Comprensión de las funciones de reconexión de IKEv2 y AnyConnect

Contenido

Introducción

Este documento describe cómo funciona la función IKEv2 Auto Reconnect en los routers Cisco IOS® y Cisco IOS® XE para AnyConnect.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Intercambio de claves de Internet versión 2 (IKEv2)
- Cisco Secure Client (CSC)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Catalyst 8000V (C8000V) con versión 17.16.01a
- Cisco Secure Client versión 5.1.8.105
- PC cliente con Cisco Secure Client instalado

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Función IKEv2 y Cisco Secure Client Reconnect

La función Auto Reconnect (Reconexión automática) de Cisco Secure Client le ayuda a recordar la sesión durante un período de tiempo y a reanudar la conexión después de establecer el canal seguro. Dado que Cisco Secure Client se utiliza ampliamente con la versión 2 de Intercambio de claves de Internet (IKEv2), IKEv2 amplía la compatibilidad con la función Reconexión automática en el software Cisco IOS mediante la función Cisco IOS IKEv2 para Reconexión automática de la función Secure Client.

La Reconexión automática en Cisco Secure Client se produce en los siguientes escenarios:

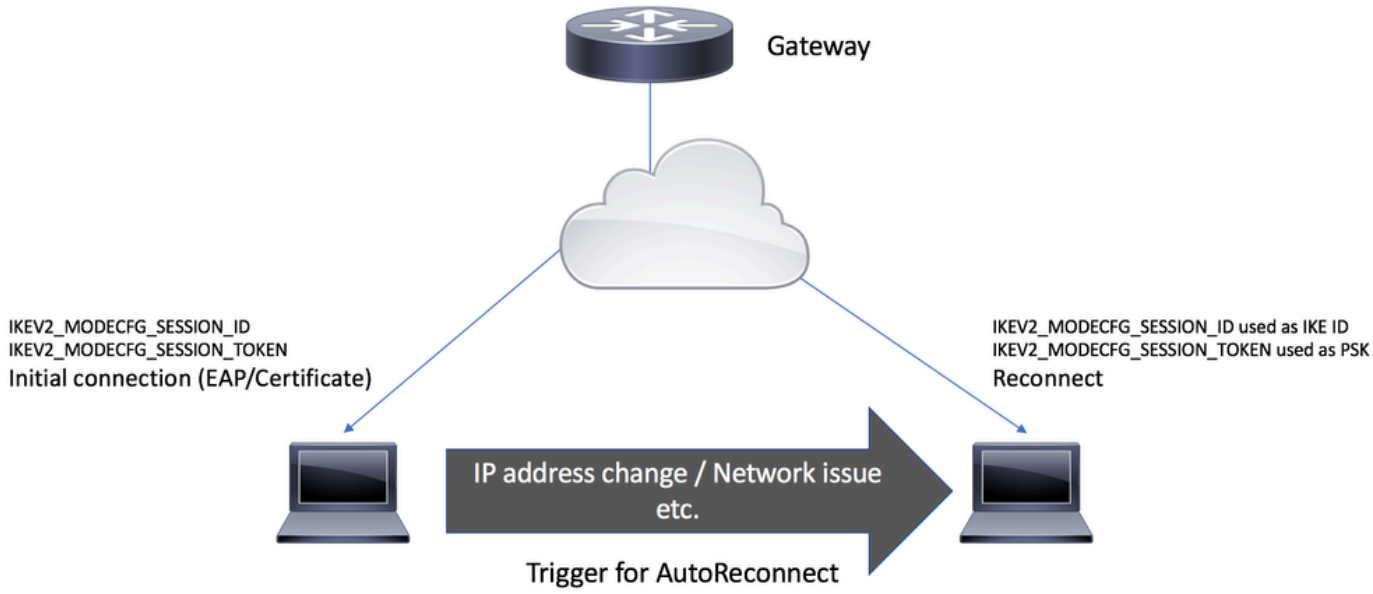
1. La red intermedia está fuera de servicio. Cisco Secure Client intenta reanudar la sesión cuando está activa.
2. El dispositivo Cisco Secure Client cambia entre redes. Esto produce un cambio en el puerto de origen, que desactiva la asociación de seguridad (SA) existente y, por lo tanto, Cisco Secure Client intenta reanudar la SA mediante la función Reconexión automática.
3. El dispositivo Cisco Secure Client intenta reanudar SA después de volver del modo de suspensión o hibernación.

Ventajas de la función de reconexión automática

- Los atributos de configuración utilizados en la sesión original se reutilizan sin consultar el servidor de autenticación, autorización y contabilidad (AAA).
- El gateway IKEv2 no tiene que ponerse en contacto con el servidor RADIUS para volver a conectarse al cliente.
- No se necesita ninguna interacción del usuario para la autenticación o autorización durante la reanudación de la sesión.
- El método de autenticación es la clave previamente compartida al volver a conectar una sesión. Este método de autenticación es rápido en comparación con otros métodos de autenticación.
- El método de autenticación de clave previamente compartida ayuda a reanudar una sesión

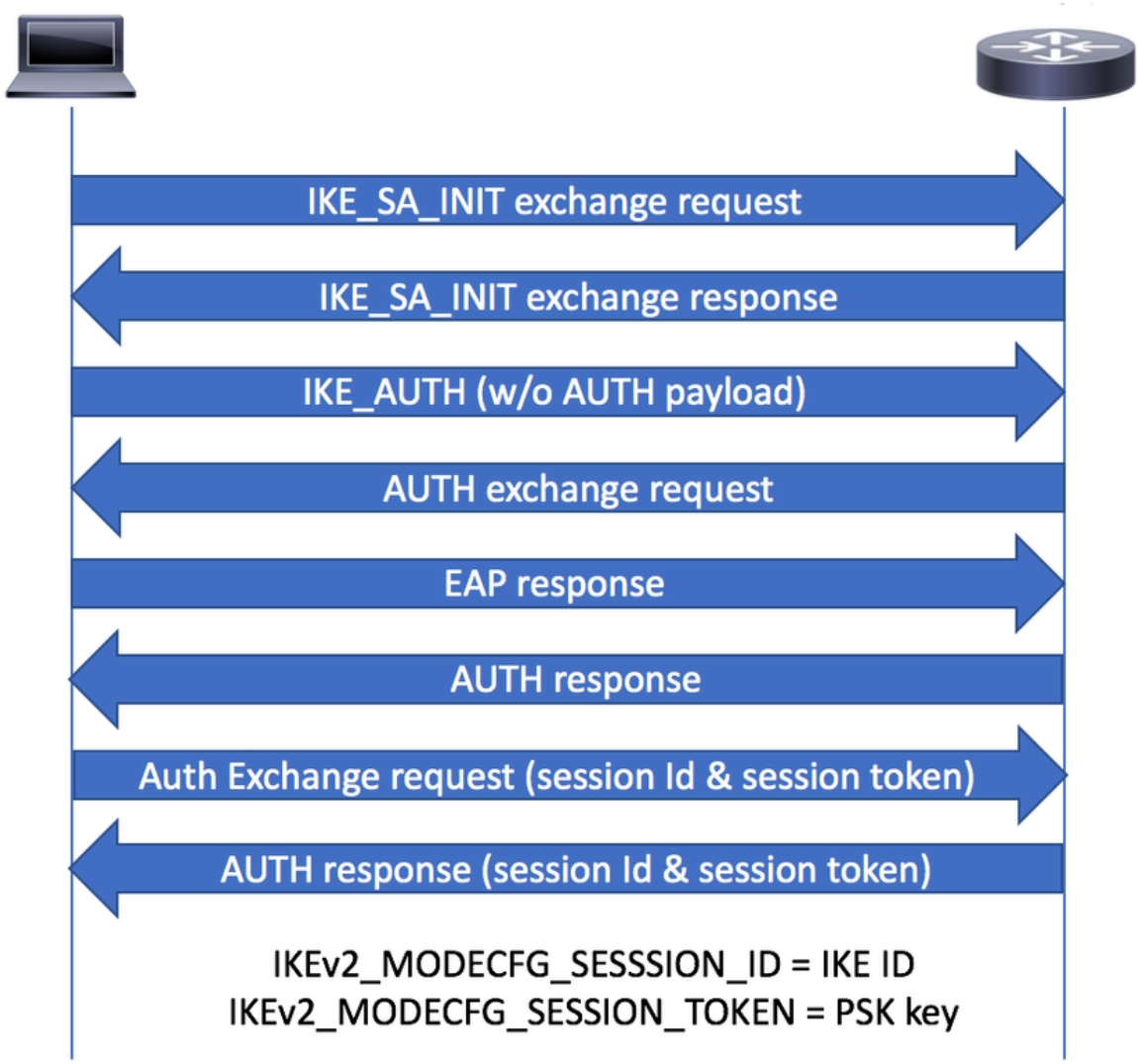
en el software Cisco IOS con recursos mínimos.
- Las asociaciones de seguridad (SA) no utilizadas se eliminan, con lo que se liberan los recursos criptográficos.

Flujo de conexión de reconexión automática

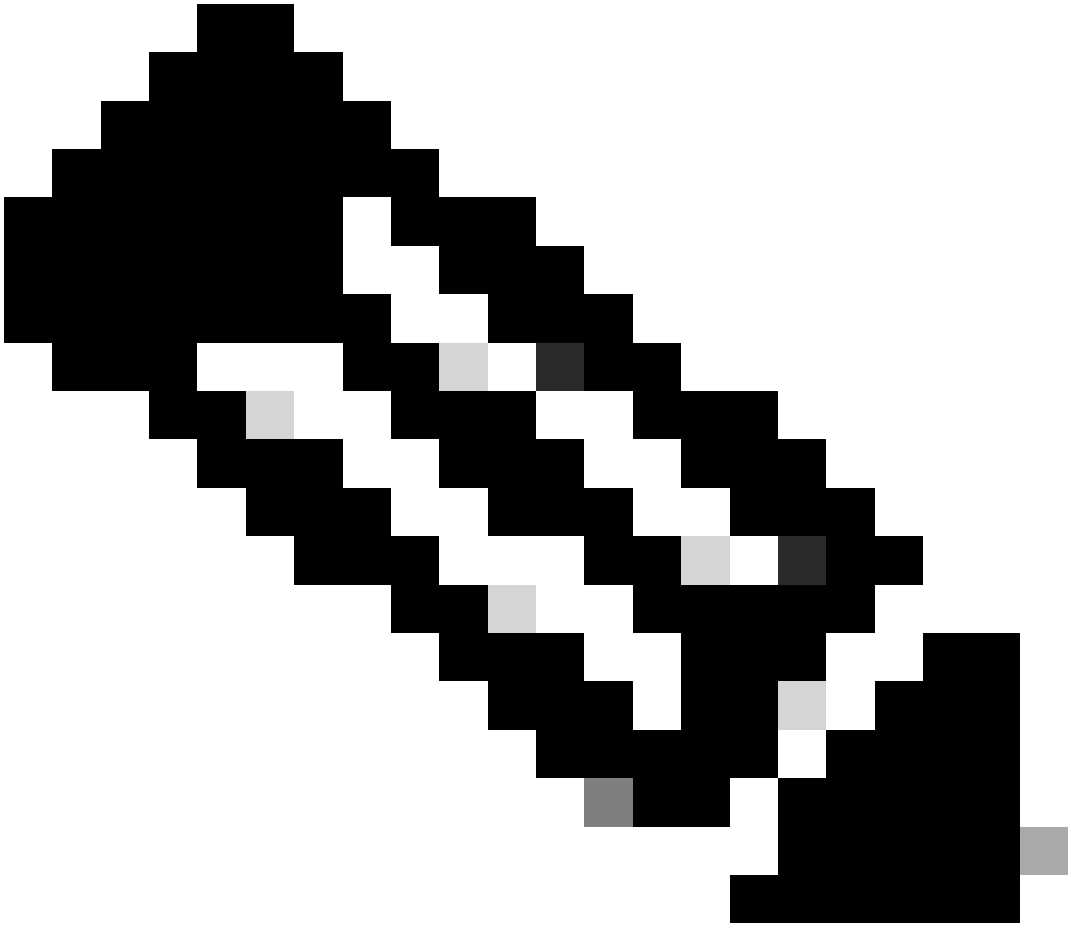


Desencadenador para la reconexión automática

1. Durante el intercambio AUTH, Cisco Secure Client solicita el token de sesión y el atributo de ID de sesión de la puerta de enlace IKEv2 en la carga útil MODECFG_REQ de la solicitud IKE_AUTH.
2. IKEv2 Gateway verifica si el soporte IKEv2 de Cisco IOS para la función de Reconexión automática de la función Secure Client está habilitado en el perfil IKEv2 mediante el comando reconnect, selecciona la política IKEv2 del perfil IKEv2 elegido y envía el ID de sesión y los atributos del token de sesión al Secure Client en la carga útil CFGMODE_REPLY de la respuesta IKE_AUTH.

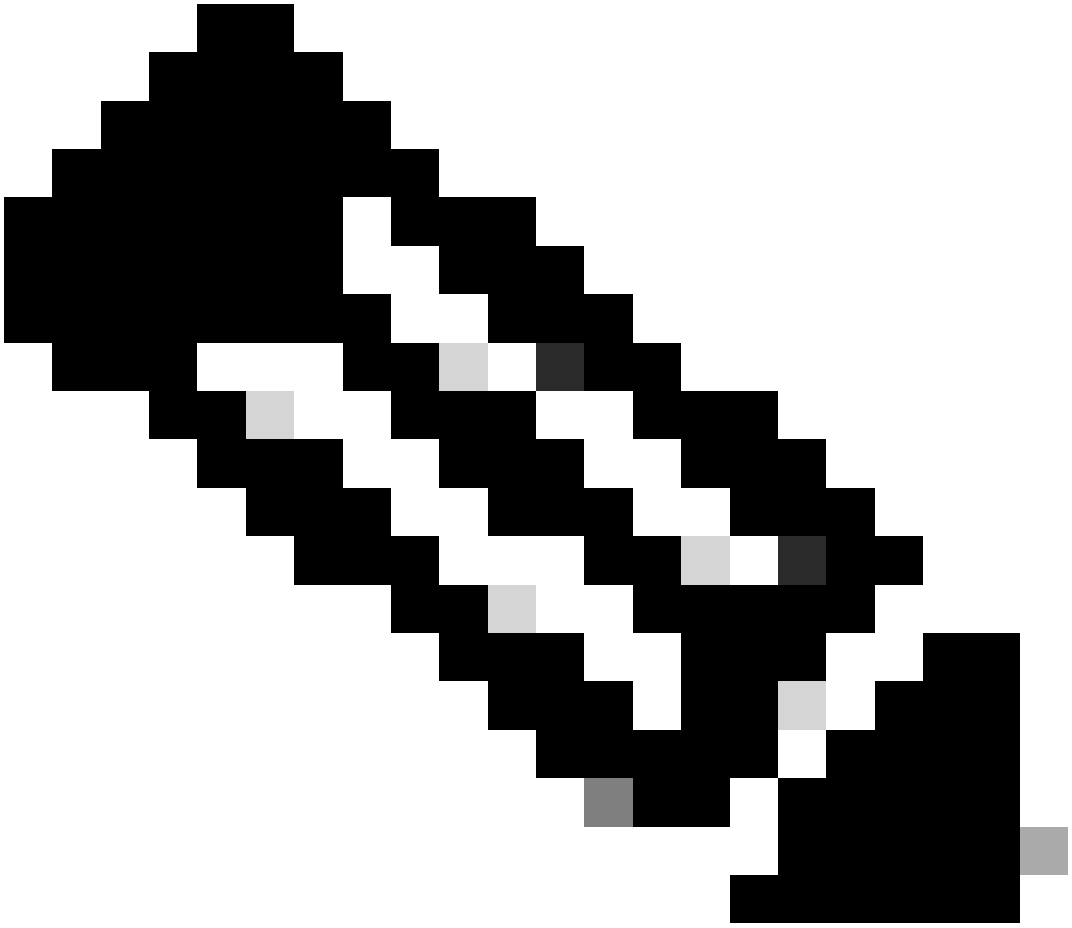


CFGMODE Exchange

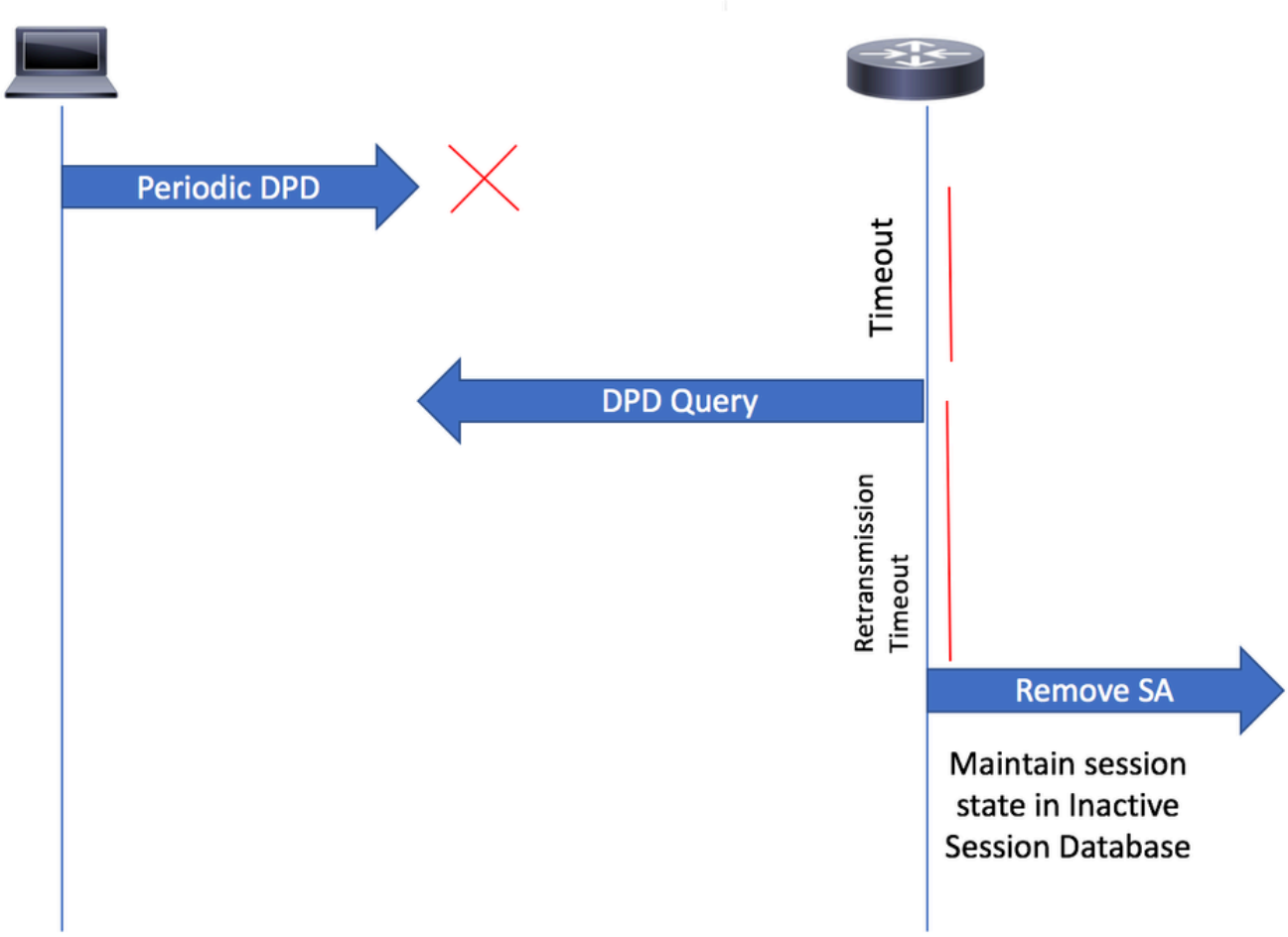


Nota: El proceso de identificación de clientes que no responden se basa en la detección de puntos inactivos (DPD). Si la función de reconexión está activada en el perfil IKEv2, no es necesario configurar DPD, ya que DPD se pone en cola a petición en IKEv2

3. Cisco Secure Client envía periódicamente mensajes DPD al gateway. Si DPD se pone en cola como a petición, el gateway no envía mensajes DPD al cliente hasta que recibe DPD del cliente. Si no se recibe DPD de Secure Client dentro del período de tiempo especificado (según el intervalo DPD configurado), el gateway envía un mensaje DPD. Si no se recibe ninguna respuesta del Secure Client, la SA se elimina de la base de datos de la sesión activa.



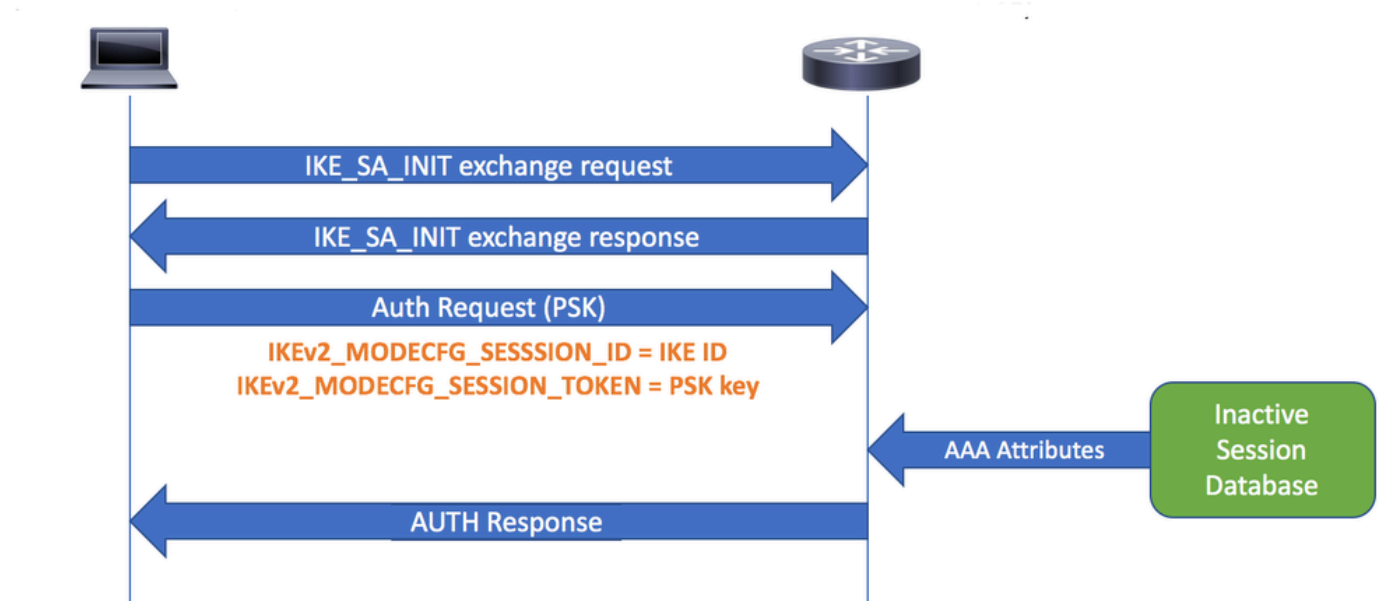
Nota: La puerta de enlace sigue manteniendo el estado de sesión (como atributos AAA) en una base de datos de sesión inactiva independiente para permitir la reconexión según el período de tiempo de espera de reconexión configurado.



Consulta DPD

4. Cuando el cliente intenta volver a conectarse, crea una nueva IKE SA y utiliza la identidad IKE (ID) como ID de sesión, que recibe de la carga útil MODECFG_REPLY. En este momento, Cisco Secure Client utiliza la autenticación IKE PSK para la reconexión, siendo la clave previamente compartida el token de sesión que recibió anteriormente.

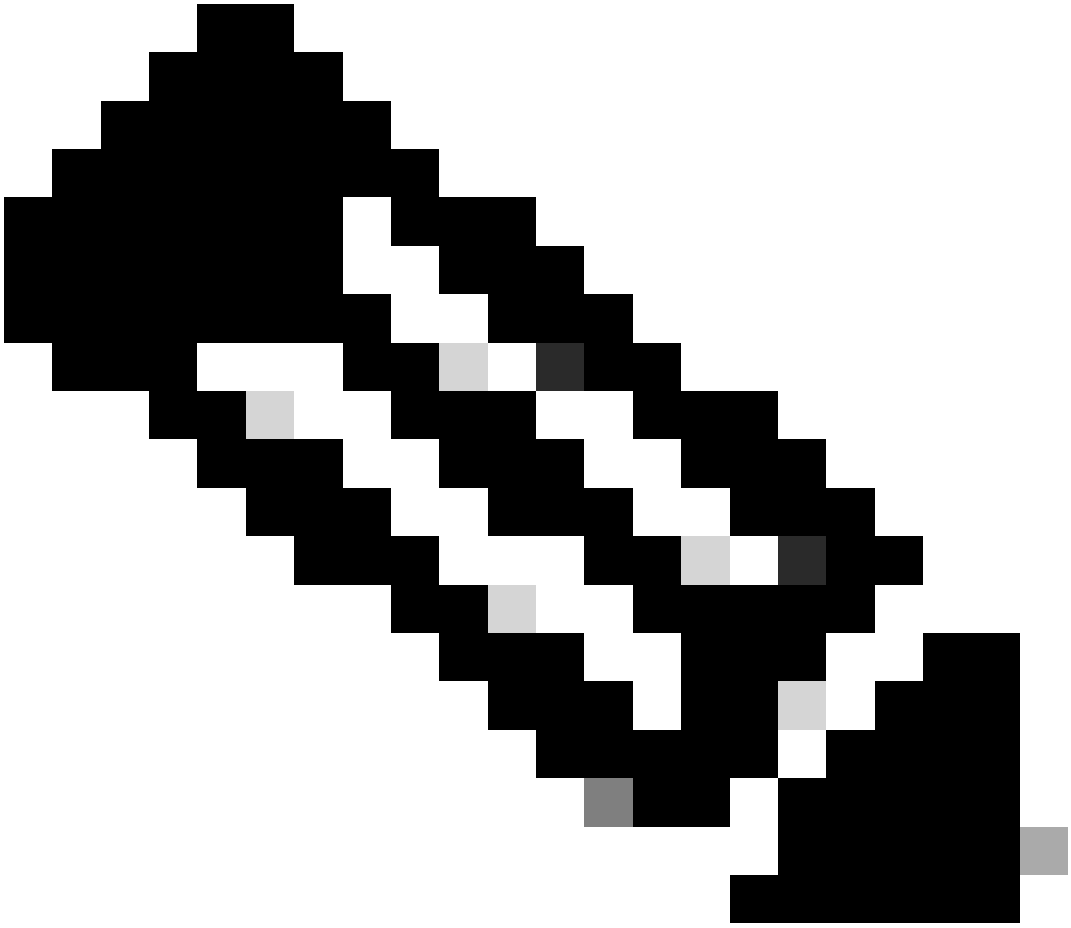
5. Cuando el gateway recibe una solicitud de reconexión, busca en la base de datos de sesiones inactiva la ID IKE del par (que sirve como ID de sesión). Durante la reconexión, los atributos personalizados almacenados de la base de datos inactiva se recuperan y se aplican a la nueva SA.



Volver a conectar

Configurar

Configuración del router



Nota: Para la configuración del router, también puede consultar el documento Configuración de la cabecera FlexVPN para el acceso remoto IKEv2 de cliente seguro (AnyConnect) mediante la base de datos de usuario local

Este fragmento de configuración muestra un ejemplo de la configuración de acceso remoto IKEv2 de Cisco Secure Client y cómo se habilita la Reconexión automática al configurar la reconexión en el perfil 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
```

Perfil de Cisco Secure Client

<#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>
```

Restricciones de Configuración de IKEv2 Reconnect

1. El método de autorización de clave previamente compartida no se puede configurar en el perfil de Intercambio de claves de Internet versión 2 (IKEv2). Esto se debe a que la función Cisco IOS IKEv2 support for AutoReconnect de la función Cisco Secure Client utiliza el método de autorización de clave previamente compartida y la configuración de la clave previamente compartida en el mismo perfil IKEv2 puede conducir a confusión.
2. Estos comandos no se pueden configurar en el perfil IKEv2:

- authentication local pre-share
- authentication remote pre-share
- keyring, aaa authorization group psk
- aaa authorization user psk

Verificación

<#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
```

Este resultado muestra que actualmente hay 1 sesión activa que es capaz de la reconexión automática:

```
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
```

Después de volver a conectar

Cuando Cisco Secure Client se vuelve a conectar, utiliza IKEV2_MODECFG_SESSION_ID como ID de IKE. Por lo tanto, después de la reconexión, Phase1_id ya no es $AnyConnectClient$; en su lugar, es el ID de sesión, como se muestra. Además, tenga en cuenta que las capacidades ahora tienen R configurado. Aquí, R indica que esta es una sesión de reconexión.

<#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
```

Después de la reconexión, el método de autenticación es ahora PSK (clave precompartida) en lugar de AnyConnect-EAP, como se muestra a continuación:

<#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#
```

Registros de DART de 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

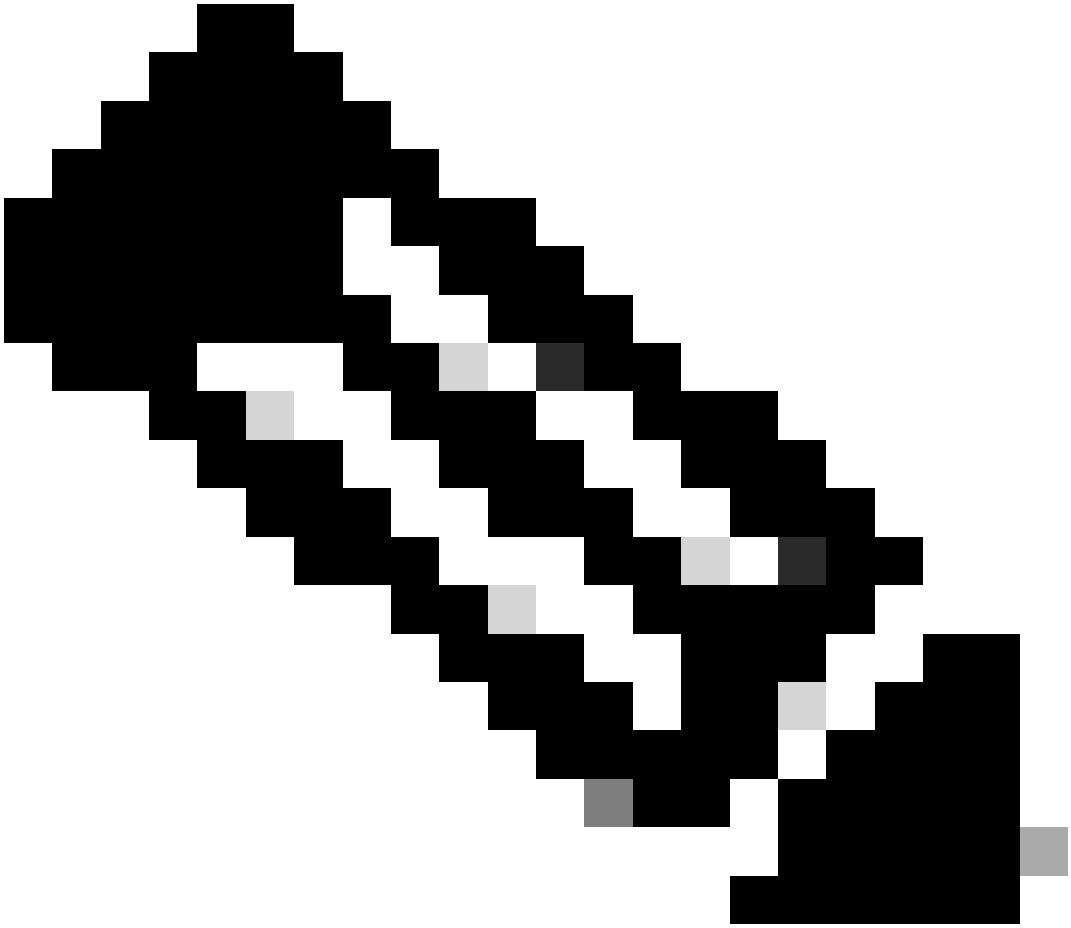
Using IKE ID 'rIUHKccDRiUtFTATwq' for reconnect

.
.
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: En los registros DART, el ID IKE se muestra como 'IUHKccDRiUtFTATwq', que es la representación ASCII de '724955484B6363445269557446544154771', que se muestra como ID remoto en la salida de "show crypto session detail".

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Depuraciones IKEv2 para verificar la negociación entre la puerta de enlace y el cliente.

```
Debug crypto condition peer ipv4
```

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

Información Relacionada

- Guía de Configuración de Seguridad y VPN, Cisco IOS XE 17.x
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).