Informazioni sulla funzione di riconnessione di IKEv2 e AnyConnect

Sommario

Introduzione

In questo documento viene descritto il funzionamento della funzione di riconnessione automatica IKEv2 sui router Cisco IOS® e Cisco IOS® XE per AnyConnect.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Catalyst 8000V (C800V) con versione 17.16.01a
- Cisco Secure Client versione 5.1.8.105
- PC client con Cisco Secure Client installato

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Funzione di riconnessione client sicura IKEv2 e Cisco

La funzione di riconnessione automatica di Cisco Secure Client consente di memorizzare la sessione per un determinato periodo di tempo e di riprendere la connessione dopo aver stabilito il canale sicuro. Poiché Cisco Secure Client è ampiamente utilizzato con Internet Key Exchange versione 2 (IKEv2), IKEv2 estende il supporto della funzione di riconnessione automatica sul software Cisco IOS tramite il supporto Cisco IKEv2 per la funzione di riconnessione automatica di Secure Client.

La riconnessione automatica in Cisco Secure Client si verifica nei seguenti scenari:

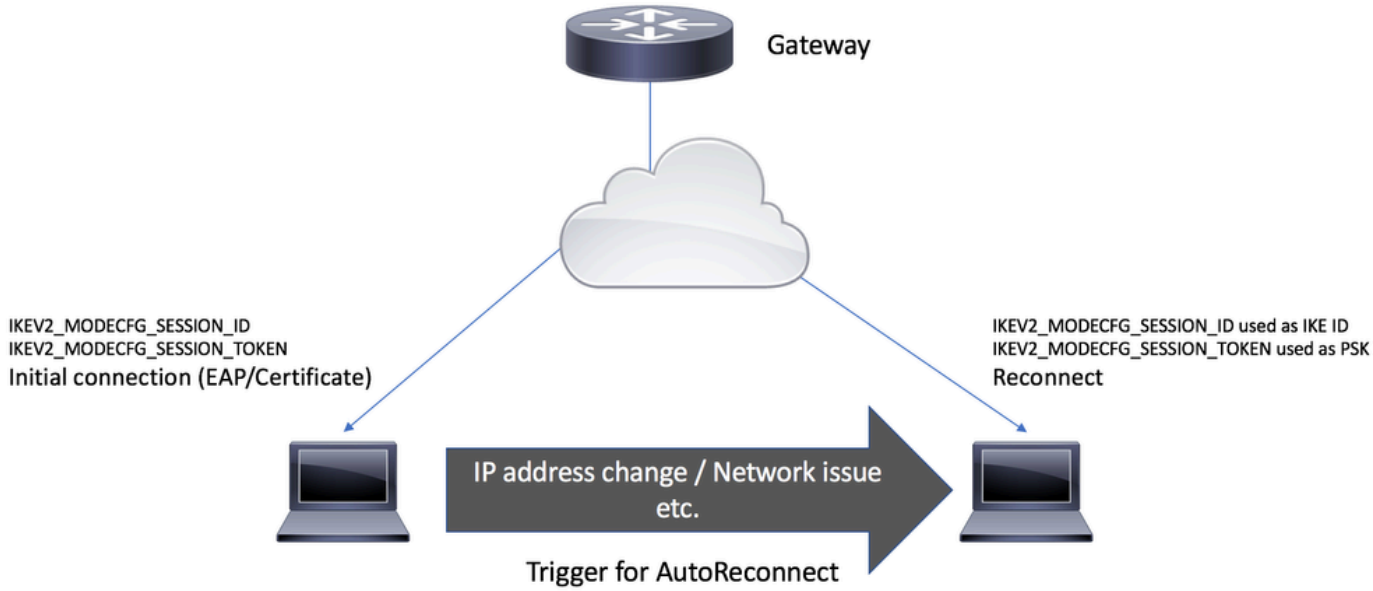
1. La rete intermedia è inattiva. Cisco Secure Client tenta di riprendere la sessione quando è attiva.
2. Il dispositivo Cisco Secure Client passa da una rete all'altra. Il risultato è una modifica della porta di origine che riduce l'associazione di sicurezza (SA) esistente e, di conseguenza, Cisco Secure Client tenta di ripristinare l'associazione di sicurezza utilizzando la funzione di riconnessione automatica.
3. Il dispositivo Cisco Secure Client tenta di riprendere l'associazione di sicurezza dopo essere tornato dalla modalità di sospensione o ibernazione.

Vantaggi della funzione di riconnessione automatica

- Gli attributi di configurazione utilizzati nella sessione originale vengono riutilizzati senza eseguire query sul server di autenticazione, autorizzazione e accounting (AAA).
- Il gateway IKEv2 non deve contattare il server RADIUS per riconnettersi al client.
- Durante la ripresa della sessione non è necessaria alcuna interazione dell'utente per l'autenticazione o l'autorizzazione.
- Il metodo di autenticazione è la chiave già condivisa quando si riconnette una sessione. Questo metodo di autenticazione è rapido rispetto ad altri metodi di autenticazione.
- Il metodo di autenticazione con chiave già condivisa consente di riprendere una sessione sul software Cisco IOS con risorse minime.

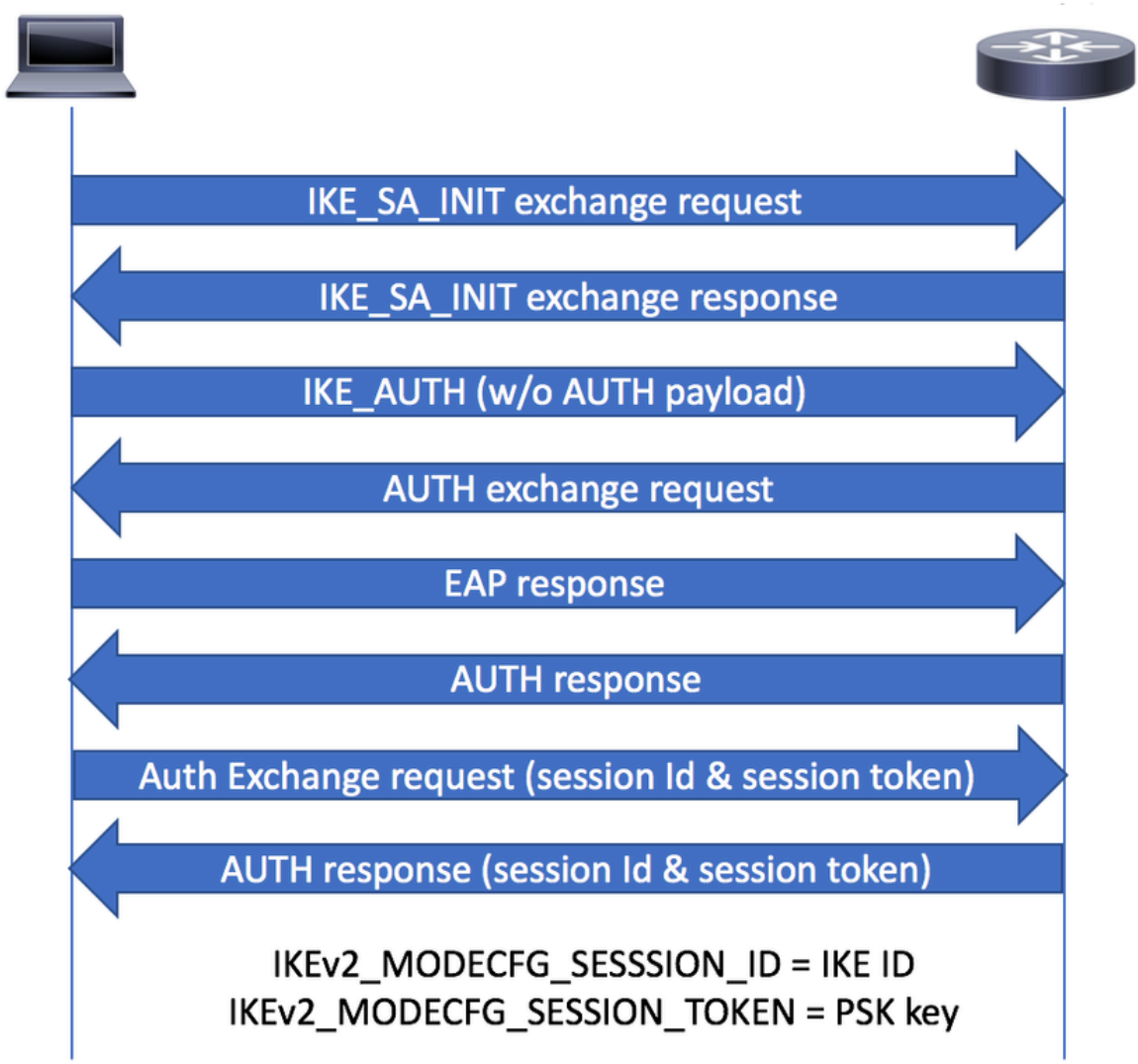
- Le associazioni di sicurezza (SA) inutilizzate vengono rimosse, liberando così le risorse di crittografia.

Flusso di connessione riconnessione automatica

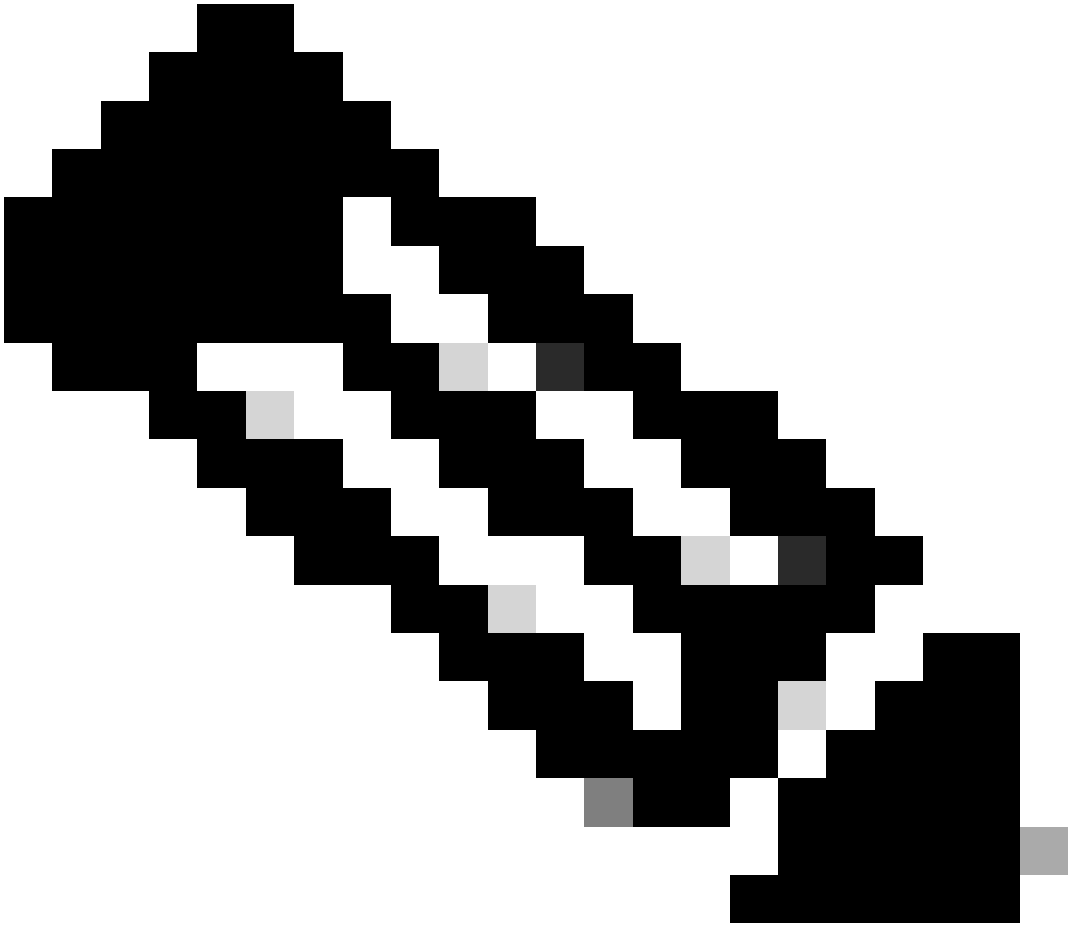


Trigger per riconnessione automatica

1. Durante lo scambio AUTH, Cisco Secure Client richiede gli attributi Session-token e Session-id dal gateway IKEv2 nel payload MODECFG_REQ della richiesta IKE_AUTH.
2. Il gateway IKEv2 controlla se il supporto IKEv2 di Cisco IOS per la funzione di riconnessione automatica della funzione Secure Client è abilitato nel profilo IKEv2 usando il comando reconnect, seleziona il criterio IKEv2 del profilo IKEv2 scelto e invia l'ID sessione e gli attributi del token di sessione al client sicuro nel payload CFGMODE_REPLY della risposta IKE_AUTH.

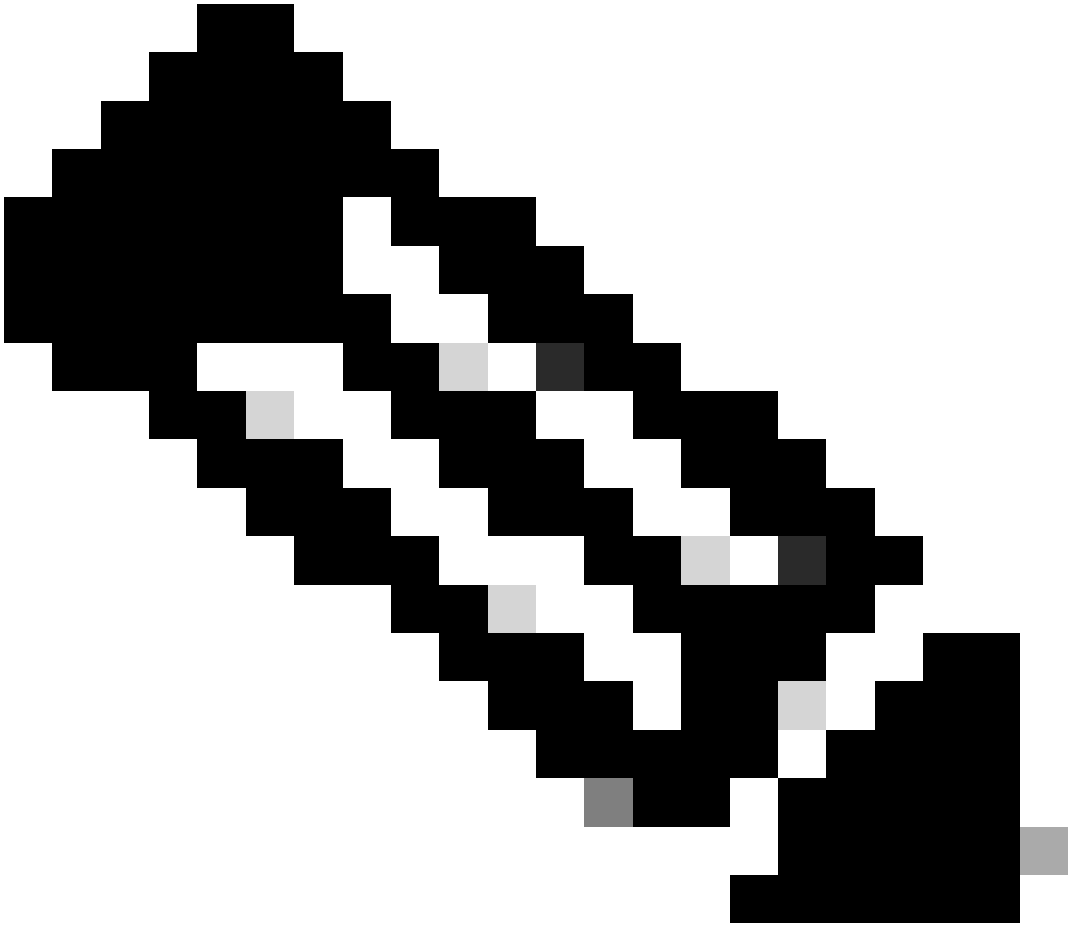


CFGMODE Exchange

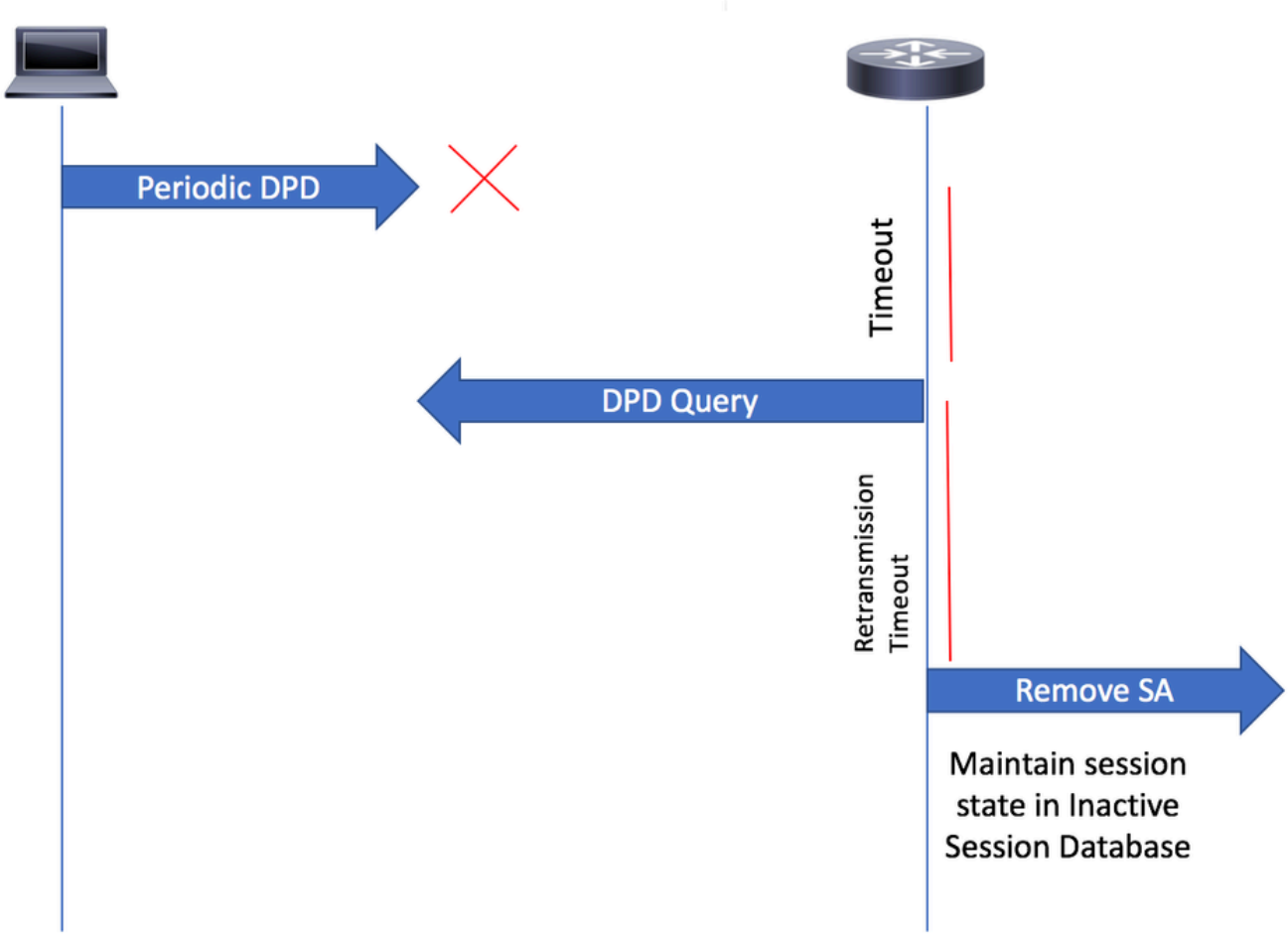


Nota: Il processo di identificazione del client che non risponde si basa sul DPD (Dead Peer Detection). Se la funzione di riconnessione è abilitata nel profilo IKEv2, non è necessario configurare DPD, in quanto DPD viene accodato come su richiesta in IKEv2

3. Cisco Secure Client invia periodicamente messaggi DPD al gateway. Se DPD viene accodato come su richiesta, il gateway non invia messaggi DPD al client finché non riceve DPD dal client. Se il DPD non viene ricevuto dal client protetto entro il periodo di tempo specificato (in base all'intervallo DPD configurato), il gateway invia un messaggio DPD. Se non si riceve alcuna risposta dal client protetto, l'associazione di protezione viene eliminata dal database della sessione attiva.



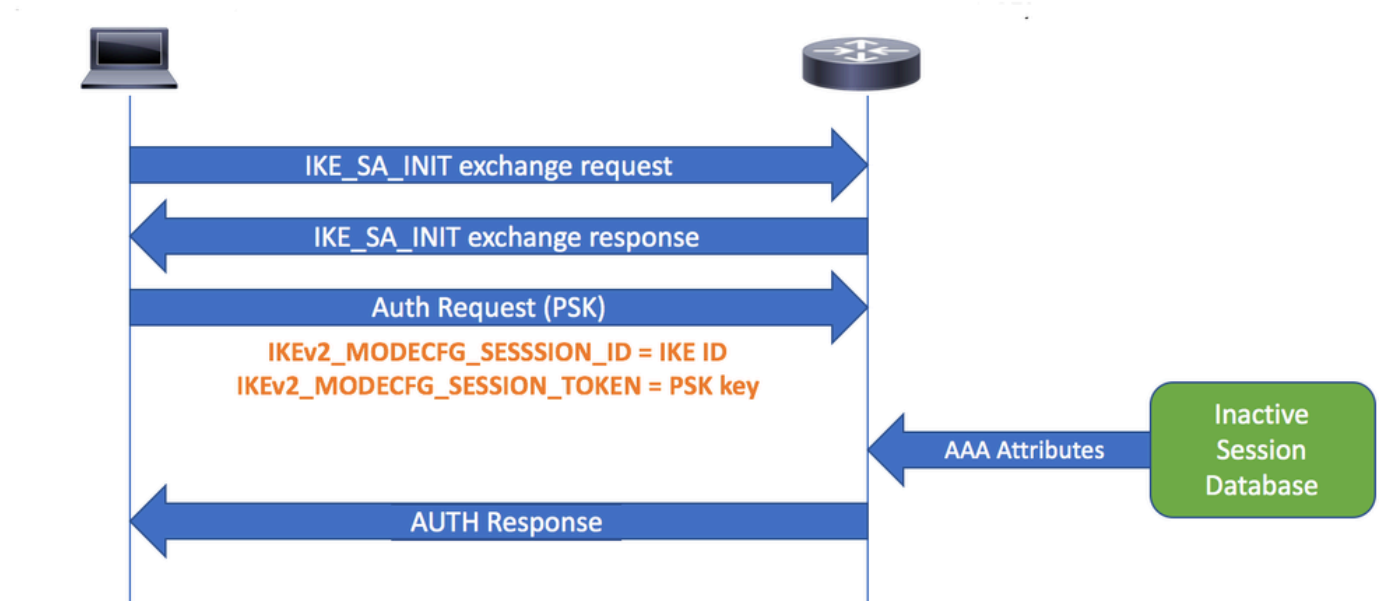
Nota: Il gateway mantiene ancora lo stato della sessione (ad esempio gli attributi AAA) in un database di sessione inattivo separato per consentire la riconnessione in base al periodo di timeout configurato per la riconnessione.



Query DPD

4. Quando il client tenta di riconnettersi, crea una nuova associazione di protezione IKE e utilizza l'identità IKE (ID) come ID sessione, ricevuta dal payload MODECFG_REPLY. A questo punto, Cisco Secure Client utilizza l'autenticazione PSK IKE per la riconnessione, con la chiave precondivisa che è il token di sessione ricevuto in precedenza.

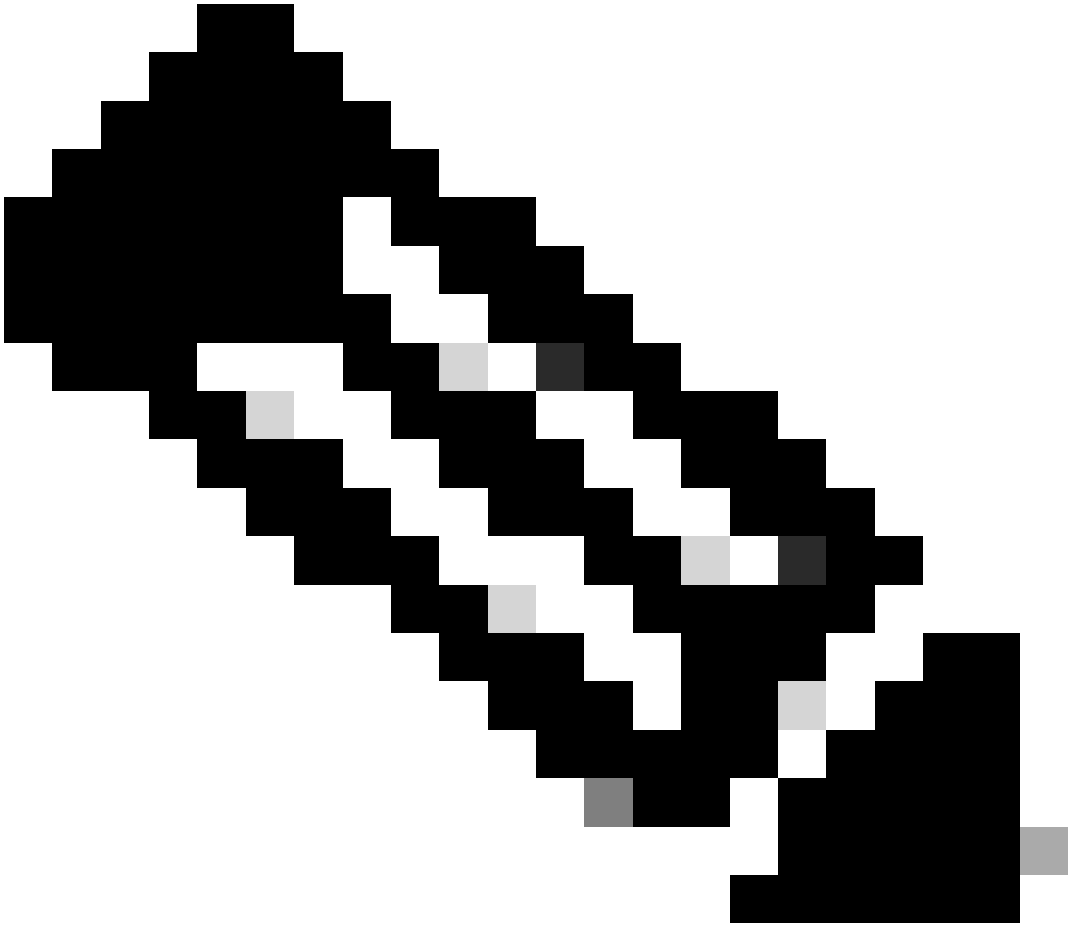
5. Quando il gateway riceve una richiesta di riconnessione, cerca nel database delle sessioni inattive l'ID IKE peer (che funge da ID sessione). Durante la riconnessione, gli attributi personalizzati memorizzati del database inattivo vengono recuperati e applicati alla nuova associazione di protezione.



Riconnetti

Configurazione

Configurazione del router



Nota: Per la configurazione del router, è possibile consultare il documento sulla [configurazione dell'headend FlexVPN per l'accesso remoto Secure Client (AnyConnect) IKEv2 con il database degli utenti locali]

Questo frammento di configurazione mostra un esempio di configurazione di Accesso remoto IKEv2 di Cisco Secure Client e come viene abilitata la riconnessione automatica configurando la riconnessione nel profilo IKEv2.

<#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>
```

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>
```

Restrizioni per la configurazione della riconnessione IKEv2

1. Impossibile configurare il metodo di autorizzazione della chiave già condivisa nel profilo IKEv2 (Internet Key Exchange versione 2). Infatti, il supporto di Cisco IOS IKEv2 per la funzione di riconnessione automatica di Cisco Secure Client utilizza il metodo di autorizzazione della chiave già condivisa e la configurazione della chiave già condivisa sullo stesso profilo IKEv2 può causare confusione.
2. Impossibile configurare questi comandi nel profilo IKEv2:

- pre-condivisione locale di autenticazione
- pre-condivisione remota per l'autenticazione
- keyring, gruppo di autorizzazioni aaa psk
- psk utente autorizzazione aaa

Verifica

<#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
```

Questo output mostra che al momento è presente una sessione attiva in grado di riconnettersi automaticamente:

```
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
```

Dopo riconnessione

Quando Cisco Secure Client si riconnette, utilizza IKEV2_MODECFG_SESSION_ID come ID IKE. Pertanto, dopo la riconnessione, Phase1_id non è più $AnyConnectClient$; è invece l'ID della sessione, come illustrato. Si noti inoltre che le funzionalità sono ora impostate in R. In questo caso, R indica che si tratta di una sessione di riconnessione.

<#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
```

Dopo la riconnessione, il metodo di autenticazione è ora PSK (chiave precondivisa) anziché AnyConnect-EAP, come mostrato:

<#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#

Registri DART Cisco Secure Client

<#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

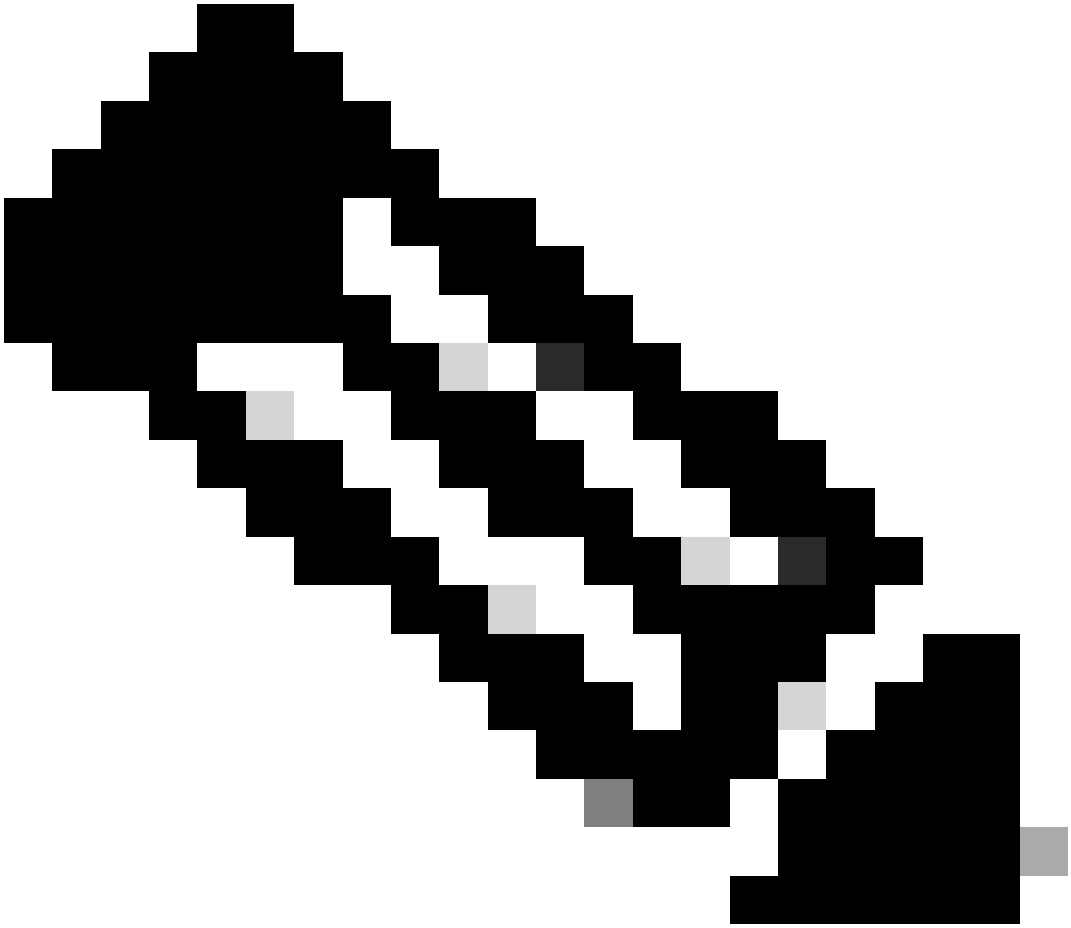
Using IKE ID 'rIUHKccDRiUtFTATwq' for reconnect

.
.
Date   : 03/13/2025
Time   : 03:11:44

```
Type        : Information
Source      : acvpnui

Description : Message type information sent to the user:

Connected to IKEv2_Gateway.
```



> Nota: Nei registri DART, l'ID IKE è indicato come 'IUHKccDRiUtFTATwq', ovvero la rappresentazione ASCII di '724955484B6363445269557446544154771', visualizzata come ID remoto nell'output di "show crypto session detail".

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Esegue il debug di IKEv2 per verificare la negoziazione tra il gateway e il client.

```
Debug crypto condition peer ipv4
```

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

Informazioni correlate

- Guida alla sicurezza e alla configurazione VPN, Cisco IOS XE 17.x
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).