Comprendre les fonctions IKEv2 et AnyConnect Reconnect

Table des matières

Introduction

Ce document décrit comment la fonction de reconnexion automatique IKEv2 fonctionne sur les routeurs Cisco IOS® et Cisco IOS® XE pour AnyConnect.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Catalyst 8000V (C8000V) version 17.16.01a
- Client sécurisé Cisco version 5.1.8.105
- PC client avec Cisco Secure Client installé

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Fonctionnalité de reconnexion IKEv2 et Cisco Secure Client

La fonction de reconnexion automatique du client sécurisé Cisco lui permet de mémoriser la session pendant un certain temps et de reprendre la connexion après avoir établi le canal sécurisé. Comme le client sécurisé Cisco est largement utilisé avec IKEv2 (Internet Key Exchange Version 2), IKEv2 étend la prise en charge de la fonctionnalité de reconnexion automatique sur le logiciel Cisco IOS via la prise en charge de la fonctionnalité de reconnexion automatique de la fonctionnalité de client sécurisé par IKEv2.

La reconnexion automatique dans le client sécurisé Cisco se produit dans les scénarios suivants :

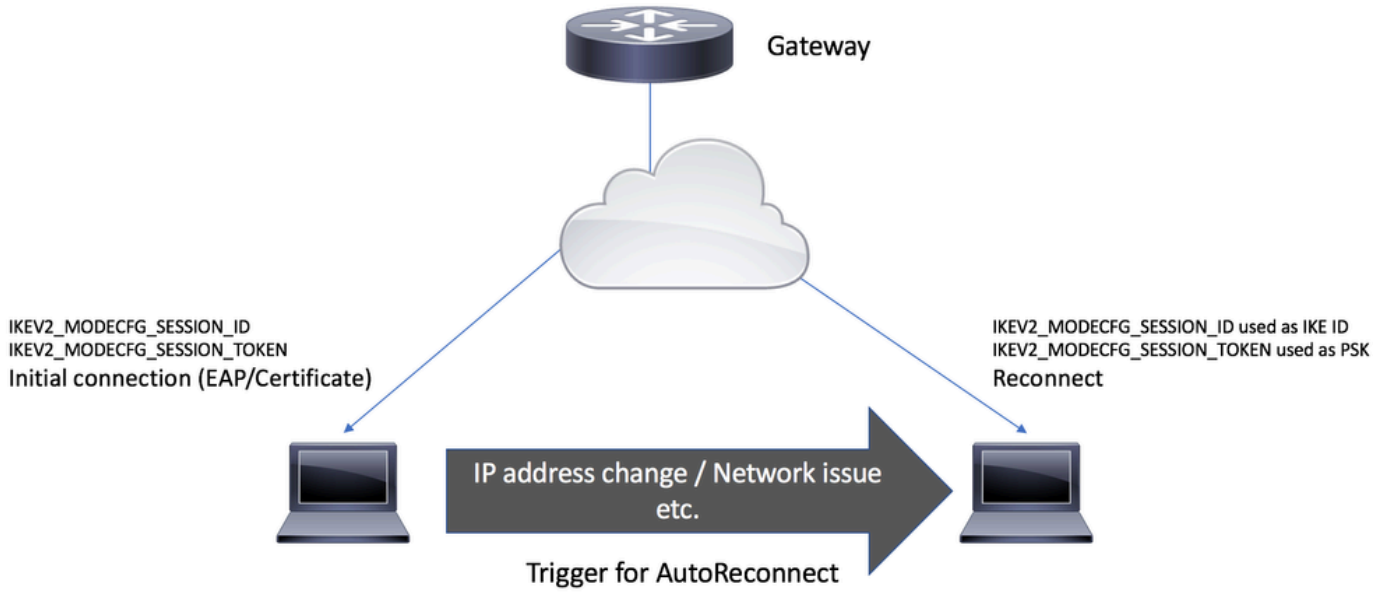
1. Le réseau intermédiaire est en panne. Le client sécurisé Cisco tente de reprendre la session lorsqu'elle est active.
2. Le périphérique Cisco Secure Client bascule entre les réseaux. Il en résulte une modification du port source, ce qui entraîne la désactivation de l'association de sécurité existante et, par conséquent, le client sécurisé Cisco tente de reprendre l'association de sécurité à l'aide de la fonction de reconnexion automatique.
3. Le périphérique Cisco Secure Client tente de reprendre sa SA après être revenu du mode veille ou veille prolongée.

Avantages de la fonction de reconnexion automatique

- Les attributs de configuration utilisés dans la session d'origine sont réutilisés sans interroger le serveur AAA (Authentication, Authorization, and Accounting).
- La passerelle IKEv2 n'a pas besoin de contacter le serveur RADIUS pour se reconnecter au client.
- Aucune interaction utilisateur n'est nécessaire pour l'authentification ou l'autorisation lors de la reprise de la session.
- La méthode d'authentification est la clé pré-partagée lors de la reconnexion d'une session. Cette méthode d'authentification est rapide par rapport aux autres méthodes d'authentification.
- La méthode d’authentification par clé pré-partagée permet de reprendre une session sur le

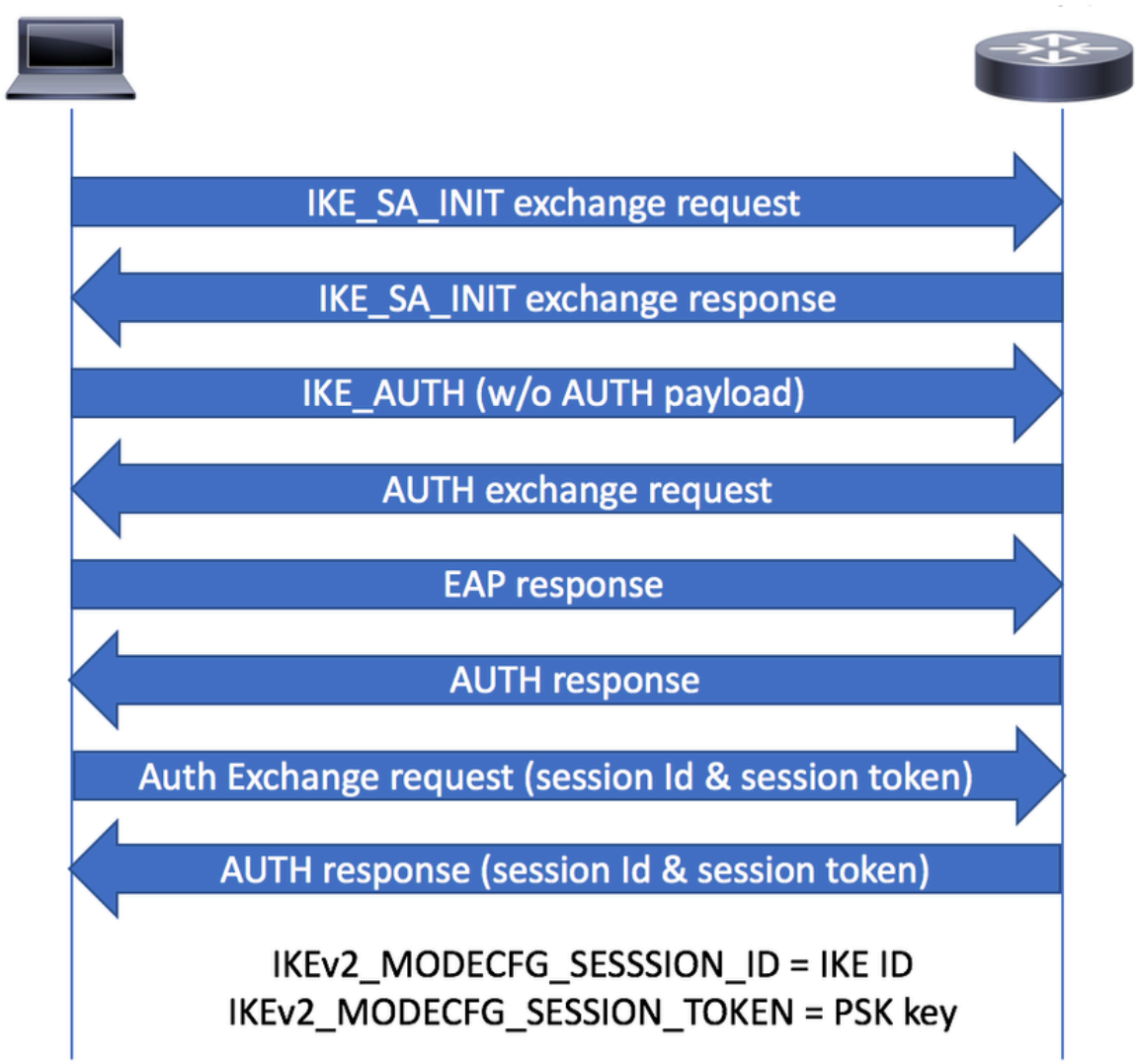
logiciel Cisco IOS avec un minimum de ressources.
- Les associations de sécurité (SA) inutilisées sont supprimées, libérant ainsi les ressources de chiffrement.

Flux de reconnexion automatique

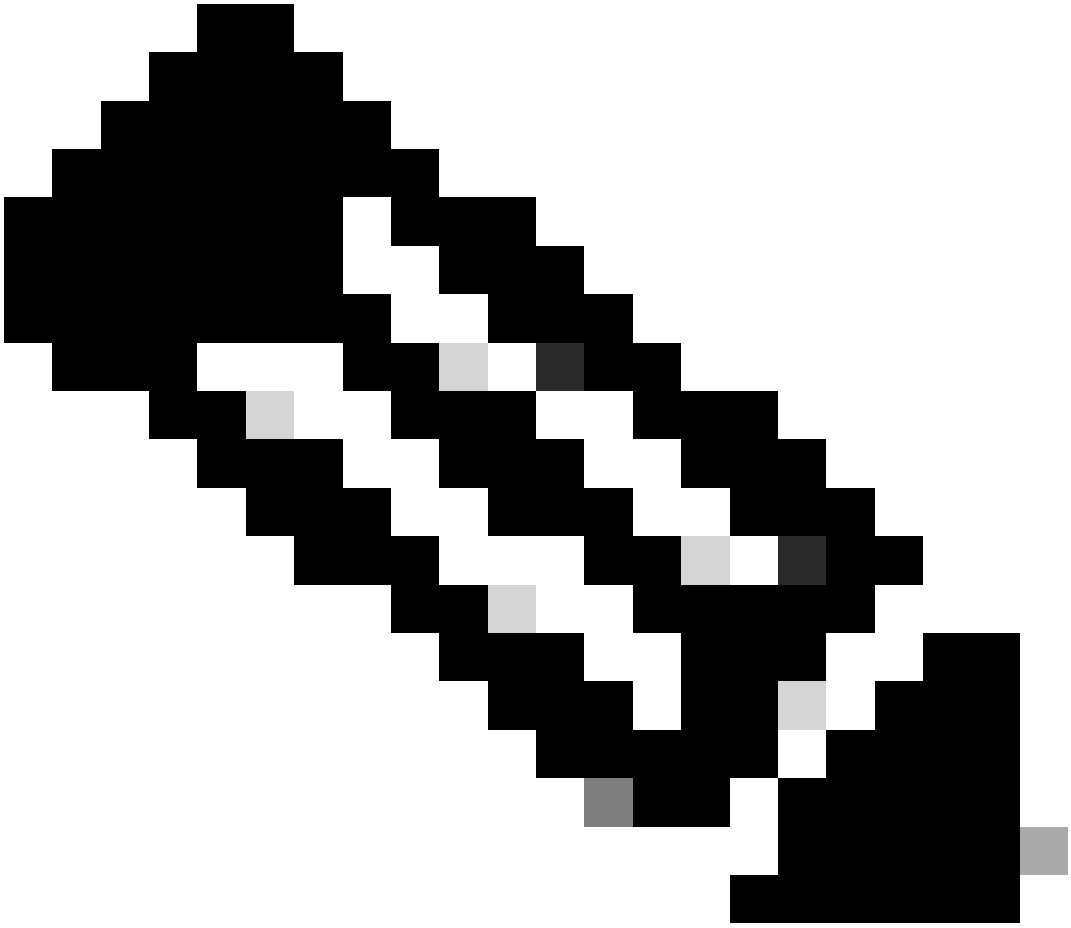


Déclencheur de la reconnexion automatique

1. Au cours de l'échange AUTH, Cisco Secure Client demande l'attribut Session-token et Session-id à partir de la passerelle IKEv2 dans la charge utile MODECFG_REQ de la requête IKE_AUTH.
2. La passerelle IKEv2 vérifie si la prise en charge par Cisco IOS IKEv2 de la fonctionnalité de reconnexion automatique du client sécurisé est activée dans le profil IKEv2 à l'aide de la commande reconnect, sélectionne la stratégie IKEv2 du profil IKEv2 choisi et envoie l'ID de session et les attributs de jeton de session au client sécurisé dans la charge utile CFGMODE_REPLY de la réponse IKE_AUTH.



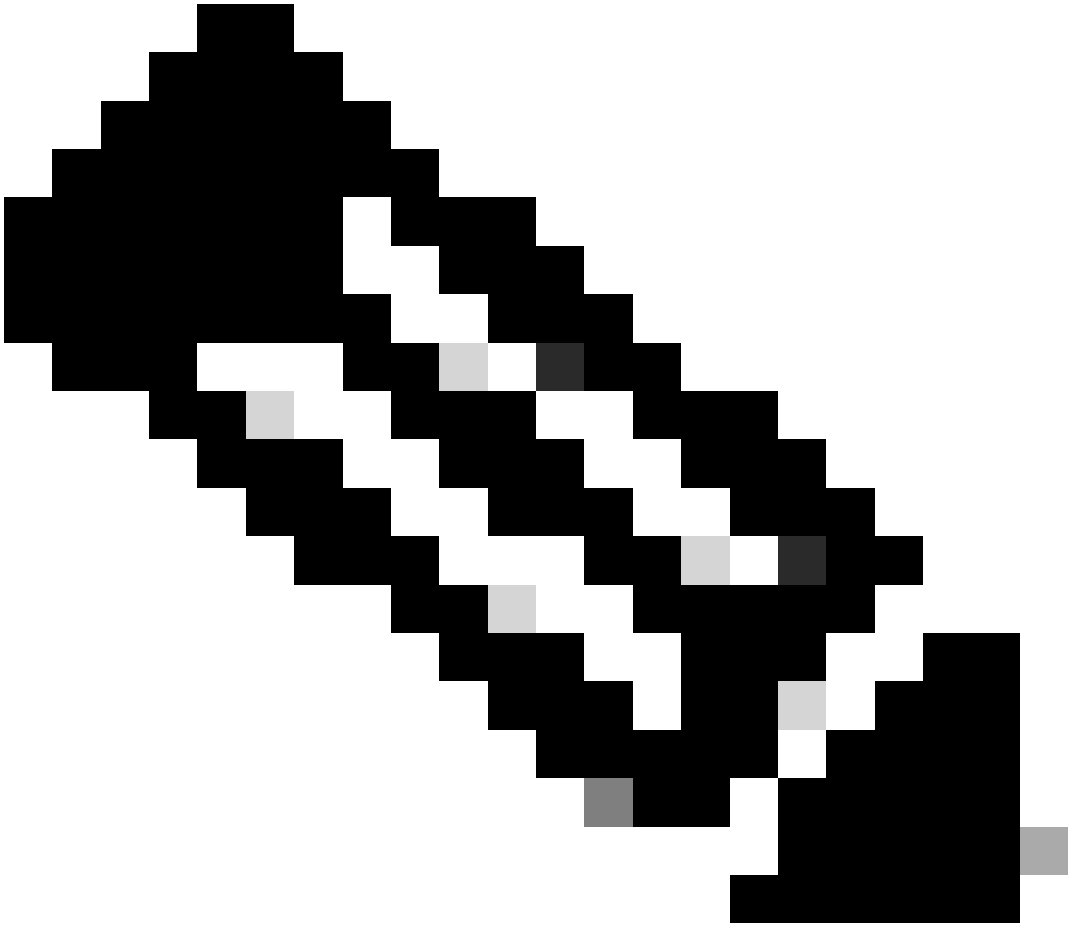
Échange CFGMODE



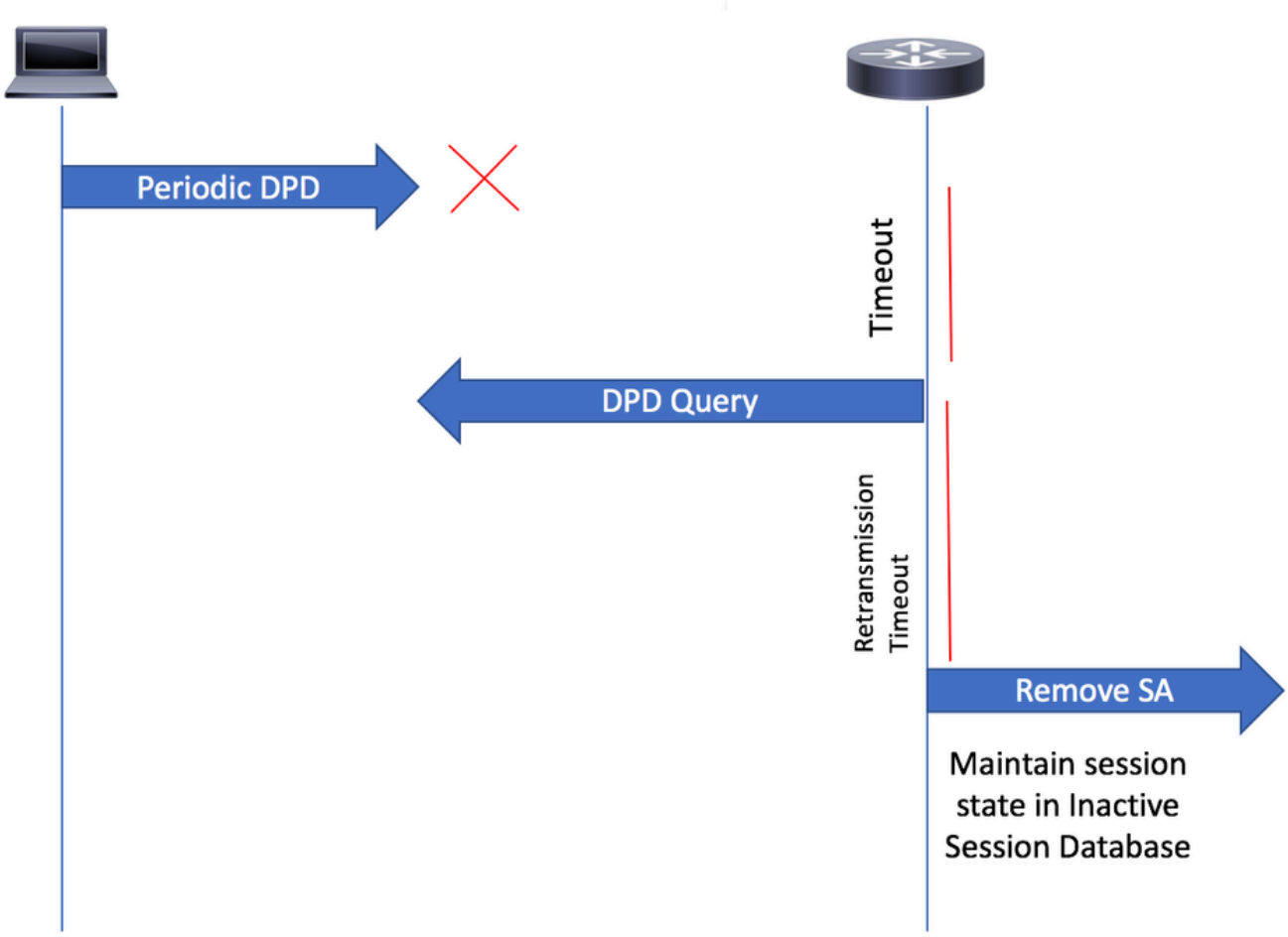
Remarque : Le processus d'identification des clients ne répondant pas est basé sur la détection des homologues morts (DPD). Si la fonction de reconnexion est activée dans le profil IKEv2, vous n'avez pas besoin de configurer DPD, car DPD est mis en file d'attente en tant que protocole à la demande dans IKEv2

---

3. Le client sécurisé Cisco envoie régulièrement des messages DPD à la passerelle. Si DPD est mis en file d'attente à la demande, la passerelle n'envoie pas de messages DPD au client tant qu'elle n'a pas reçu DPD du client. Si DPD n'est pas reçu du client sécurisé dans le délai spécifié (selon l'intervalle DPD configuré), la passerelle envoie un message DPD. Si aucune réponse n'est reçue du client sécurisé, l'association de sécurité est supprimée de la base de données de session active.



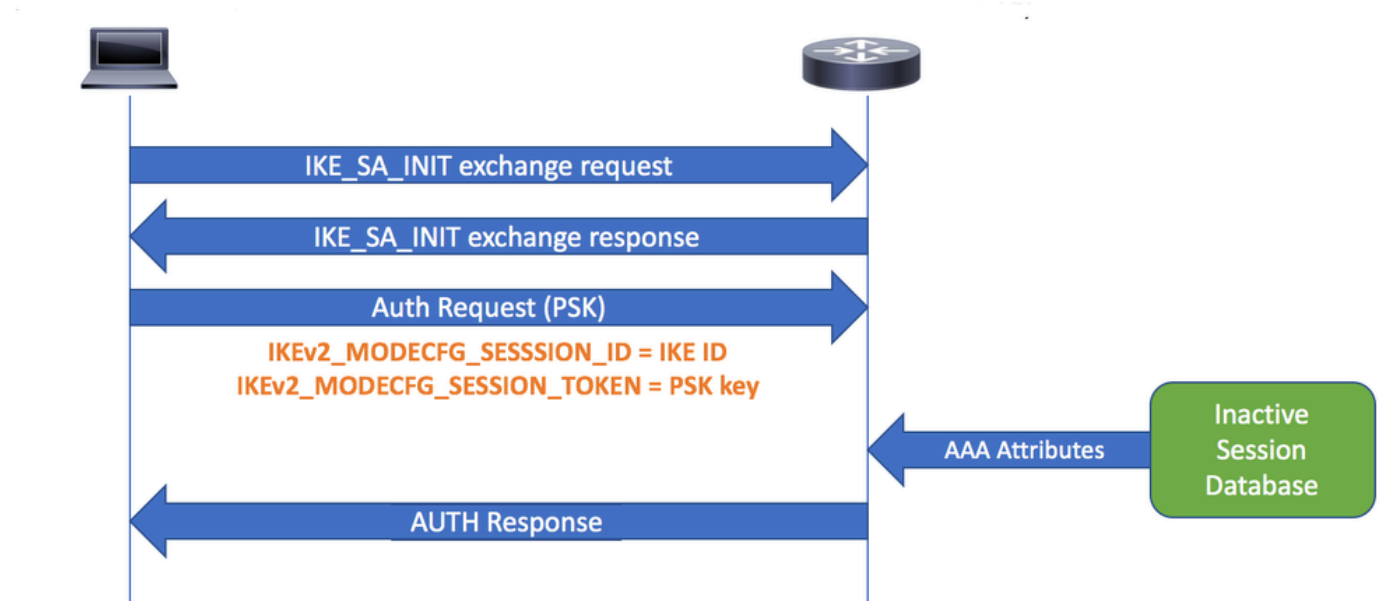
Remarque : Le modem routeur conserve toujours l'état de session (par exemple, les attributs AAA) dans une base de données de session inactive distincte pour permettre la reconnexion conformément au délai d'expiration de reconnexion configuré.



Requête DPD

4. Lorsque le client tente de se reconnecter, il crée une nouvelle association de sécurité IKE et utilise l'identité (ID) IKE comme ID de session, qu'il a reçue de la charge utile MODECFG_REPLY. À ce stade, Cisco Secure Client utilise l'authentification IKE PSK pour la reconnexion, la clé pré-partagée étant le jeton de session qu'il a reçu précédemment.

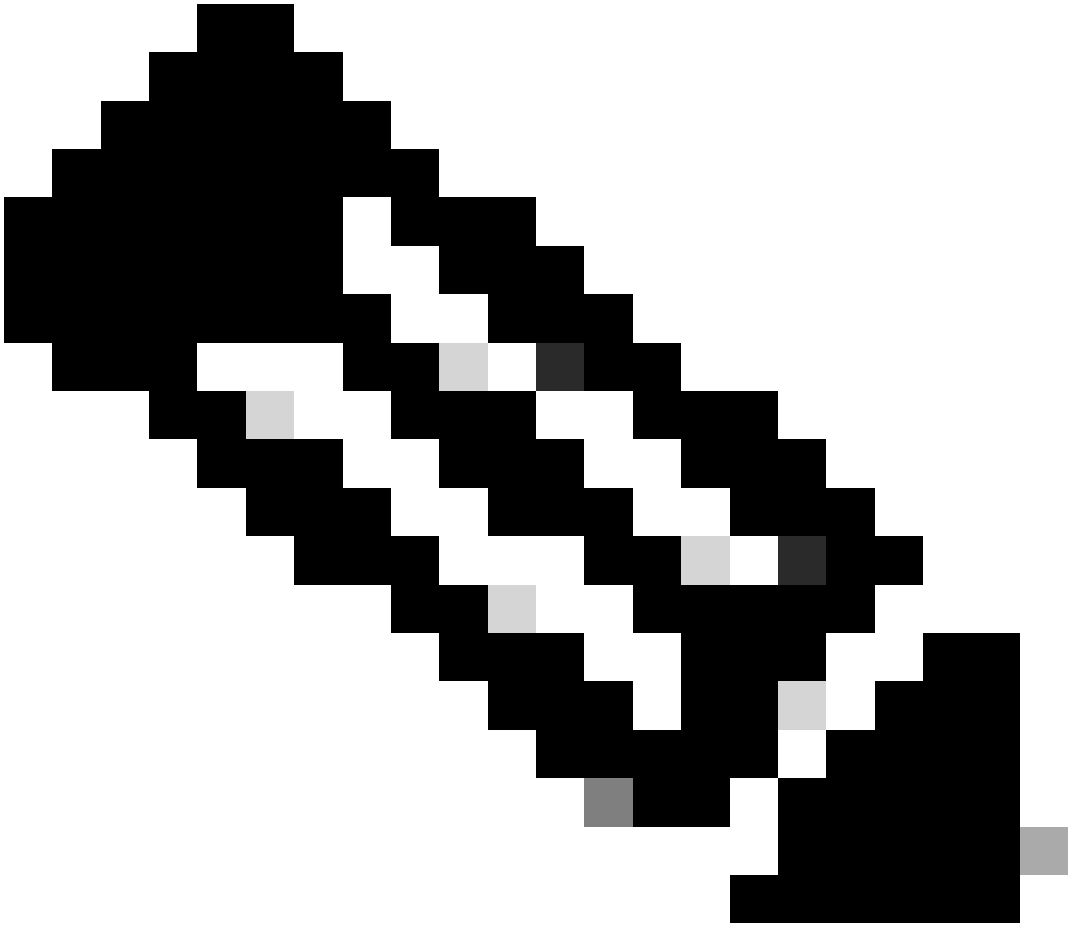
5. Lorsque la passerelle reçoit une demande de reconnexion, elle recherche l'ID IKE homologue (qui sert d'ID de session) dans la base de données de session inactive. Lors de la reconnexion, les attributs personnalisés stockés dans la base de données inactive sont récupérés et appliqués à la nouvelle association de sécurité.



Reconnecter

Configurer

Configuration du routeur



Remarque : Pour la configuration du routeur, vous pouvez également vous référer au document Configure FlexVPN Headend for Secure Client (AnyConnect) IKEv2 Remote Access Using Local User Database

Cet extrait de configuration montre un exemple de configuration de l'accès à distance IKEv2 du client sécurisé Cisco et comment la reconnexion automatique est activée en configurant la reconnexion sous le profil 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
```

Profil de client sécurisé Cisco

<#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>
```

Restrictions de configuration de la reconnexion IKEv2

1. La méthode d'autorisation de clé pré-partagée ne peut pas être configurée sur le profil IKEv2 (Internet Key Exchange Version 2). En effet, la prise en charge par Cisco IOS IKEv2 de la fonctionnalité AutoReconnect de Cisco Secure Client utilise la méthode d'autorisation de clé pré-partagée et la configuration de la clé pré-partagée sur le même profil IKEv2 peut être source de confusion.
2. Ces commandes ne peuvent pas être configurées sur le profil IKEv2 :

- authentication local pre-share
- authentication remote pre-share
- porte-clés, psk de groupe d'autorisation aaa
- aaa authorization user psk

Vérifier

<#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
```

Ce résultat montre qu'il y a actuellement 1 session active qui est capable de reconnexion automatique :

```
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
```

Après reconnexion

Lorsque le client sécurisé Cisco se reconnecte, il utilise l'ID IKE IKEV2_MODECFG_SESSION_ID. Par conséquent, après la reconnexion, Phase1_id n'est plus $AnyConnectClient$; il s'agit plutôt de l'ID de session, comme indiqué. En outre, notez que les fonctionnalités sont désormais définies sur R. Ici, R indique qu'il s'agit d'une session de reconnexion.

<#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
```

Après la reconnexion, la méthode d'authentification est désormais PSK (clé pré-partagée) au lieu d'AnyConnect-EAP, comme indiqué :

<#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#

Journaux DART du client sécurisé Cisco

<#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

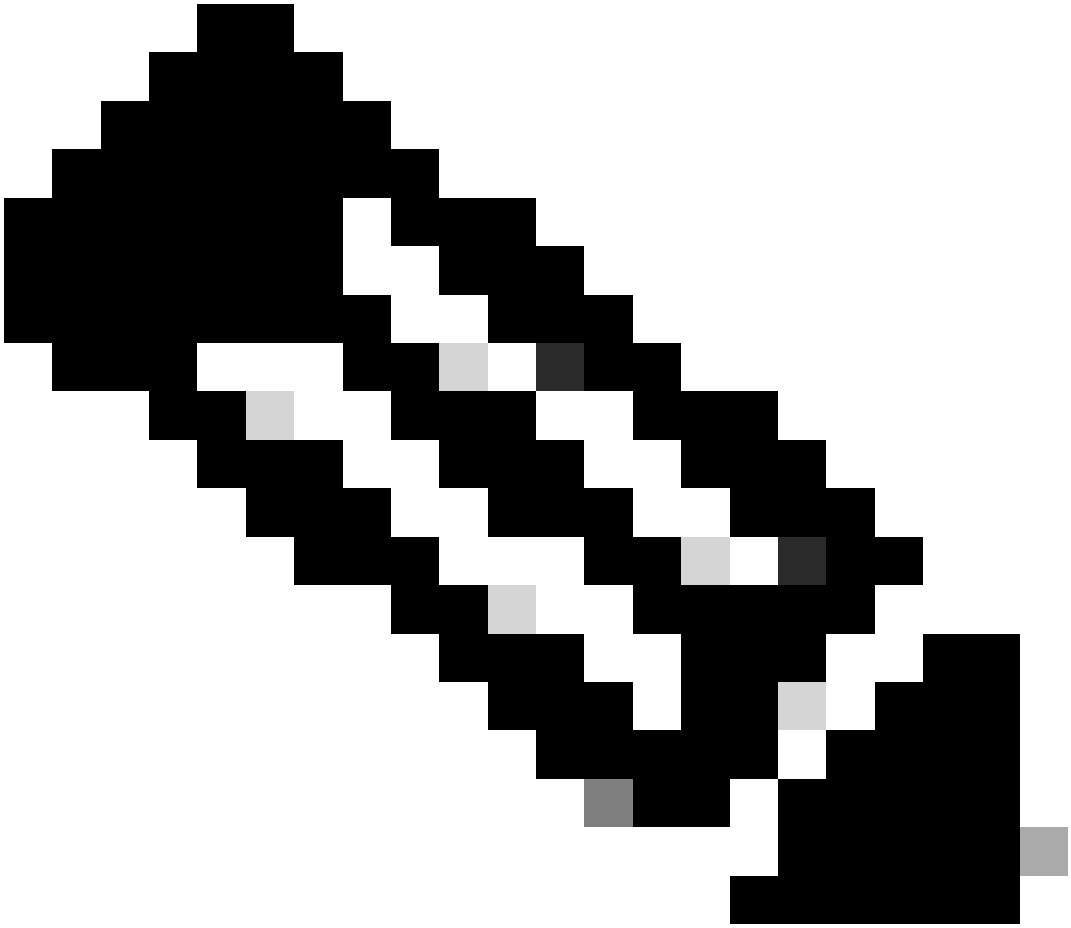
Using IKE ID 'rIUHKccDRiUtFTATwq' for reconnect

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

```
Type        : Information
Source      : acvpnui

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

Connected to IKEv2_Gateway.



Remarque : Dans les journaux DART, l'ID IKE est affiché sous la forme 'rIUHKccDRiUtFTATwq', qui est la représentation ASCII de '724955484B6363445269557446544154771', affichée sous la forme d'ID distant dans le résultat de "show crypto session detail".

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Débogues IKEv2 pour vérifier la négociation entre la passerelle et le client.

```
Debug crypto condition peer ipv4
```

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

Informations connexes

- Guide de configuration de la sécurité et du VPN, Cisco IOS XE 17.x
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.