# IKEv2 und die AnyConnect-Verbindungsfunktion verstehen

## Inhalt



## Einleitung

In diesem Dokument wird die Funktionsweise der IKEv2 Auto Reconnect-Funktion auf Cisco IOS®- und Cisco IOS® XE-Routern für AnyConnect beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst 8000V (C8000V) mit Version 17.16.01a
- Cisco Secure Client Version 5.1.8.105
- Client-PC mit installiertem Cisco Secure Client

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## IKEv2 und Cisco Secure Client Reconnect-Funktion

Mit der Funktion zur automatischen Wiederverbindung im Cisco Secure Client kann der Benutzer sich die Sitzung für einen bestimmten Zeitraum merken und die Verbindung nach Einrichtung des sicheren Kanals fortsetzen. Da der Cisco Secure Client häufig mit Internet Key Exchange Version 2 (IKEv2) verwendet wird, erweitert IKEv2 die Unterstützung der Auto Reconnect-Funktion der Cisco IOS-Software durch die Cisco IOS IKEv2-Unterstützung der Auto Reconnect-Funktion der Secure Client-Funktion.

Die automatische Verbindungsherstellung im Cisco Secure Client erfolgt in den folgenden Szenarien:

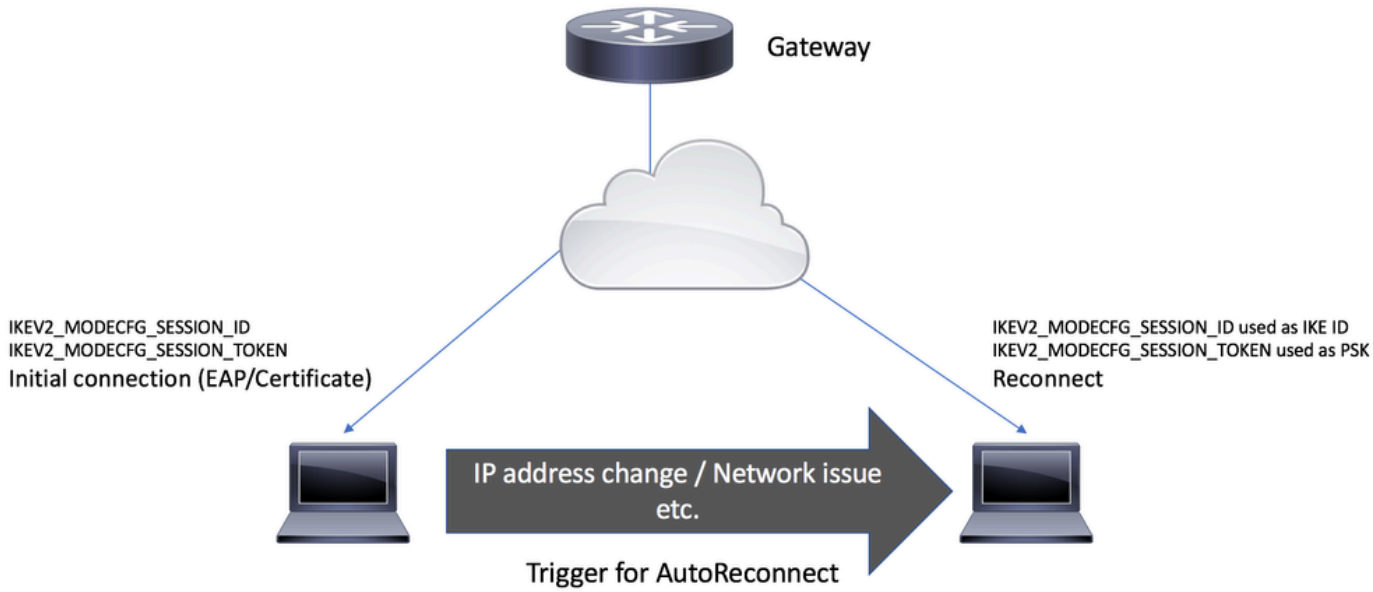
1. Das Zwischennetzwerk ist ausgefallen. Der Cisco Secure Client versucht, die Sitzung wieder aufzunehmen, sobald sie aktiv ist.
2. Das Cisco Secure Client-Gerät wechselt zwischen Netzwerken. Dies führt zu einer Änderung des Quellports, wodurch die vorhandene Sicherheitszuordnung (SA) deaktiviert wird. Daher versucht der Cisco Secure Client, die SA mithilfe der Funktion zur automatischen Wiederherstellung wieder herzustellen.
3. Das Cisco Secure Client-Gerät versucht, die Sicherheitszuordnung nach der Rückkehr aus dem Energiesparmodus oder Ruhezustand wieder aufzunehmen.

## Vorteile der Funktion für die automatische Verbindungswiederherstellung

- Die in der ursprünglichen Sitzung verwendeten Konfigurationsattribute werden ohne Abfrage des AAA-Servers (Authentication, Authorization, Accounting) wiederverwendet.
- Das IKEv2-Gateway muss keine Verbindung zum RADIUS-Server herstellen, um erneut eine Verbindung zum Client herzustellen.
- Während der Fortsetzung der Sitzung ist keine Benutzerinteraktion zur Authentifizierung oder Autorisierung erforderlich.
- Die Authentifizierungsmethode ist der vorinstallierte Schlüssel, wenn eine Sitzung erneut

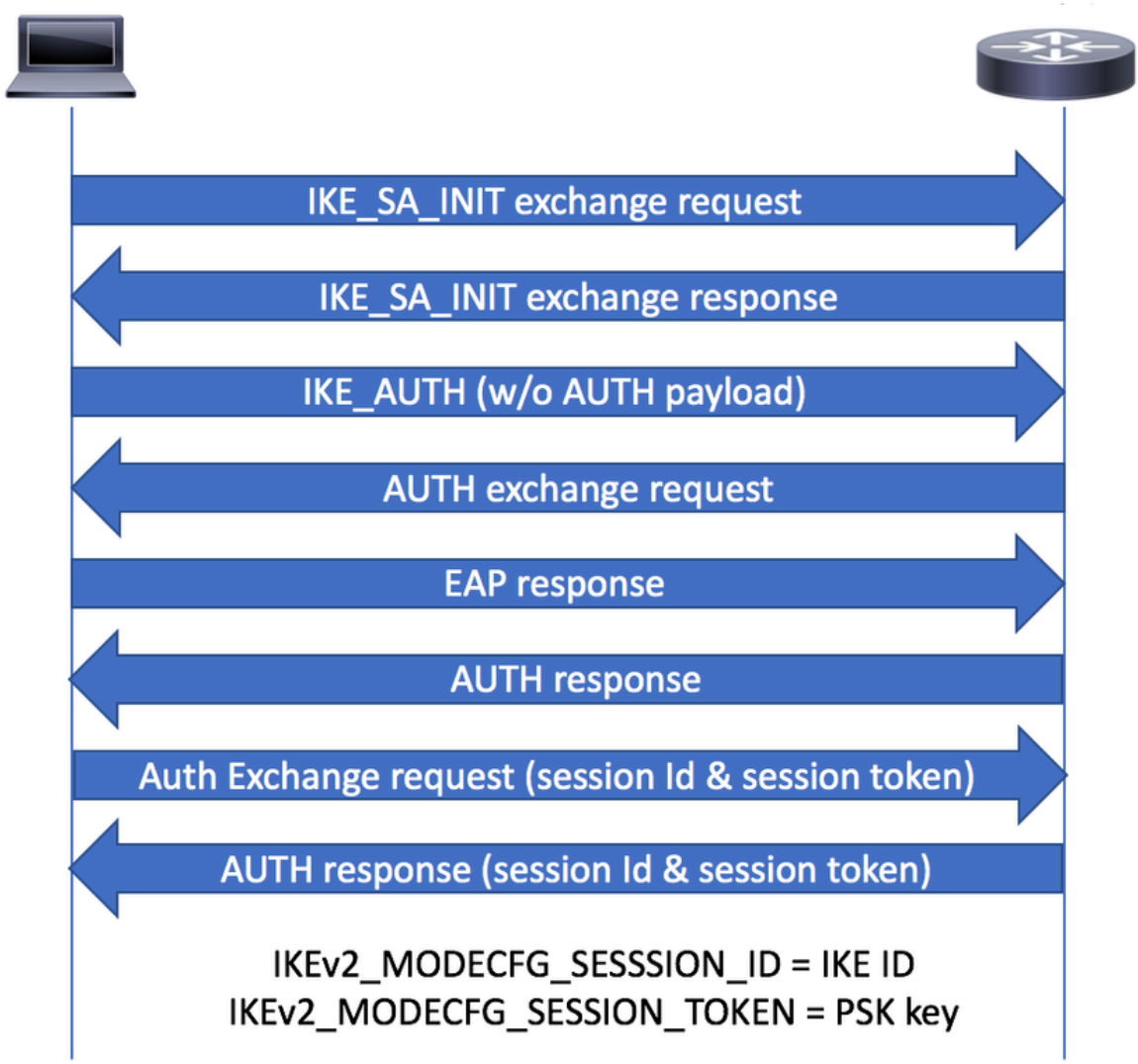
verbunden wird. Diese Authentifizierungsmethode ist im Vergleich zu anderen Authentifizierungsmethoden schnell.
- Die Authentifizierungsmethode für vorinstallierte Schlüssel hilft bei der Wiederaufnahme einer Sitzung mit der Cisco IOS-Software mit minimalen Ressourcen.
- Die nicht verwendeten Sicherheitszuordnungen (SAs) werden entfernt, wodurch die Krypto-Ressourcen freigegeben werden.

## Verbindungsfluss automatisch wiederherstellen

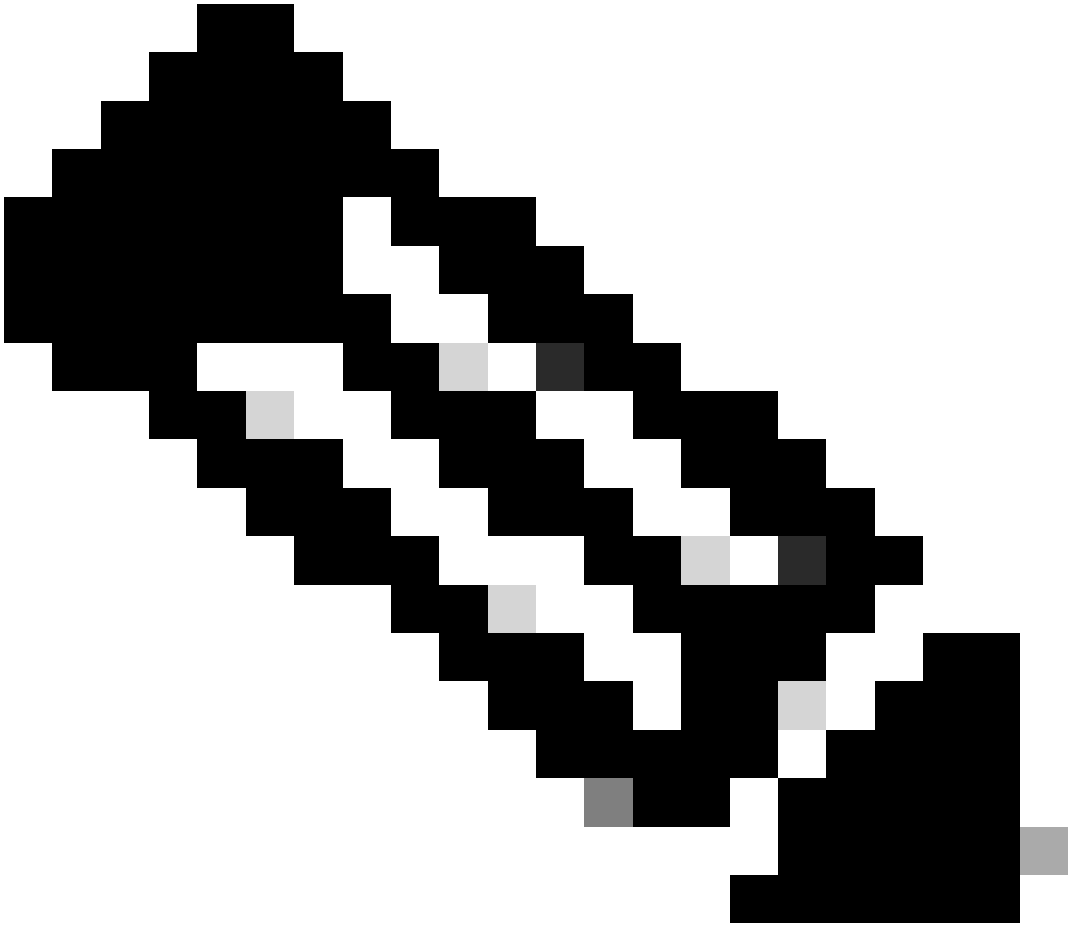



Trigger für AutoReconnect

1. Während des AUTH-Austauschs fordert der Cisco Secure Client das Session-Token- und Session-ID-Attribut vom IKEv2-Gateway in der MODECFG_REQ-Nutzlast von IKE_AUTH-Anforderung an.
2. Das IKEv2-Gateway überprüft mithilfe des Befehls reconnect, ob die Cisco IOS IKEv2-Unterstützung für die Funktion "Auto Reconnect" der Secure Client-Funktion im IKEv2-Profil aktiviert ist, wählt die IKEv2-Richtlinie des ausgewählten IKEv2-Profils aus und sendet die Sitzungs-ID und die Sitzungstokenattribute an den Secure Client in der Payload "CFGMODE_REPLY" des IKE_AUTH-Antwort.

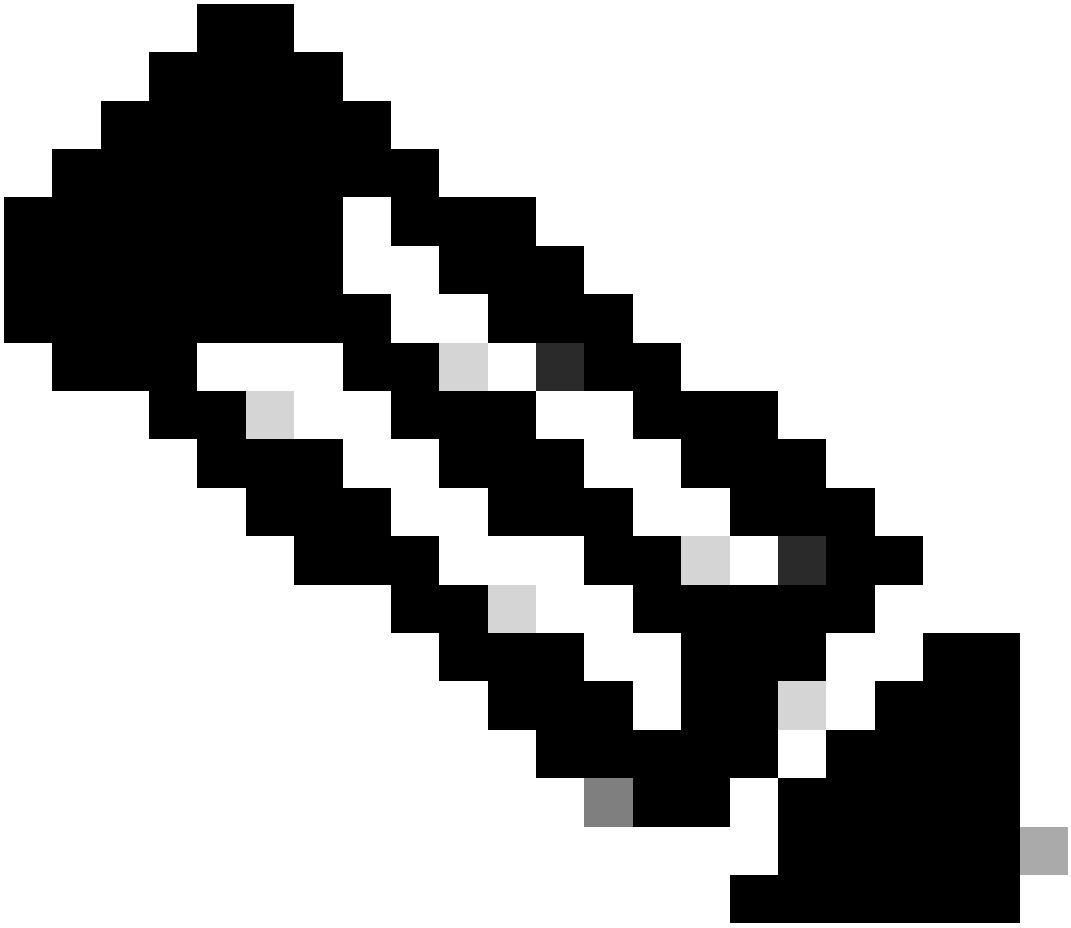



CFGMODE-Austausch

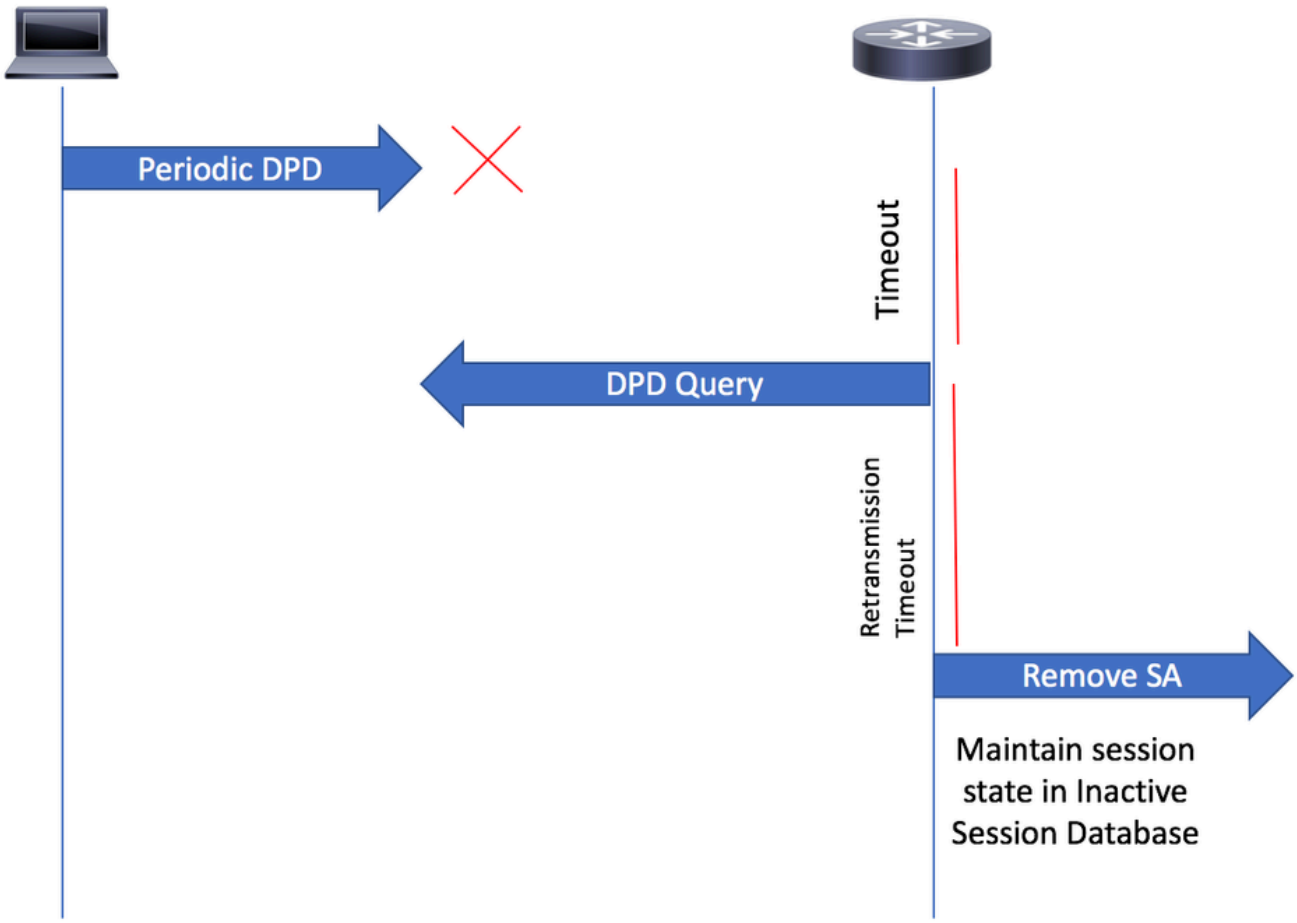


Anmerkung: Der Prozess zur Identifizierung nicht antwortender Clients basiert auf Dead Peer Detection (DPD). Wenn die Funktion zum erneuten Verbinden im IKEv2-Profil aktiviert ist, müssen Sie DPD nicht konfigurieren, da DPD in IKEv2 als On-Demand-Anwendung in die Warteschlange gestellt wird.

3. Der Cisco Secure Client sendet regelmäßig DPD-Nachrichten an das Kabelmodem. Wenn DPD als On-Demand-Nachricht in die Warteschlange gestellt wird, sendet das Gateway keine DPD-Nachrichten an den Client, bis es DPD vom Client empfängt. Wenn DPD nicht innerhalb des festgelegten Zeitraums vom Secure Client empfangen wird (gemäß konfiguriertem DPD-Intervall), sendet das Gateway eine DPD-Nachricht. Wenn vom Secure Client keine Antwort empfangen wird, wird die SA aus der Datenbank der aktiven Sitzung gelöscht.



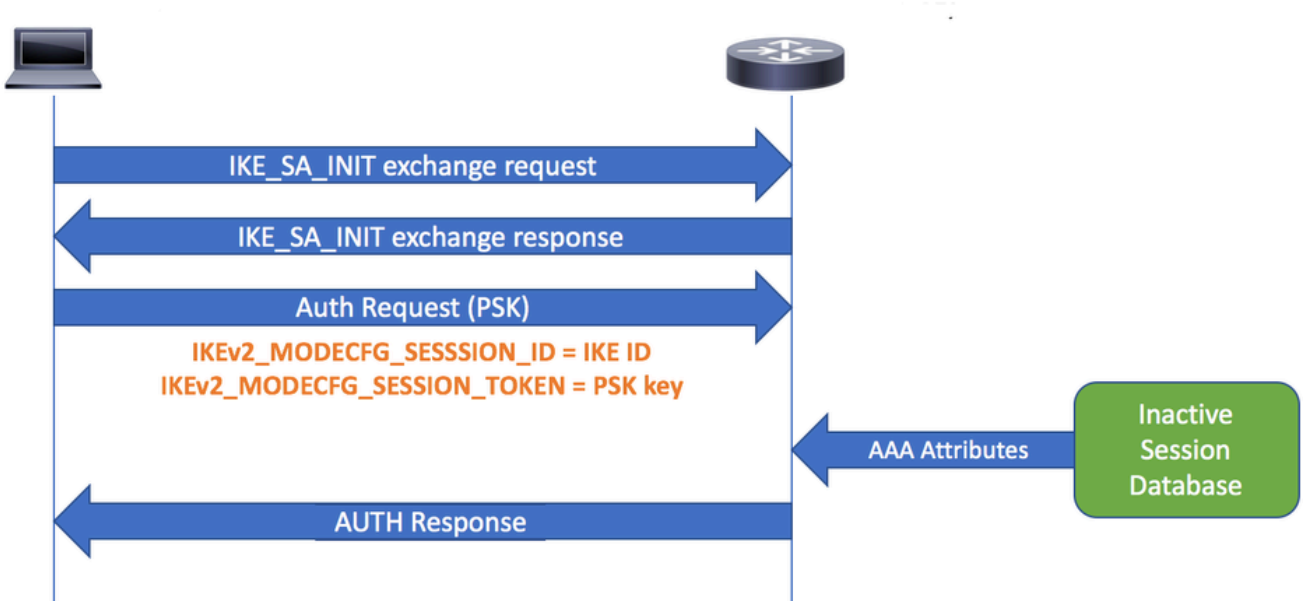
Anmerkung: Das Gateway erhält den Sitzungsstatus (z. B. AAA-Attribute) weiterhin in einer separaten inaktiven Sitzungsdatenbank aufrecht, um die erneute Verbindung gemäß dem konfigurierten Timeout für erneute Verbindungen zuzulassen.




DPD-Abfrage

4. Wenn der Client versucht, die Verbindung wiederherzustellen, erstellt er eine neue IKE SA und verwendet die IKE-Identität (ID) als Sitzungs-ID, die er von der Payload MODECFG_REPLY erhalten hat. Zu diesem Zeitpunkt verwendet der Cisco Secure Client die IKE PSK-Authentifizierung für die erneute Verbindung, wobei der vorinstallierte Schlüssel das zuvor empfangene Sitzungstoken ist.

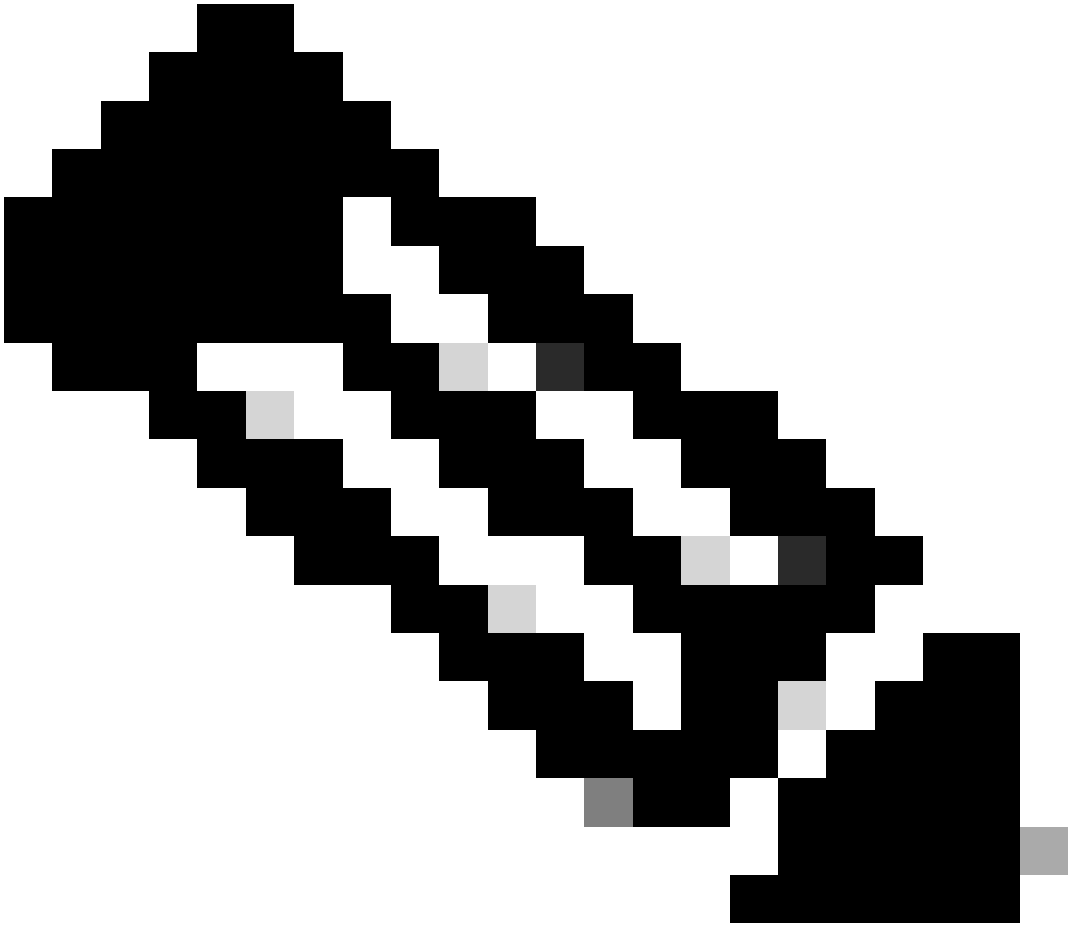
5. Wenn das Gateway eine Anforderung zur erneuten Verbindung empfängt, sucht es in der Datenbank für inaktive Sitzungen nach der IKE-Peer-ID (die als Sitzungs-ID dient). Während der erneuten Verbindung werden die gespeicherten benutzerdefinierten Attribute aus der inaktiven Datenbank abgerufen und auf die neue SA angewendet.




Erneut verbinden

# Konfigurieren

## Router-Konfiguration



Anmerkung: Weitere Informationen zur Routerkonfiguration finden Sie im Dokument Konfigurieren des FlexVPN-Headends für den sicheren Client (AnyConnect) IKEv2-Remote-Zugriff mithilfe der lokalen Benutzerdatenbank.

Dieser Konfigurationsausschnitt zeigt ein Beispiel für die Konfiguration von Cisco Secure Client IKEv2 Remote Access und wie AutoReconnect durch die Konfiguration von reconnect unter dem IKEv2-Profil aktiviert wird.

<#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-Profil

## <#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>
```

# Einschränkungen für die Konfiguration der IKEv2-Wiederverbindung

1. Die Methode zur Autorisierung des vorinstallierten Schlüssels kann im IKEv2-Profil (Internet Key Exchange Version 2) nicht konfiguriert werden. Dies liegt daran, dass die Cisco IOS IKEv2-Unterstützung für AutoReconnect-Funktion der Cisco Secure Client-Funktion die Autorisierungsmethode für vorinstallierte Schlüssel verwendet und die Konfiguration des vorinstallierten Schlüssels auf demselben IKEv2-Profil zu Verwirrung führen kann.
2. Diese Befehle können im IKEv2-Profil nicht konfiguriert werden:

- Authentifizierung lokale Pre-Share
- Authentifizierung Remote Pre-Share
- Schlüsselbund, aaa Autorisierungsgruppe psk
- aaa, Autorisierungsbenutzer, PSK

# Überprüfung

<#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
```

Diese Ausgabe zeigt, dass derzeit 1 aktive Sitzung vorhanden ist, die eine automatische Wiederherstellung der Verbindung ermöglicht:

```
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
```

## Nach erneuter Verbindung

Wenn der Cisco Secure Client erneut eine Verbindung herstellt, verwendet er IKEV2_MODECFG_SESSION_ID als IKE-ID. Daher ist Phase1_id nach der erneuten Verbindung nicht mehr $AnyConnectClient$; Stattdessen ist es die Session-ID, wie dargestellt. Beachten Sie außerdem, dass für die Funktionen jetzt R festgelegt sind. R gibt hier an, dass es sich um eine Verbindungswiederherstellung handelt.

<#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: 72495548 4B6363445269557 4465441547771

      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
```

Nach der erneuten Verbindung lautet die Authentifizierungsmethode jetzt PSK (Pre-Shared Key) anstatt AnyConnect-EAP wie dargestellt:

<#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-Protokolle

### <#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**

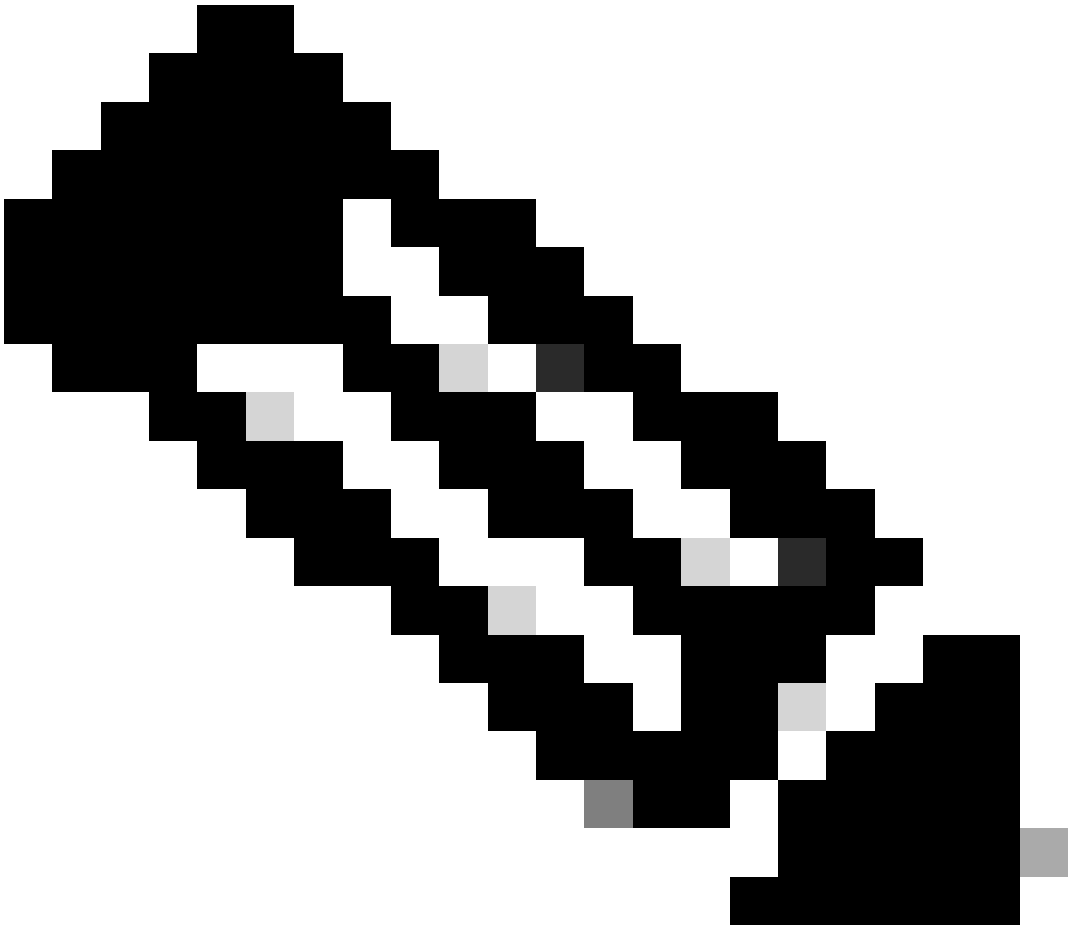
.
.
Date        : 03/13/2025

```
Time        : 03:11:44
Type        : Information
Source      : acvpnui

Description : Message type information sent to the user:
```

**Connected to IKEv2_Gateway.**

---



> Anmerkung: In DART-Protokollen wird die IKE-ID als 'rIUHKccDRiUtFTATwq' angezeigt. Dabei handelt es sich um die ASCII-Darstellung von '724955484B6363445269557446544154771', die als Remote-ID in der Ausgabe von 'show crypto session detail' angezeigt wird.

---

# Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

IKEv2-Debugging-Vorgänge, um die Aushandlung zwischen dem Gateway und dem Client zu überprüfen.

```
Debug crypto condition peer ipv4
```

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

## Zugehörige Informationen

- Sicherheits- und VPN-Konfigurationsleitfaden, Cisco IOS XE 17.x
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.