De functies IKEv2 en AnyConnect opnieuw verbinden begrijpen

Inhoud

Inleiding

Dit document beschrijft hoe de functie IKEv2 Auto Reconconnect werkt op Cisco IOS® en Cisco IOS® XE-routers voor AnyConnect.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Internet Key Exchange, versie 2 (IKEv2)
- Cisco Secure-client (CSC)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst 8000V (C800V) actieve versie 17.16.01a
- Cisco Secure-clientversie 5.1.8.105
- Clientpc met geïnstalleerde Cisco Secure-client

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

IKEv2- en Cisco Secure Client Reconconnect-functie

De functie Automatisch opnieuw verbinden in de beveiligde client van Cisco helpt u de sessie voor een bepaalde tijd te onthouden en de verbinding te hervatten na het instellen van het beveiligde kanaal. Aangezien de Cisco Secure Client uitgebreid wordt gebruikt met Internet Key Exchange versie 2 (IKEv2), breidt IKEv2 de ondersteuning van de Auto Reconconnect-functie uit op Cisco IOS-software via de ondersteuning van Cisco IOS IKEv2 voor Auto Reconconnect-functie van Secure Client.

Automatisch opnieuw verbinden in de beveiligde Cisco-client vindt in de volgende scenario's plaats:

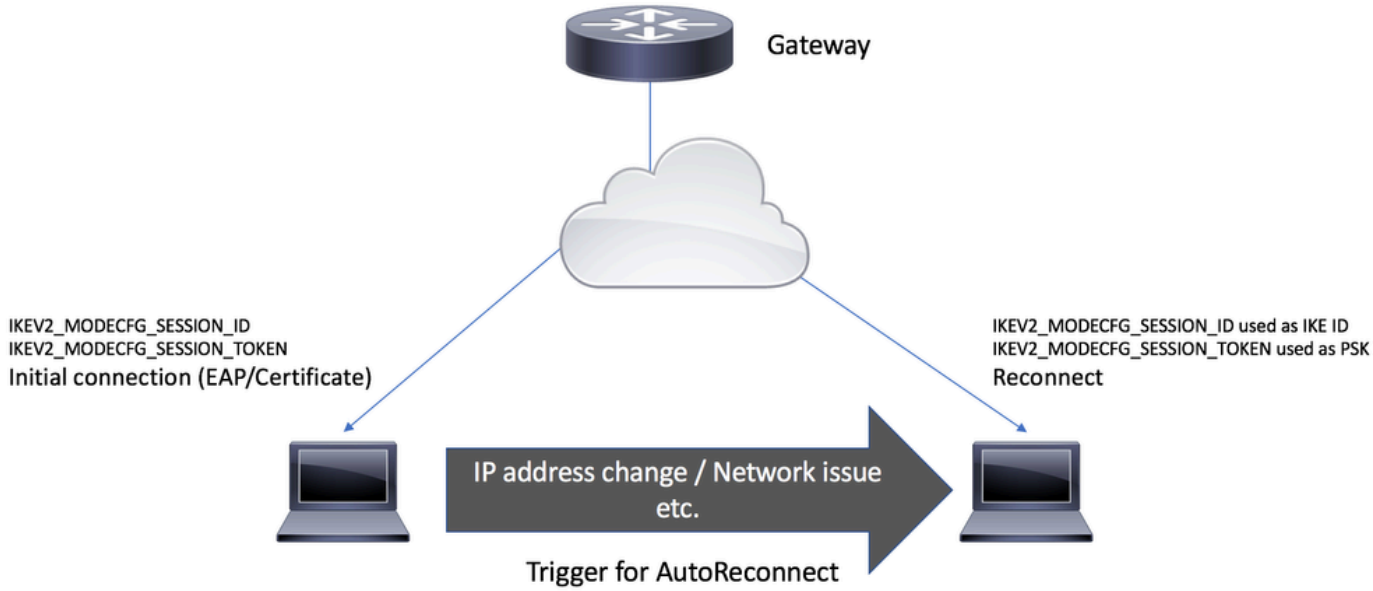
1. Het intermediaire netwerk is down. De Cisco Secure-client probeert de sessie te hervatten wanneer deze is gestart.
2. De Cisco Secure Client-apparaat switch tussen netwerken. Dit resulteert in een wijziging van de bronpoort, waardoor de bestaande beveiligingsassociatie (SA) wordt uitgeschakeld en de Cisco Secure-client probeert de SA te hervatten met de functie Auto Reconconnect.
3. Het Cisco Secure-clientapparaat probeert de overschakeling op de slaapstand of de slaapstand te hervatten nadat het is teruggekeerd.

Voordelen van de functie Automatisch opnieuw verbinden

- De configuratiekenmerken die in de oorspronkelijke sessie zijn gebruikt, worden opnieuw gebruikt zonder de verificatie-, autorisatie- en accounting (AAA) server op te vragen.
- De IKEv2-gateway hoeft niet contact op te nemen met de RADIUS-server om opnieuw verbinding te maken met de client.
- Er is geen gebruikersinteractie voor verificatie of autorisatie nodig tijdens het hervatten van de sessie.
- De verificatiemethode is de vooraf gedeelde sleutel bij het opnieuw verbinden van een sessie. Deze verificatiemethode is snel in vergelijking met andere verificatiemethoden.
- De methode voor vooraf gedeelde sleutelverificatie helpt bij het hervatten van een sessie over de Cisco IOS-software met minimale bronnen.

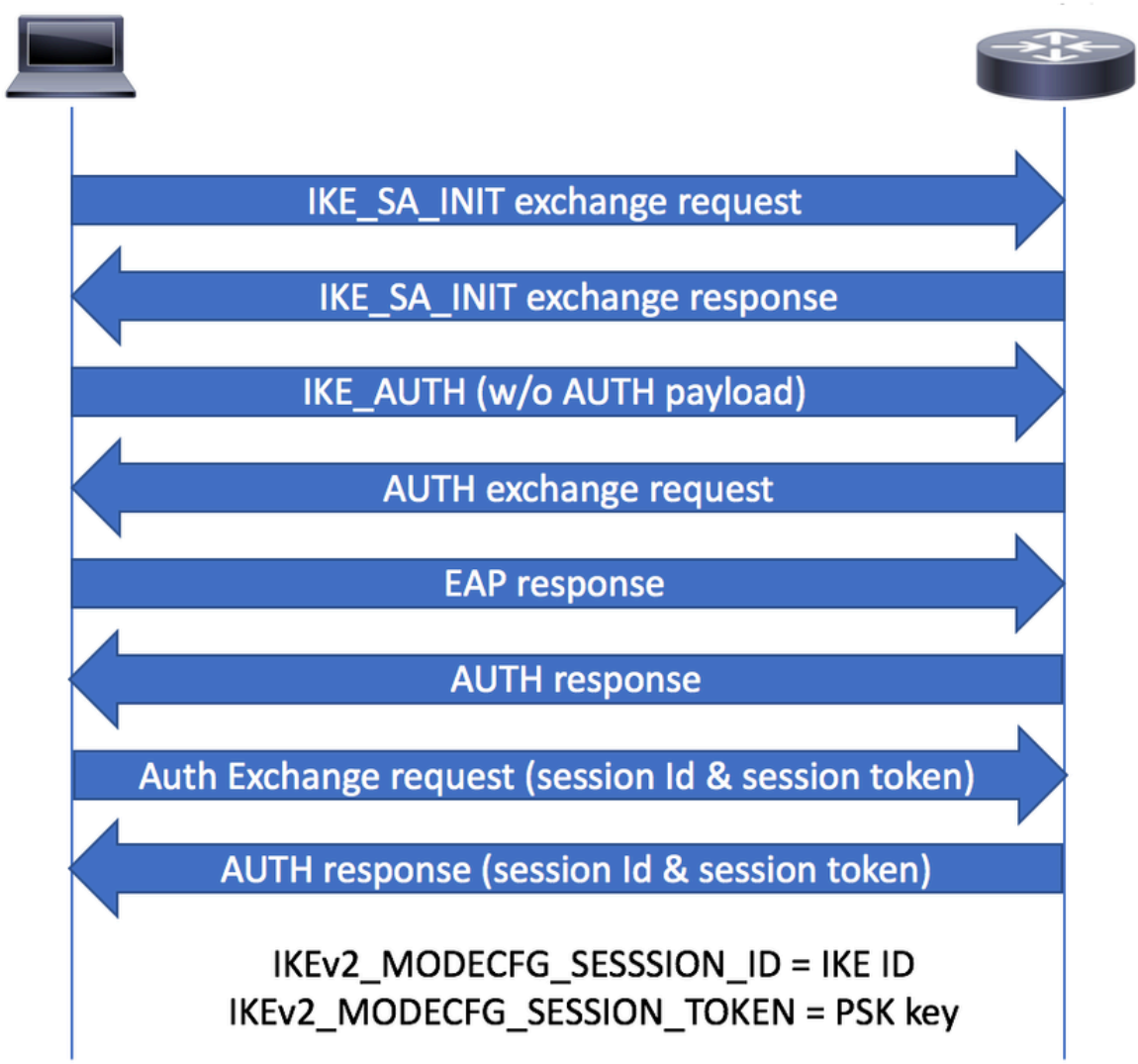
- De ongebruikte beveiligingsassociaties (SA's) worden verwijderd, waardoor de crypto-middelen worden vrijgemaakt.

Automatisch opnieuw verbinden, verbindingsstroom

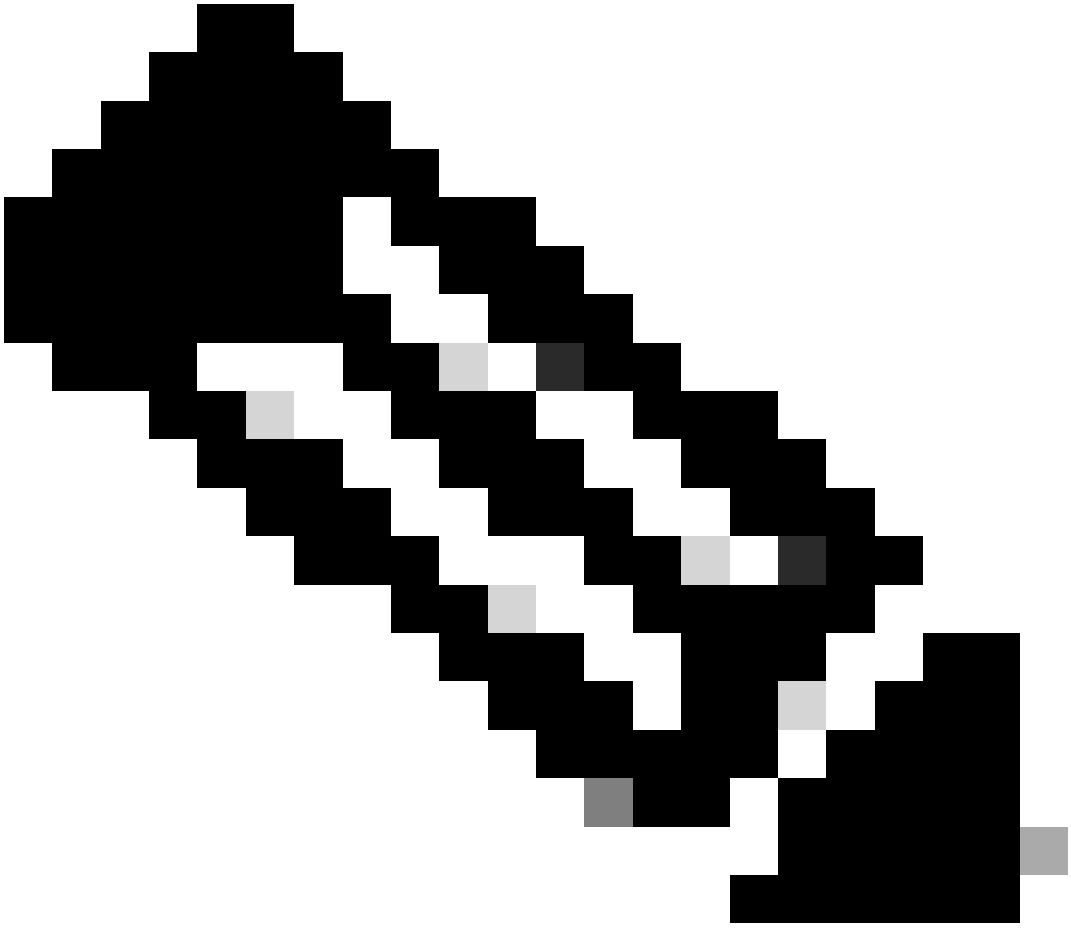


Trigger voor automatisch opnieuw verbinden

1. Tijdens de AUTH-uitwisseling vraagt Cisco Secure Client om het Session-token en Session-id attribuut van IKEv2 Gateway in MODECFG_REQ payload van IKE_AUTH Verzoek.
2. IKEv2-gateway controleert of de Cisco IOS IKEv2-ondersteuning voor de functie Auto Reconconnect van Secure Client in het IKEv2-profiel is ingeschakeld met de opdracht Reconnect, selecteert het IKEv2-beleid van het gekozen IKEv2-profiel en verstuurt de sessieid en de sessietekenkenmerken naar de beveiligde client in CFGMODE_REPLIL-payload van de IKE_AUTH-respons.



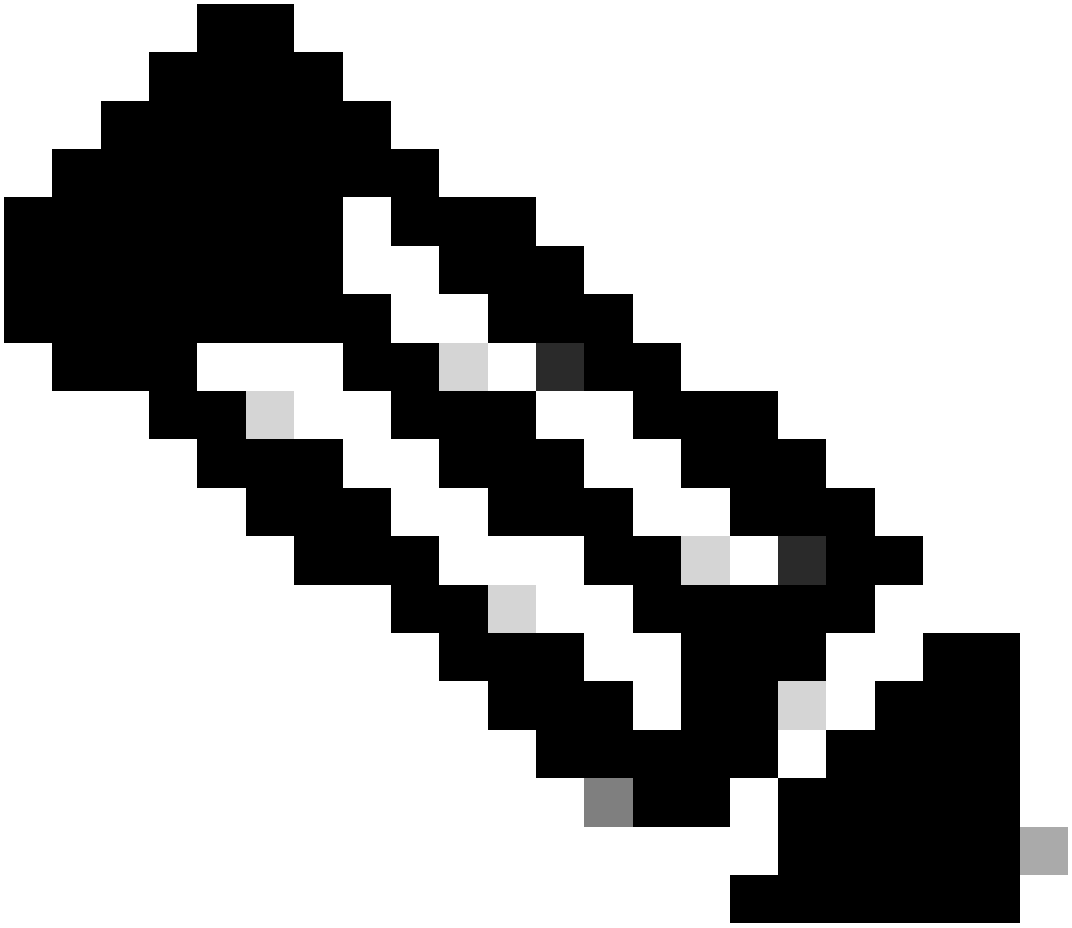
CFGodus exchange



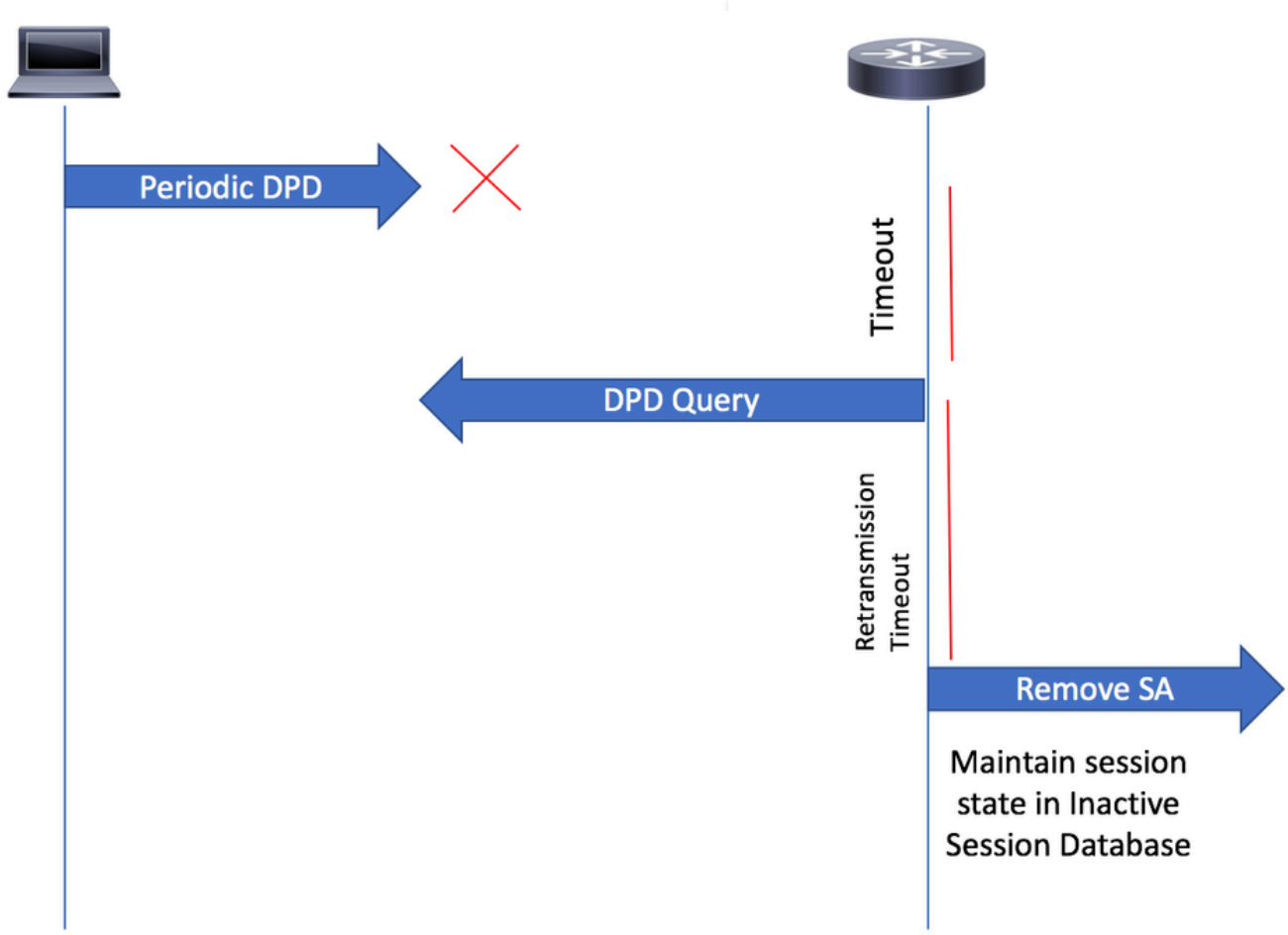
Opmerking: Het proces van het identificeren van niet-reagerende cliënt is gebaseerd op Dead Peer Detection (DPD). Als de functie voor opnieuw verbinden in het IKEv2-profiel is ingeschakeld, hoeft u DPD niet te configureren, aangezien DPD in IKEv2 als wachtrij wordt geplaatst op verzoek

---

3. De beveiligde Cisco-client verzendt periodiek DPD-berichten naar de gateway. Als DPD als on-demand wordt geplaatst, verstuurt de gateway geen DPD-berichten naar de client totdat hij DPD van de client ontvangt. Als DPD niet wordt ontvangen van Secure Client binnen de opgegeven tijdsperiode (zoals per geconfigureerd DPD-interval), verstuurt de gateway een DPD-bericht. Als er geen reactie wordt ontvangen van de beveiligde client, wordt de SA verwijderd uit de actieve sessiedatabank.



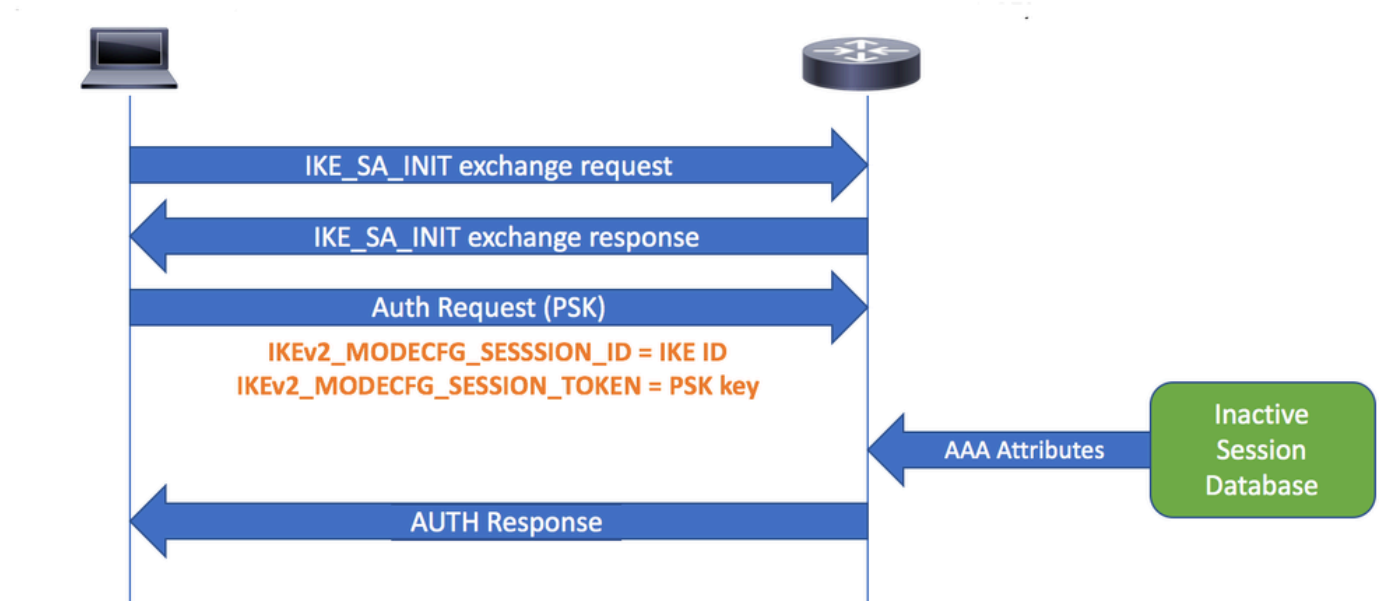
Opmerking: De gateway handhaaft nog de sessiestatus (zoals AAA-kenmerken) in een afzonderlijke inactieve sessiedatabank om de herverbinding mogelijk te maken zoals per geconfigureerde time-outperiode voor opnieuw verbinden.



DPD-query

4. Wanneer de client probeert opnieuw verbinding te maken, maakt hij een nieuwe IKE SA en gebruikt hij de IKE-identiteit (ID) als sessie-ID, die hij heeft ontvangen van de lading MODECFG_RERESPONSE. Op dit punt maakt Cisco Secure Client gebruik van IKE PSK-verificatie voor het opnieuw verbinden, waarbij de vooraf gedeelde sleutel het eerder ontvangen sessieteken is.

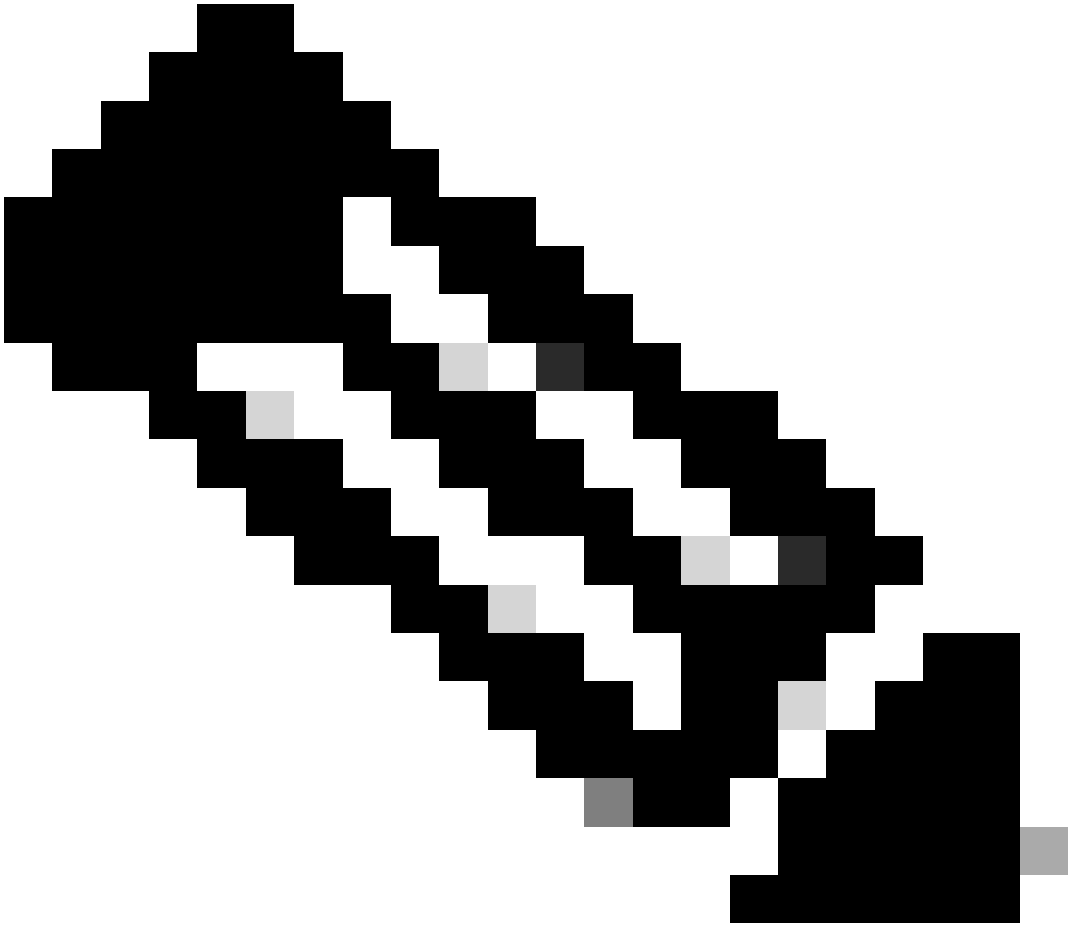
5. Wanneer de gateway een verzoek om opnieuw verbinding ontvangt, zoekt hij de Inactieve Sessiedatabank naar de peer IKE-id (die als sessie-ID fungeert). Tijdens het opnieuw verbinden worden de opgeslagen douaneattributen van de Inactieve Database opgehaald en toegepast op de nieuwe SA.



opnieuw verbinden

Configureren

Routerconfiguratie



Opmerking: Voor routerconfiguratie kunt u ook het document Configure FlexVPN Head-end voor Secure Client (AnyConnect) IKEv2 Remote Access gebruiken met lokale gebruikersdatabase

Dit configuratiefragment laat een voorbeeld zien van Cisco Secure Client IKEv2 Remote Access-configuratie en hoe AutoReconconnect is ingeschakeld door opnieuw verbinding te maken onder het IKEv2-profiel te configureren.

<#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-clientprofiel

<#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>
```

Beperkingen voor het configureren van IKEv2 opnieuw verbinden

1. De methode voor het vooraf delen van een sleutel kan niet worden geconfigureerd op het Internet Key Exchange Versie 2 (IKEv2)-profiel. Dit komt doordat de functie Cisco IOS IKEv2 voor AutoReconconnect van de Secure Client-functie van Cisco de sleutelautorisatiemethode (preshared) gebruikt en omdat het configureren van de vooraf gedeelde sleutel op hetzelfde IKEv2-profiel tot verwarring kan leiden.
2. Deze opdrachten kunnen niet op het IKEv2-profiel worden geconfigureerd:

- lokale pre-share verificatie
- verificatie vooraf delen op afstand
- sleutelring, aaa autorisatiegroep psk
- aaa autorisatiegebruiker psk

Verifiëren

<#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
```

Deze uitvoer toont aan dat er momenteel 1 actieve sessie is die automatisch opnieuw verbinding kan maken:

```
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
```

Na opnieuw verbinden

Wanneer de beveiligde client van Cisco opnieuw wordt verbonden, gebruikt deze de IKEV2_MODECFG_SESSION_ID als IKE-id. Daarom na het opnieuw verbinden is Phase1_id niet meer $AnyConnectClient$; in plaats daarvan, is het de sessie-ID, zoals getoond. Let er bovendien op dat de mogelijkheden nu R hebben ingesteld. Hier geeft R aan dat dit een herverbindingssessie is.

<#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
```

Na het opnieuw verbinden is de verificatiemethode nu PSK (vooraf gedeelde sleutel) in plaats van AnyConnect-EAP, zoals aangegeven op de afbeelding:

<#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-logbestanden

<#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

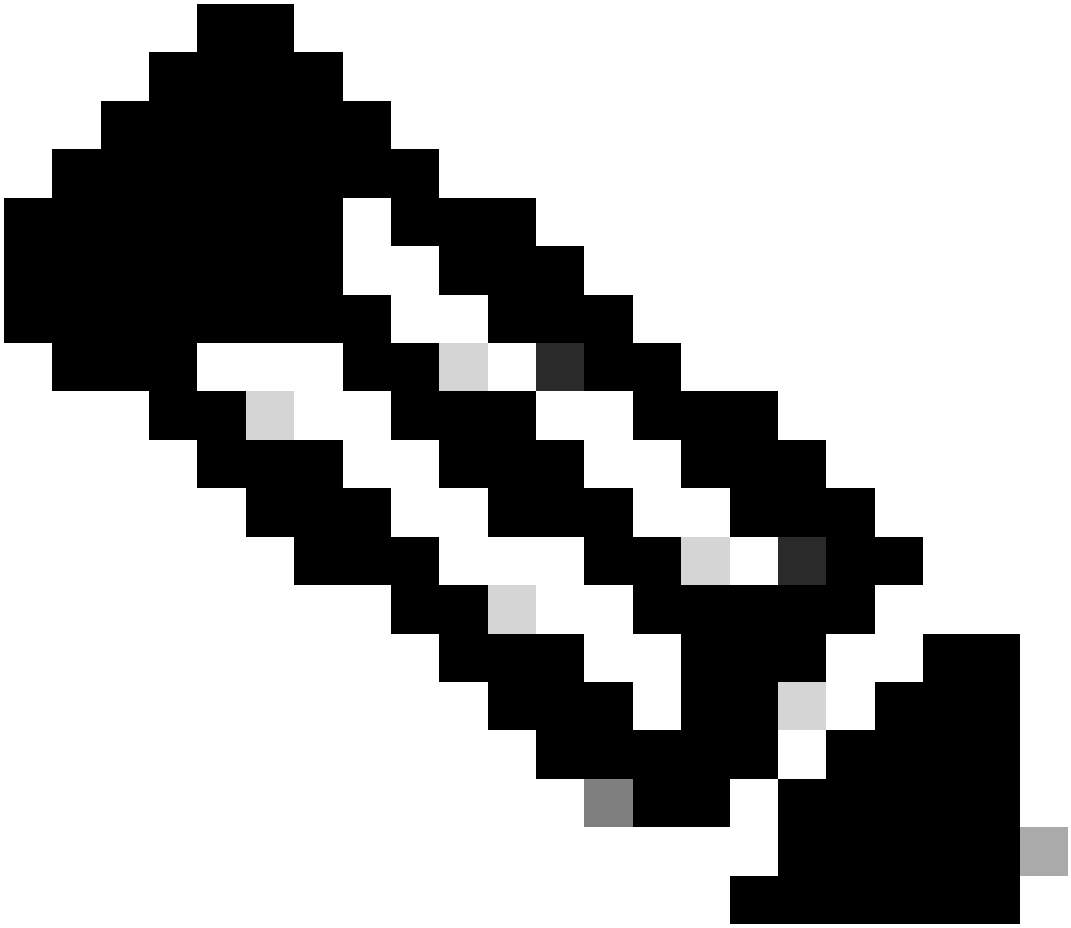
Using IKE ID 'rIUHKccDRiUtFTATwq' for reconnect

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

```
Type        : Information
Source      : acvpnui

Description : Message type information sent to the user:

Connected to IKEv2_Gateway.
```



> Opmerking: In DART-logbestanden wordt IKE-ID weergegeven als 'IUHKccDRiUtFTATwq' wat de ASCII-weergave is van '724955484B6363445269557446544154771', weergegeven als Remote ID in de uitvoer van "toon crypto sessiedetail".

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

IKEv2 debugt om de onderhandeling tussen de gateway en de client te verifiëren.

```
Debug crypto condition peer ipv4
```

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

Gerelateerde informatie

- Beveiligings- en VPN-configuratiehandleiding, Cisco IOS XE 17.x
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.