以最少的資源在Cisco IOS軟體上恢復會話。
- 未使用的安全關聯(SA)被移除，從而釋放了加密資源。

自動重新連線連線流

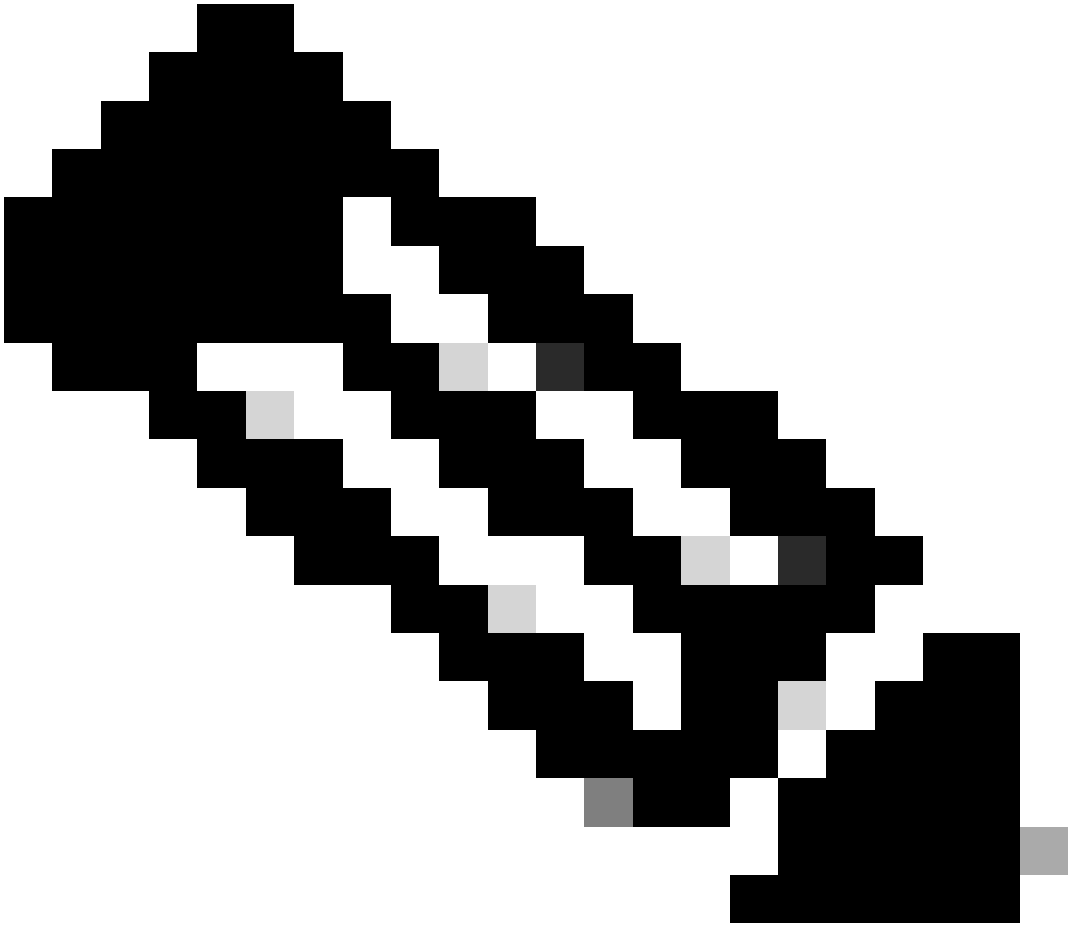


AutoReconnect觸發器

1. 在AUTH交換期間，Cisco安全使用者端會從IKE_AUTH請求的MODECFG_REQ負載中的IKEv2閘道要求Session-token和Session-id屬性。
2. IKEv2網關使用reconnect命令檢查IKEv2配置檔案中是否啟用了對安全客戶端功能的自動重新連線功能的Cisco IOS IKEv2支援，選擇所選IKEv2配置檔案的IKEv2策略，並在IKE_AUTH響應的CFGMODE_REPLY負載中將會話ID和會話令牌屬性傳送到安全客戶端。

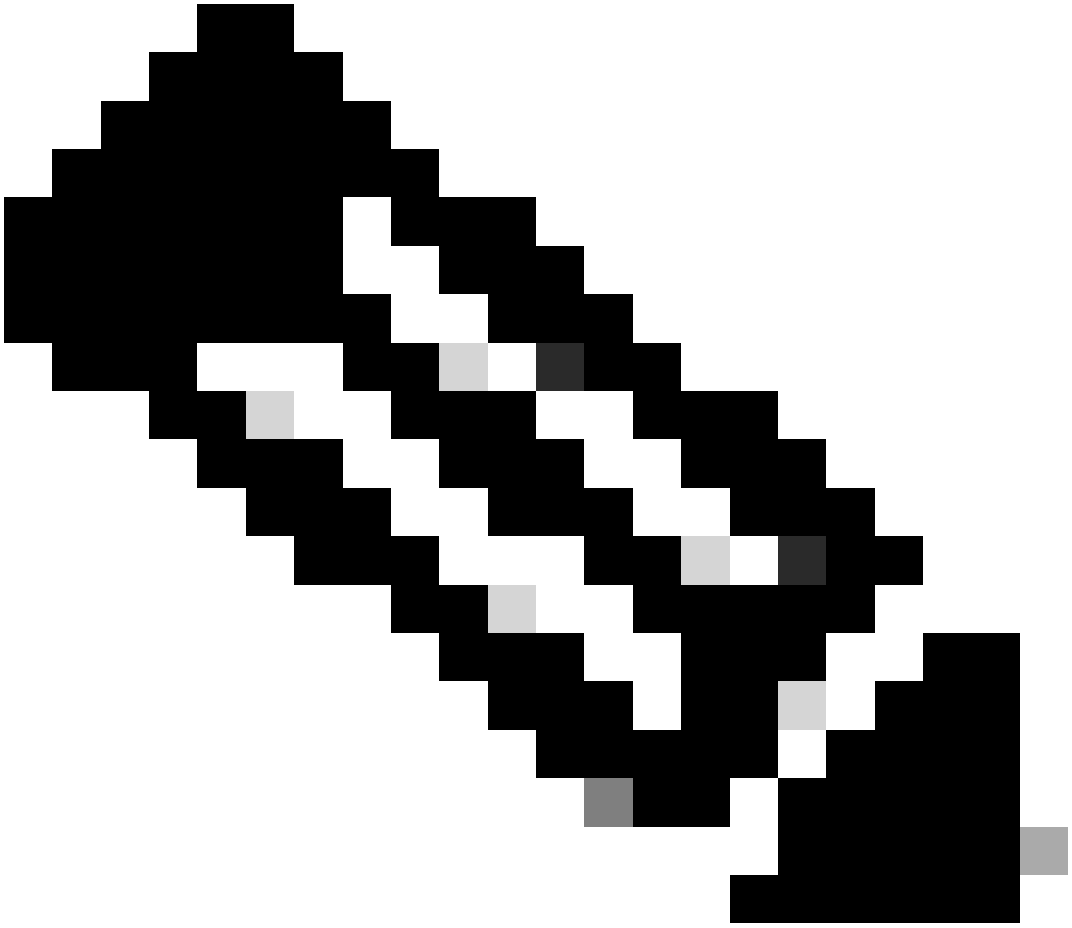


CFGMODE Exchange

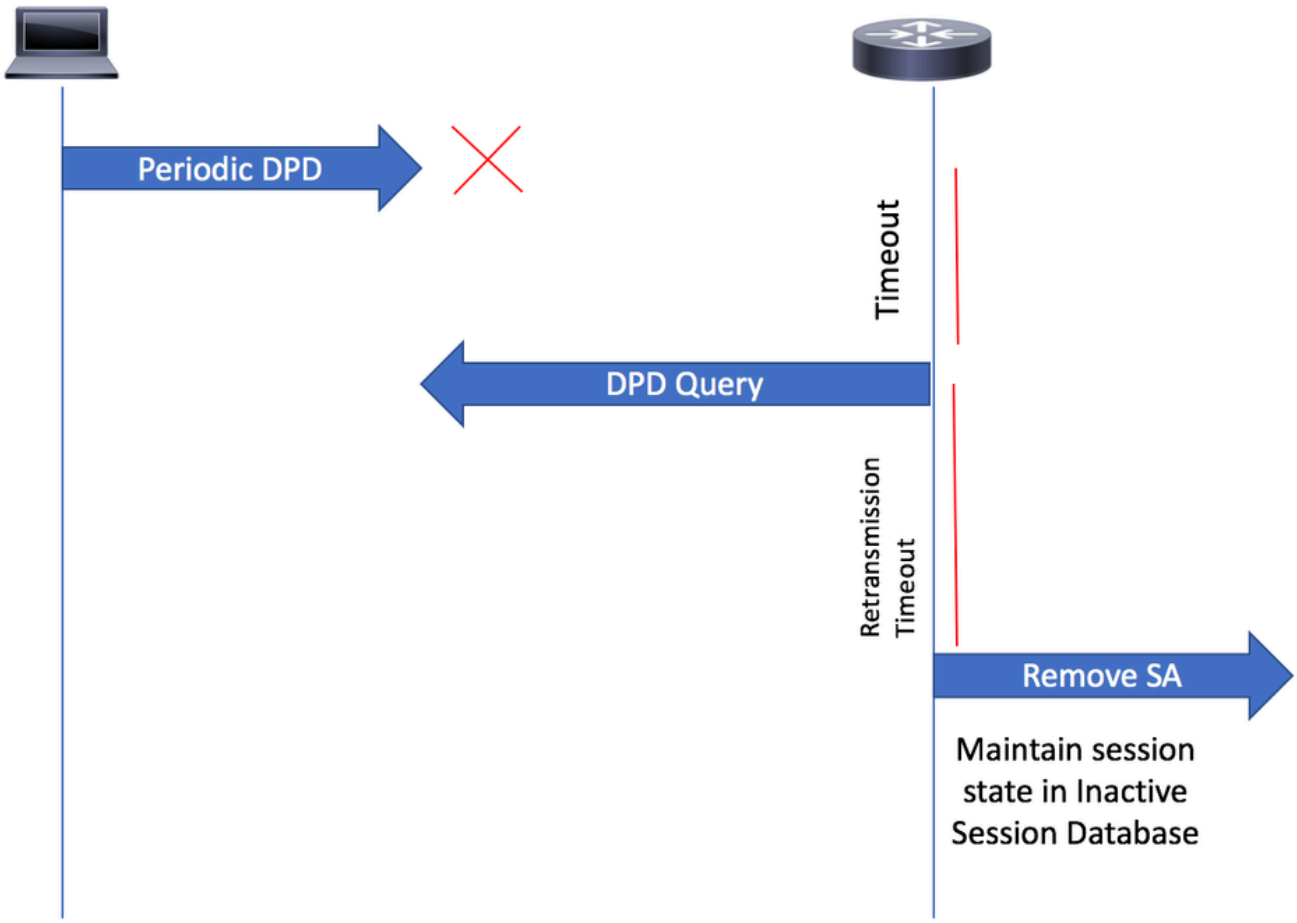


附註：識別無響應客戶端的過程基於失效對等體檢測(DPD)。 如果在IKEv2配置檔案中啟用了「重新連線」功能，則不需要配置DPD，因為DPD在IKEv2中按要求排隊

3.思科安全客戶端定期向網關傳送DPD消息。如果DPD以按需排隊方式排隊，網關不會將DPD消息傳送到客戶端，直到它收到來自客戶端的DPD。如果在指定的時間段內沒有從安全客戶端收到DPD（根據配置的DPD間隔），網關將傳送DPD消息。如果未收到來自安全客戶端的響應，則會從活動會話資料庫中刪除SA。



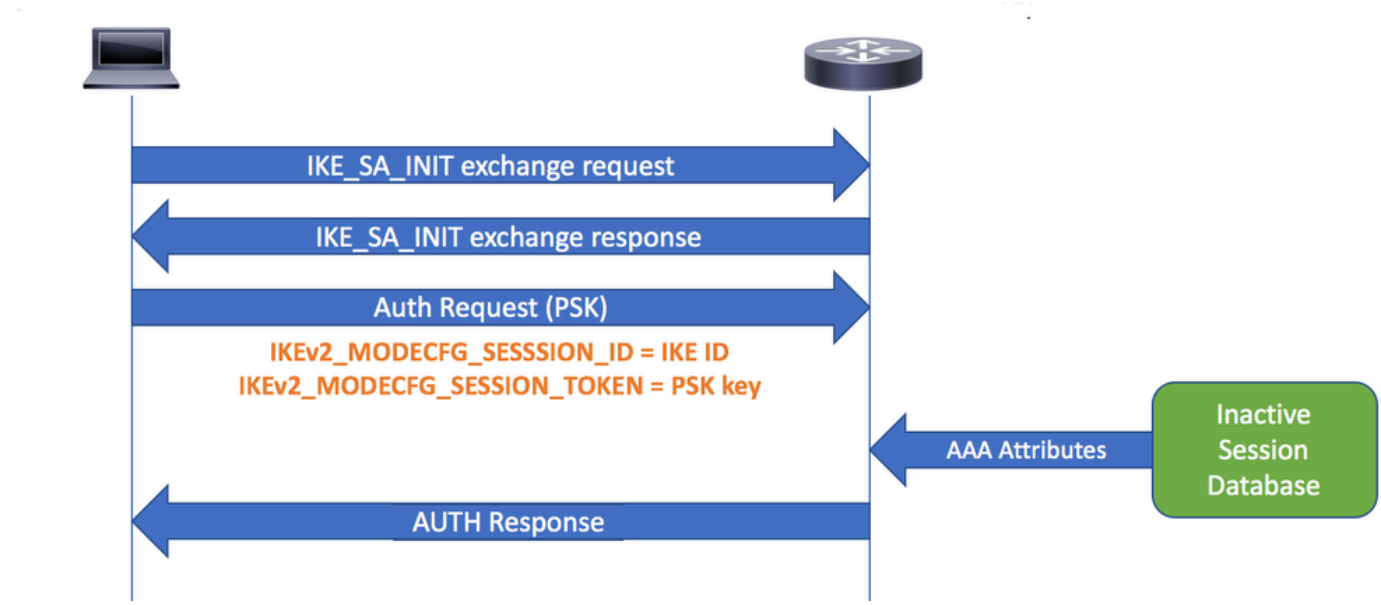
附註：網關仍會在單獨的非活動會話資料庫中維護會話狀態（如AAA屬性），以便根據配置的重新連線超時時間段允許重新連線。



DPD查詢

4.當客戶端嘗試重新連線時，它會建立一個新的IKE SA，並使用IKE標識(ID)作為會話ID，它從MODECFG_REPLY負載接收該會話ID。此時，思科安全客戶端使用IKE PSK身份驗證進行重新連線，預共用金鑰是之前收到的會話令牌。

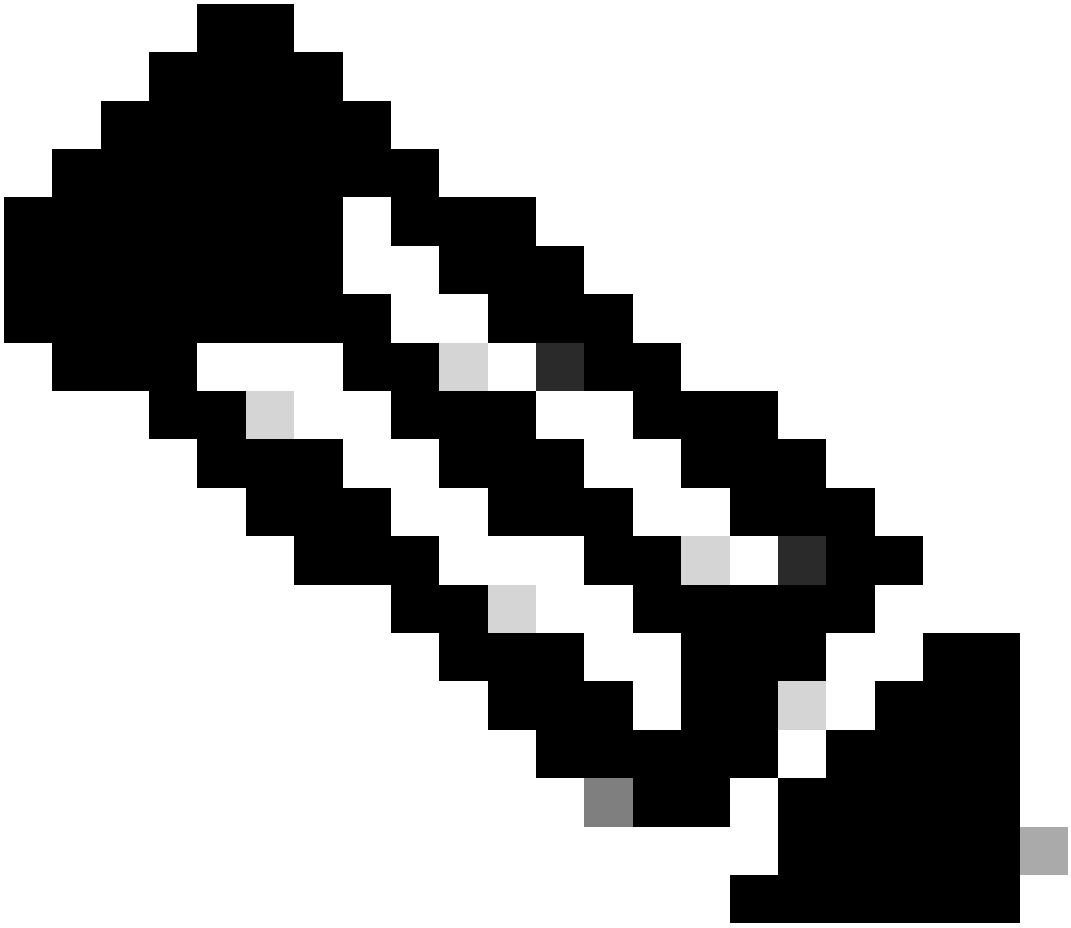
5.當網關收到重新連線請求時，它會在非活動會話資料庫中搜尋對等IKE ID（用作會話ID）。 在重新連線期間，將從非活動資料庫中檢索儲存的自定義屬性並將其應用到新的SA。



重新連線

設定

路由器配置



附註：對於路由器配置，您還可以參閱使用本地使用者資料庫為安全客戶端(AnyConnect)IKEv2遠端訪問配置FlexVPN頭端

此配置片段顯示了Cisco安全客戶端IKEv2遠端訪問配置的示例，以及如何通過在IKEv2配置檔案中配置reconnect來啟用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
```

思科安全使用者端設定檔

<#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重新連線的限制

1. 無法在Internet金鑰交換版本2(IKEv2)配置檔案中配置預共用金鑰授權方法。這是因為Cisco安全客戶端功能的Cisco IOS IKEv2自動重新連線功能支援使用預共用金鑰授權方法，並且在同一IKEv2配置檔案上配置預共用金鑰會導致混亂。
2. 無法在IKEv2配置檔案中配置以下命令：

- 身份驗證本地預共用
- 身份驗證遠端預共用
- keyring, aaa authorization group psk
- aaa authorization user psk

驗證

<#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
```

此輸出顯示，目前有1個可自動重新連線的作用中作業階段：

```
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
```

重新連線後

思科安全客戶端重新連線時，會使用IKEV2_MODECFG_SESSION_ID作為IKE ID。因此，重新連線後，Phase1_id不再是$AnyConnectClient$;而是會話ID，如圖所示。此外，請注意，功能現在已設定了R。此處，R表示這是重新連線會話。

<#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
```

重新連線後，驗證方法現在為PSK（預共用金鑰）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#
```

Cisco Secure Client DART日誌

<#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

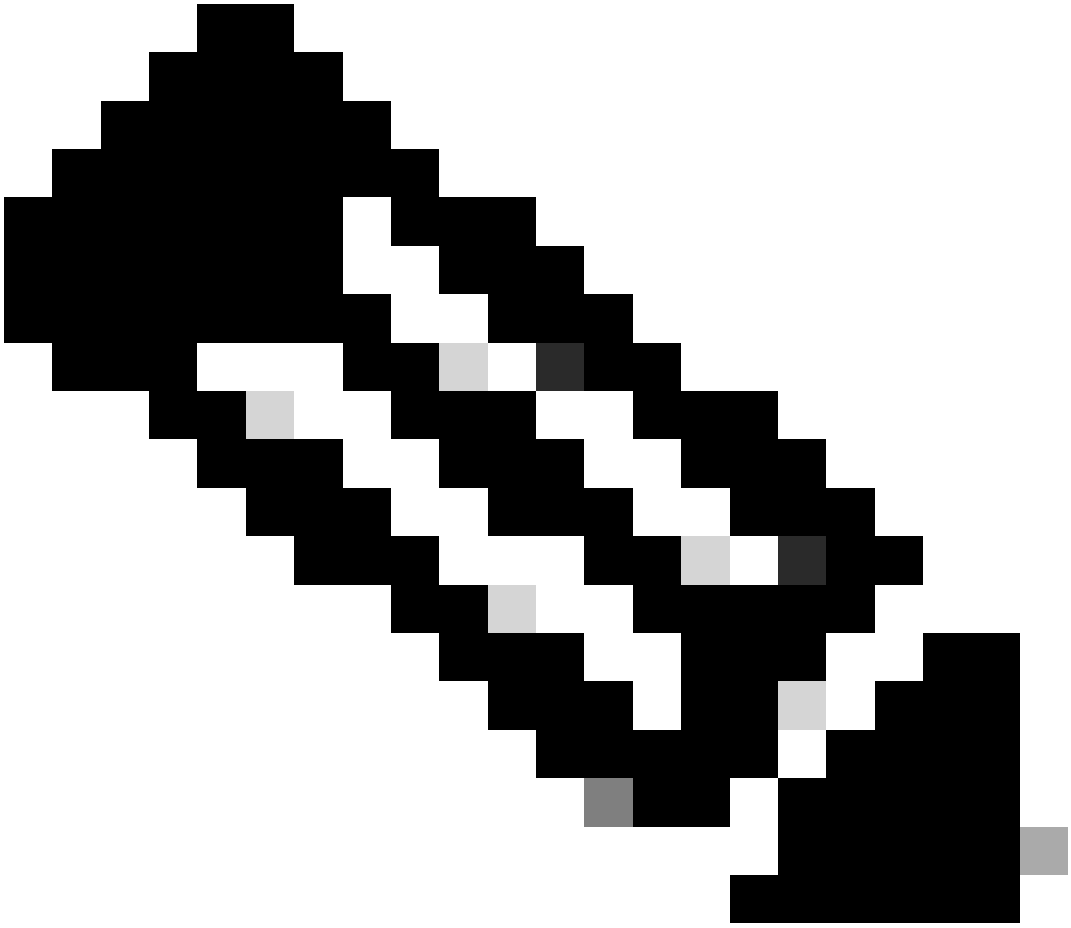
Description : Function: CIPsecProtocol::initiateTunnel
File: IPsecProtocol.cpp
Line: 613

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.



附註：在DART日誌中，IKE ID顯示為「rIUHKccDRiUtFTATwq」，這是「724955484B6363445269557446544154771」的ASCII表示形式，在「show crypto session detail」的輸出中顯示為遠端ID。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

IKEv2調試，驗證網關和客戶端之間的協商。

```
Debug crypto condition peer ipv4
```

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

```
Debug crypto ikev2 error
```

相關資訊

- 安全和VPN配置指南，Cisco IOS XE 17.x
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。