Entender o recurso de reconexão do IKEv2 e do AnyConnect

Contents

Introdução

Este documento descreve como o recurso de reconexão automática IKEv2 funciona no Cisco IOS® e nos roteadores Cisco IOS® XE para o AnyConnect.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Catalyst 8000V (C8000V) executando a versão 17.16.01a
- Cisco Secure Client versão 5.1.8.105
- PC cliente com Cisco Secure Client instalado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

IKEv2 e recurso de reconexão do Cisco Secure Client

O recurso de reconexão automática no Cisco Secure Client ajuda o cliente a lembrar a sessão por um período de tempo e a retomar a conexão após estabelecer o canal seguro. Como o Cisco Secure Client é usado extensivamente com o Internet Key Exchange Versão 2 (IKEv2), o IKEv2 estende o suporte ao recurso de Reconexão Automática no software Cisco IOS através do suporte do Cisco IOS IKEv2 para o recurso de Reconexão Automática do recurso de Cliente Seguro.

A reconexão automática no Cisco Secure Client ocorre nos seguintes cenários:

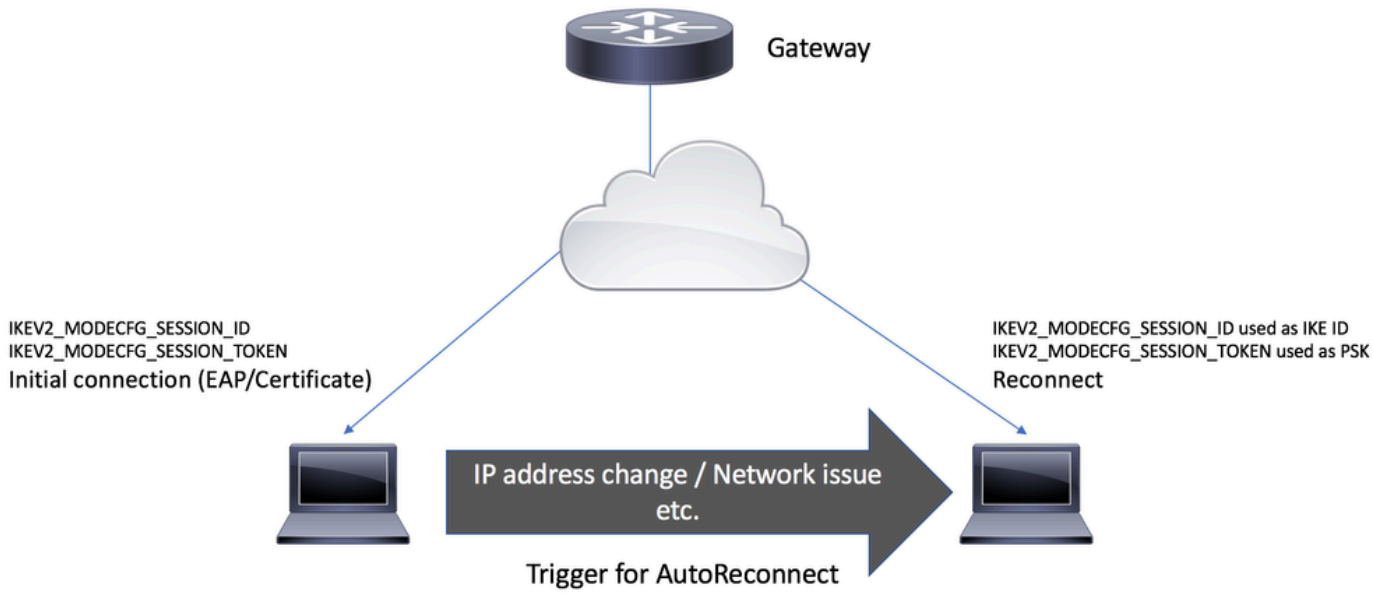
1. A rede intermediária está inoperante. O Cisco Secure Client tenta retomar a sessão quando ela está ativa.
2. O dispositivo Cisco Secure Client alterna entre redes. Isso resulta na alteração da porta de origem, o que desativa a associação de segurança (SA) existente e, portanto, o Cisco Secure Client tenta retomar a SA usando o recurso de Reconexão Automática.
3. O dispositivo Cisco Secure Client tenta retomar a AS após retornar do modo de espera ou hibernação.

Vantagens do recurso de reconexão automática

- Os atributos de configuração usados na sessão original são reutilizados sem consultar o servidor de autenticação, autorização e contabilização (AAA).
- O gateway IKEv2 não precisa entrar em contato com o servidor RADIUS para se reconectar ao cliente.
- Nenhuma interação do usuário para autenticação ou autorização é necessária durante a retomada da sessão.
- O método de autenticação é a chave pré-compartilhada ao reconectar uma sessão. Este método de autenticação é rápido em comparação com outros métodos de autenticação.
- O método de autenticação de chave pré-compartilhada ajuda a retomar uma sessão no software Cisco IOS com recursos mínimos.
- As SAs (associações de segurança) não utilizadas são removidas, liberando assim os

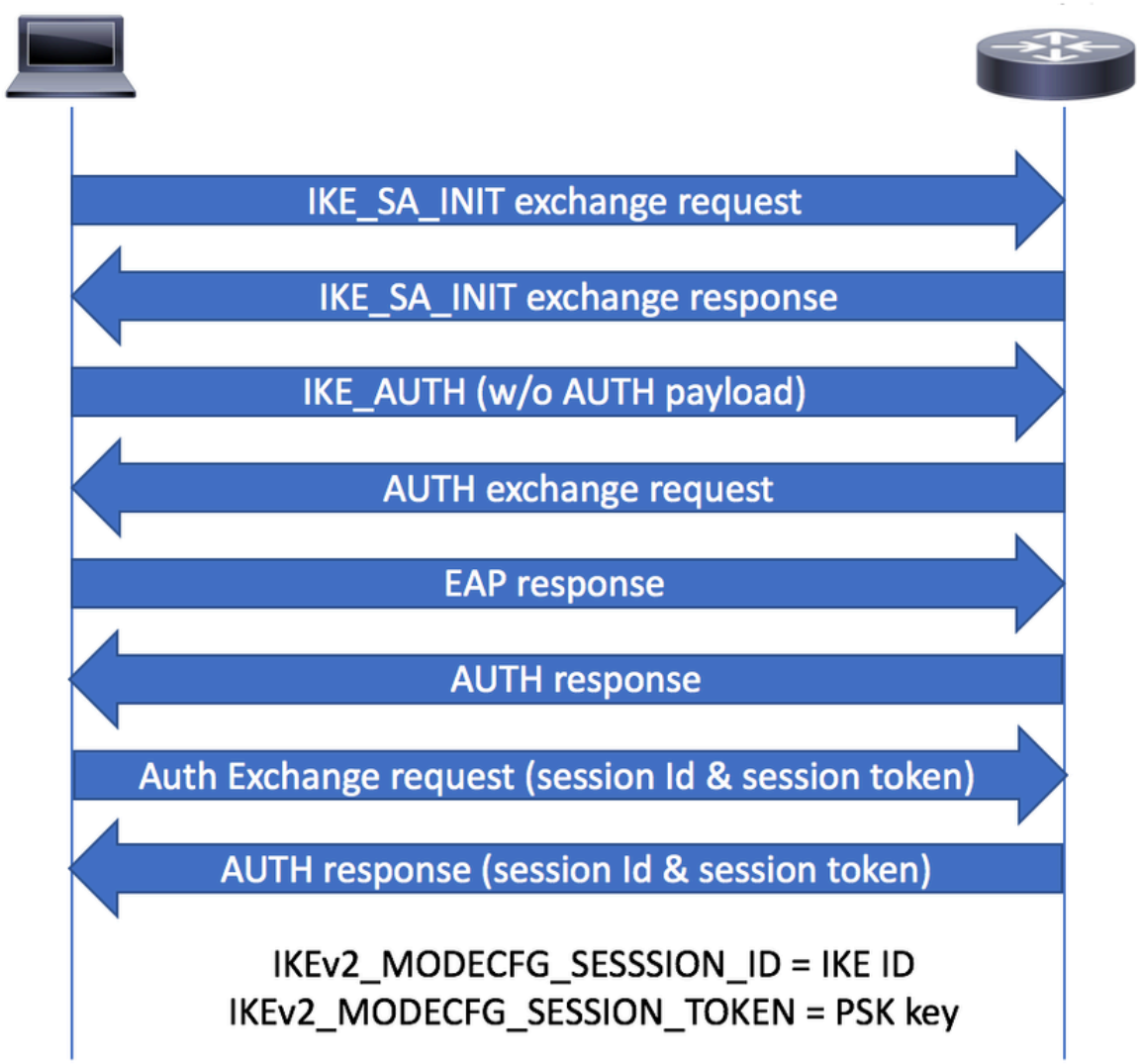
recursos de criptografia.

Fluxo de conexão de reconexão automática

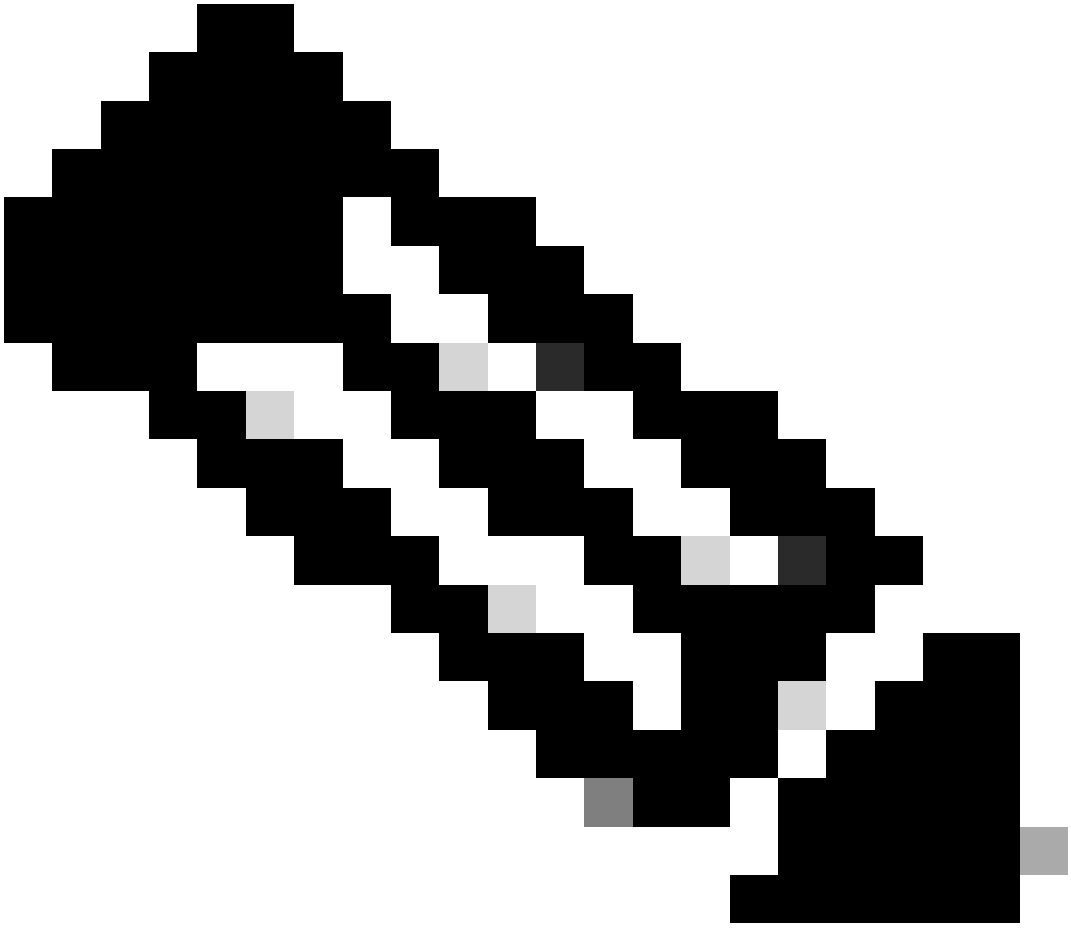


Gatilho para Reconexão Automática

1. Durante a troca de AUTH, o Cisco Secure Client solicita o atributo Session-token e Session-id do Gateway IKEv2 na carga MODECFG_REQ da Solicitação IKE_AUTH.
2. O Gateway IKEv2 verifica se o suporte do Cisco IOS IKEv2 para o recurso de Reconexão Automática do Cliente Seguro está habilitado no perfil IKEv2 usando o comando reconnect, seleciona a política IKEv2 do perfil IKEv2 escolhido e envia a ID da sessão e os atributos do token da sessão para o Cliente Seguro no payload CFGMODE_REPLY da resposta IKE_AUTH.

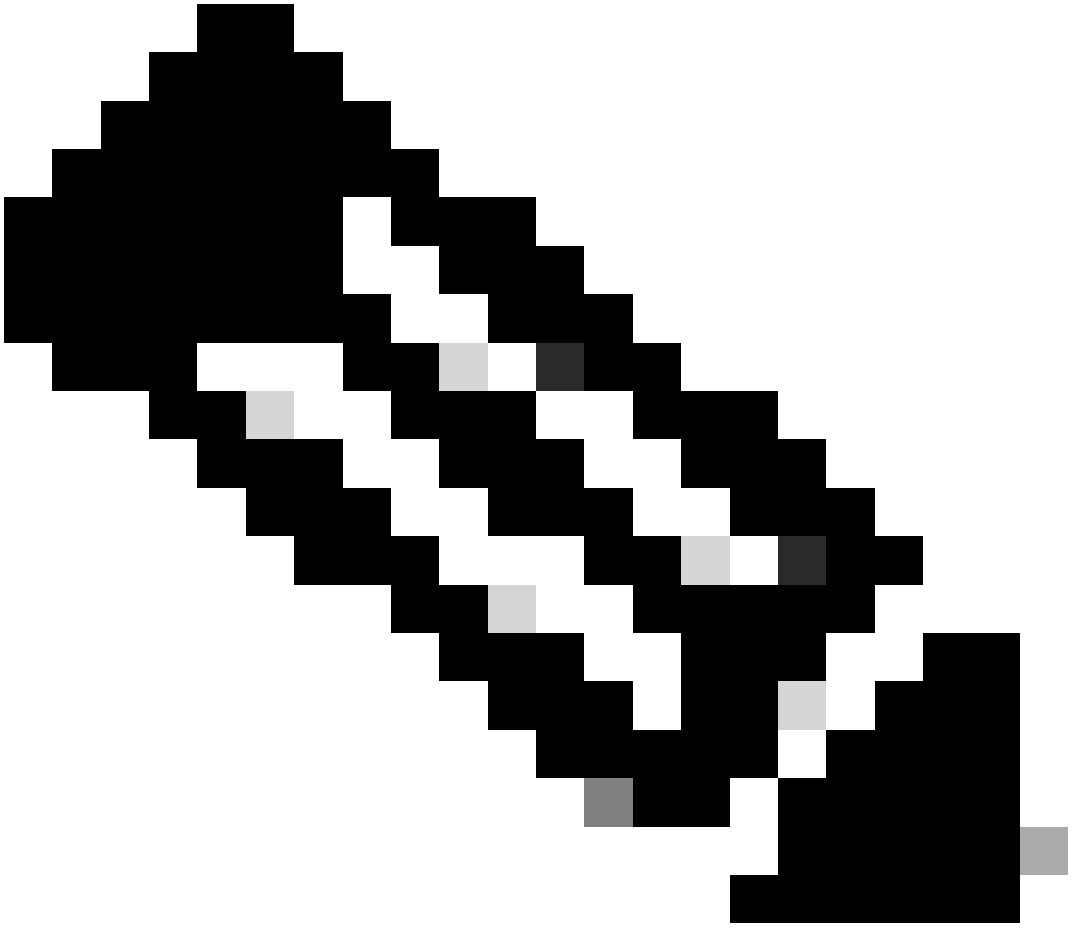


Troca de CFGMODE

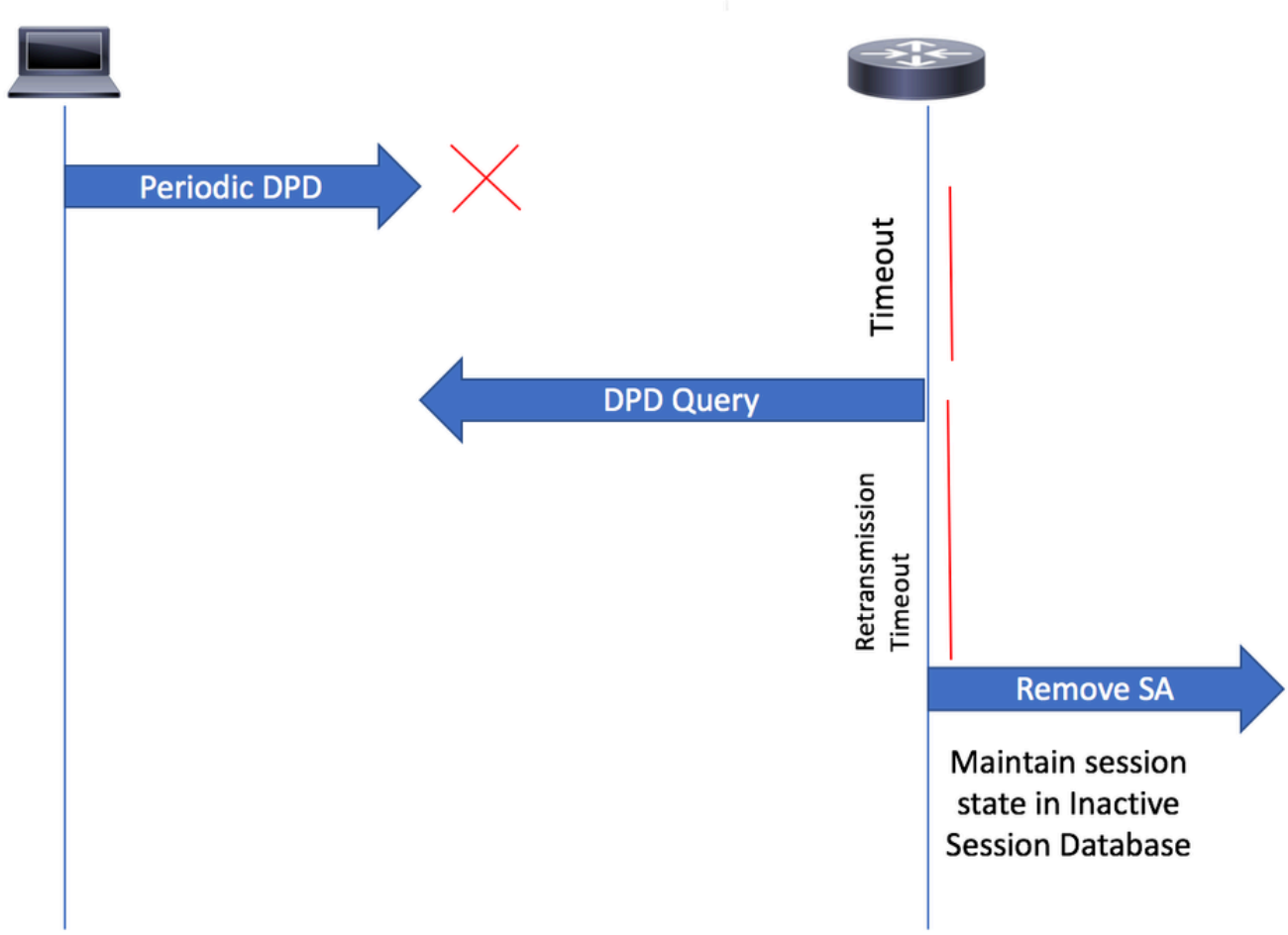


Note: O processo de identificação de clientes que não respondem é baseado na detecção de pares inativos (DPD). Se o recurso de reconexão estiver habilitado no perfil IKEv2, não será necessário configurar o DPD, pois ele será enfileirado como sob demanda no IKEv2

3. O Cisco Secure Client envia periodicamente mensagens DPD ao gateway. Se o DPD for enfileirado como sob demanda, o gateway não enviará mensagens DPD ao cliente até receber o DPD do cliente. Se o DPD não for recebido do Secure Client dentro do período de tempo especificado (de acordo com o intervalo DPD configurado), o gateway enviará uma mensagem DPD. Se nenhuma resposta for recebida do Secure Client, a AS será excluída do banco de dados da sessão ativa.



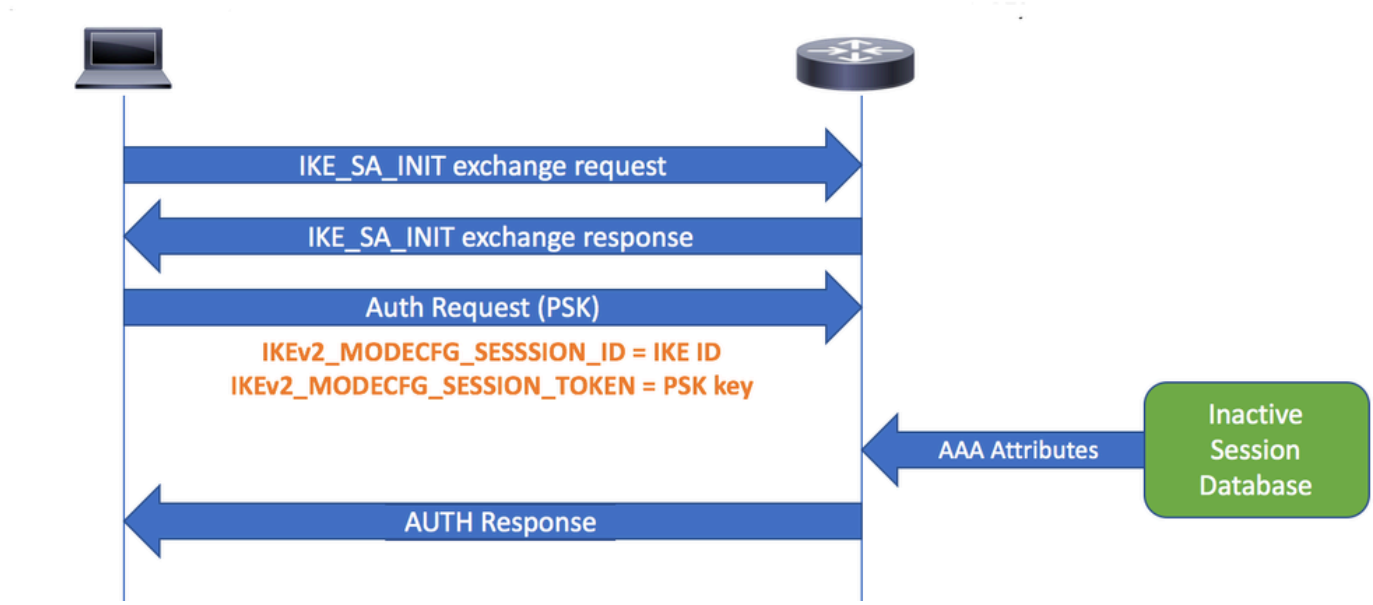
Note: O Gateway ainda mantém o estado da sessão (como Atributos AAA) em um banco de dados de sessão inativo separado para permitir a reconexão de acordo com o período de timeout de reconexão configurado.



Consulta DPD

4. Quando o cliente tenta se reconectar, ele cria uma nova SA de IKE e usa a identidade (ID) de IKE como ID da sessão, que ele recebe da carga útil MODECFG_REPLY. Neste ponto, o Cisco Secure Client usa a autenticação IKE PSK para a reconexão, com a chave pré-compartilhada sendo o token de sessão recebido anteriormente.

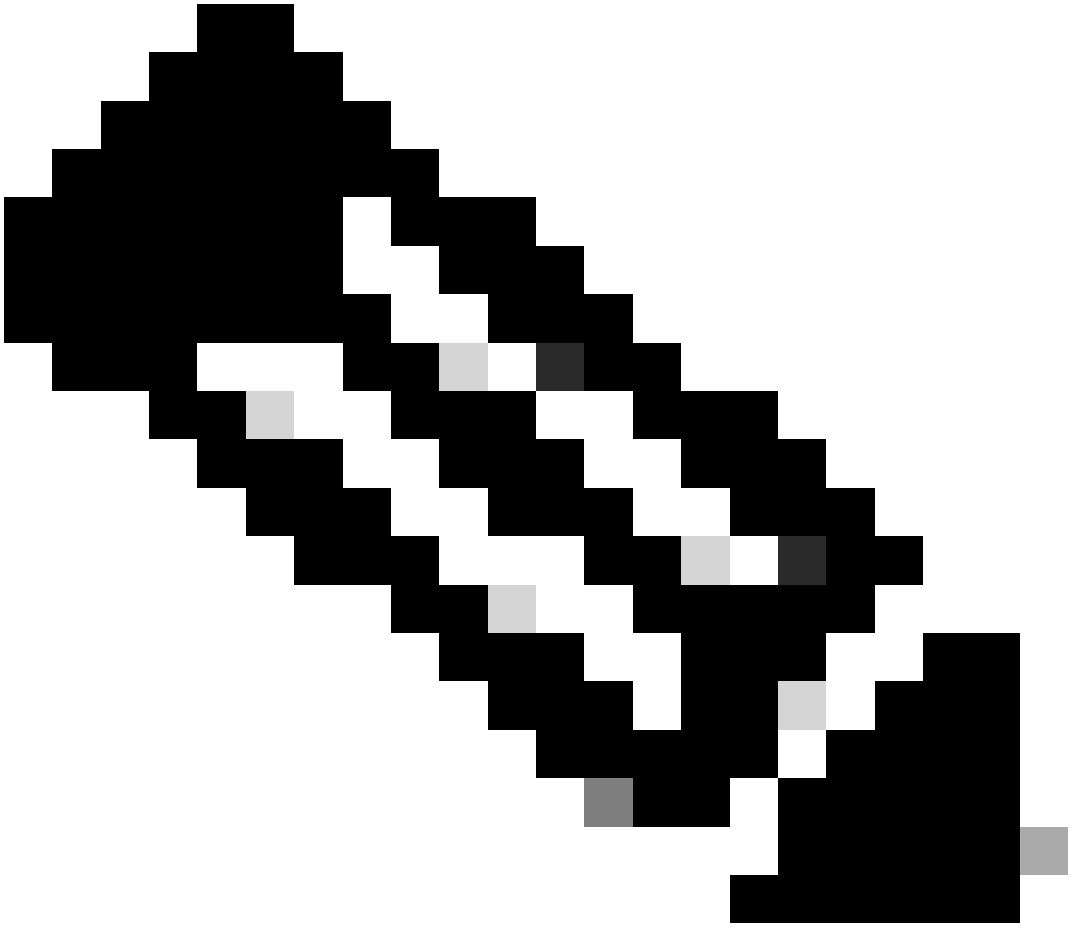
5. Quando o gateway recebe uma solicitação de reconexão, ele procura no Banco de Dados de Sessão Inativa o ID IKE do peer (que serve como ID da sessão). Durante a reconexão, os atributos personalizados armazenados do banco de dados inativo são recuperados e aplicados ao novo SA.



Reconectar

Configurar

Configuração do roteador



Note: Para a configuração do roteador, você também pode consultar o documento [Configure FlexVPN Headend for Secure Client (AnyConnect) IKEv2 Remote Access Using Local User Database]

Este snippet de configuração mostra um exemplo da configuração do Cisco Secure Client IKEv2 Remote Access e como o AutoReconnect é habilitado configurando reconnect sob o 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 do 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>
```

Restrições para configurar a reconexão de IKEv2

1. O método de autorização de chave pré-compartilhada não pode ser configurado no perfil IKEv2 (Internet Key Exchange Version 2). Isso ocorre porque o suporte do Cisco IOS IKEv2 para o recurso AutoReconnect do recurso Cisco Secure Client usa o método de autorização de chave pré-compartilhada e configurar a chave pré-compartilhada no mesmo perfil IKEv2 pode causar confusão.
2. Estes comandos não podem ser configurados no perfil IKEv2:

- pré-compartilhamento local de autenticação
- pré-compartilhamento remoto de autenticação
- keyring, aaa authorization group psk
- aaa authorization user psk

Verificar

<#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
```

Esta saída mostra que atualmente há 1 sessão ativa que é capaz de reconectar 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
```

Após Reconectar

Quando o Cisco Secure Client se reconecta, ele usa o IKEV2_MODECFG_SESSION_ID como ID do IKE. Portanto, após a reconexão, Phase1_id não é mais $AnyConnectClient$; em vez disso, é a ID da sessão, como mostrado. Além disso, observe que os recursos agora têm R definido. Aqui, R indica que esta é uma sessão de reconexão.

<#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
```

Após a reconexão, o método de autenticação agora é PSK (chave pré-compartilhada) em vez do AnyConnect-EAP, como mostrado:

<#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 do Cisco Secure Client DART

<#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

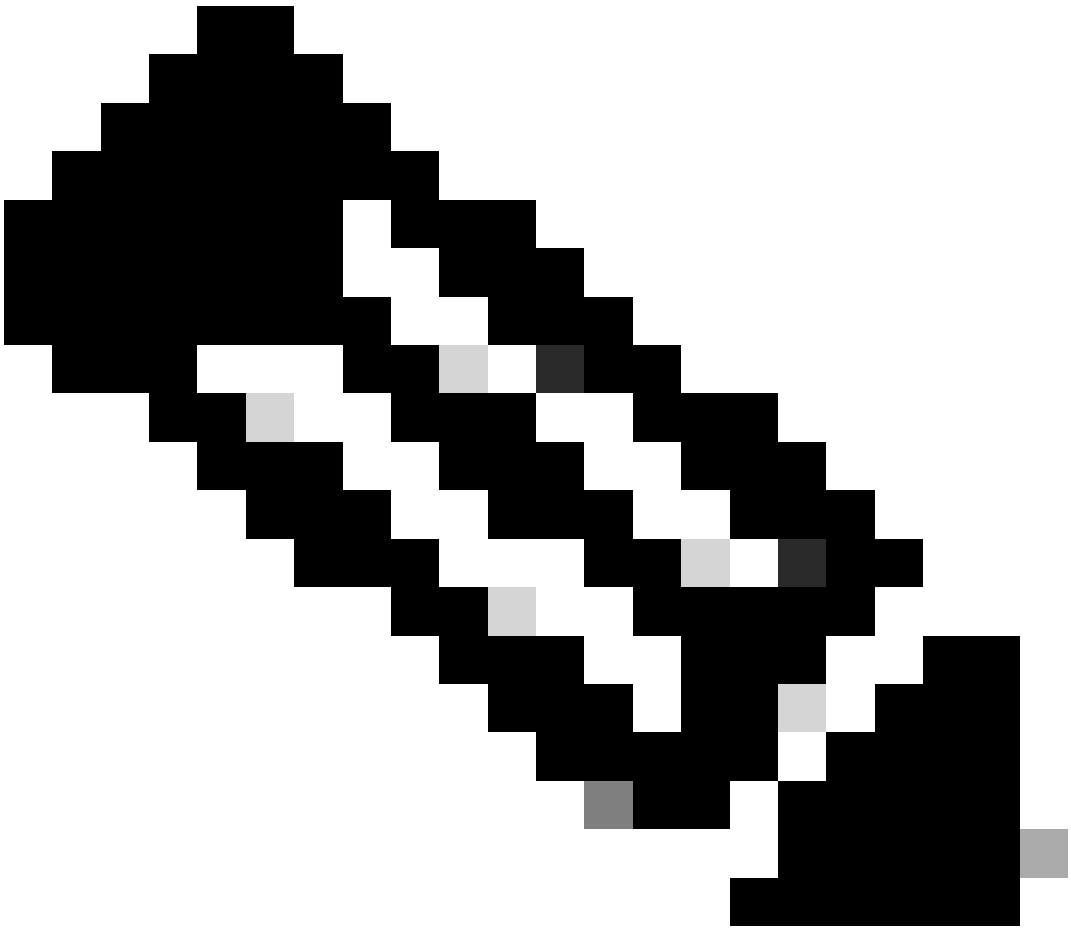
Description : Function: CIPsecProtocol::initiateTunnel
File: IPsecProtocol.cpp
Line: 613

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.



Note: Nos registros do DART, o ID do IKE é mostrado como 'rIUHKccDRiUtFTATwq', que é a representação ASCII de '724955484B6363445269557446544154771', mostrado como ID remoto na saída de "show crypto session detail".

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Depurações IKEv2 para verificar a negociação entre o gateway e o cliente.

```
Debug crypto condition peer ipv4
```

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

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

Informações Relacionadas

- Guia de configuração de segurança e VPN, Cisco IOS XE 17.x
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.