Configurer un VPN SSL AnyConnect sur C8000v avec authentification locale

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Diagramme du réseau
- Configurations

Flux de connexion

- Flux de connexion de haut niveau Cisco Secure Client (AnyConnect) vers C8000v

Vérifier

Dépannage

Informations connexes

Introduction

Ce document décrit comment configurer la tête de réseau Cisco IOS XE C8000v pour VPN SSL AnyConnect avec une base de données d'utilisateurs locaux.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco IOS XE
- Cisco Secure Client (CSC)
- Fonctionnement général de SSL
- Infrastructures à clé publique (PKI)

Composants utilisés

ThLes informations contenues dans ce document sont basées sur les versions logicielles et matérielles 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.

Informations générales

Le VPN SSL (Secure Socket Layer) Cisco IOS XE est une solution basée sur routeur offrant une connectivité d'accès à distance VPN SSL intégrée avec des fonctionnalités de sécurité et de routage de pointe sur une plate-forme convergée de données, voix et sans fil. Grâce au VPN SSL de Cisco IOS XE, les utilisateurs finaux peuvent accéder en toute sécurité depuis leur domicile ou n'importe quel site Internet, tel que les points d'accès sans fil. Le VPN SSL de Cisco IOS XE permet également aux entreprises d'étendre l'accès au réseau d'entreprise aux partenaires et consultants offshore, tout en protégeant les données d'entreprise.

Cette fonctionnalité est prise en charge sur les plates-formes indiquées :

Plateforme	Version prise en charge de Cisco IOS XE
Routeur de services cloud Cisco, série 1000V	Cisco IOS XE version 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bangalore 17.4.1
Routeur à services intégrés Cisco 4461 Routeur à services intégrés Cisco 4451 Routeur à services intégrés Cisco 4431	Cisco IOS XE Cupertino 17.7.1a

Configurer

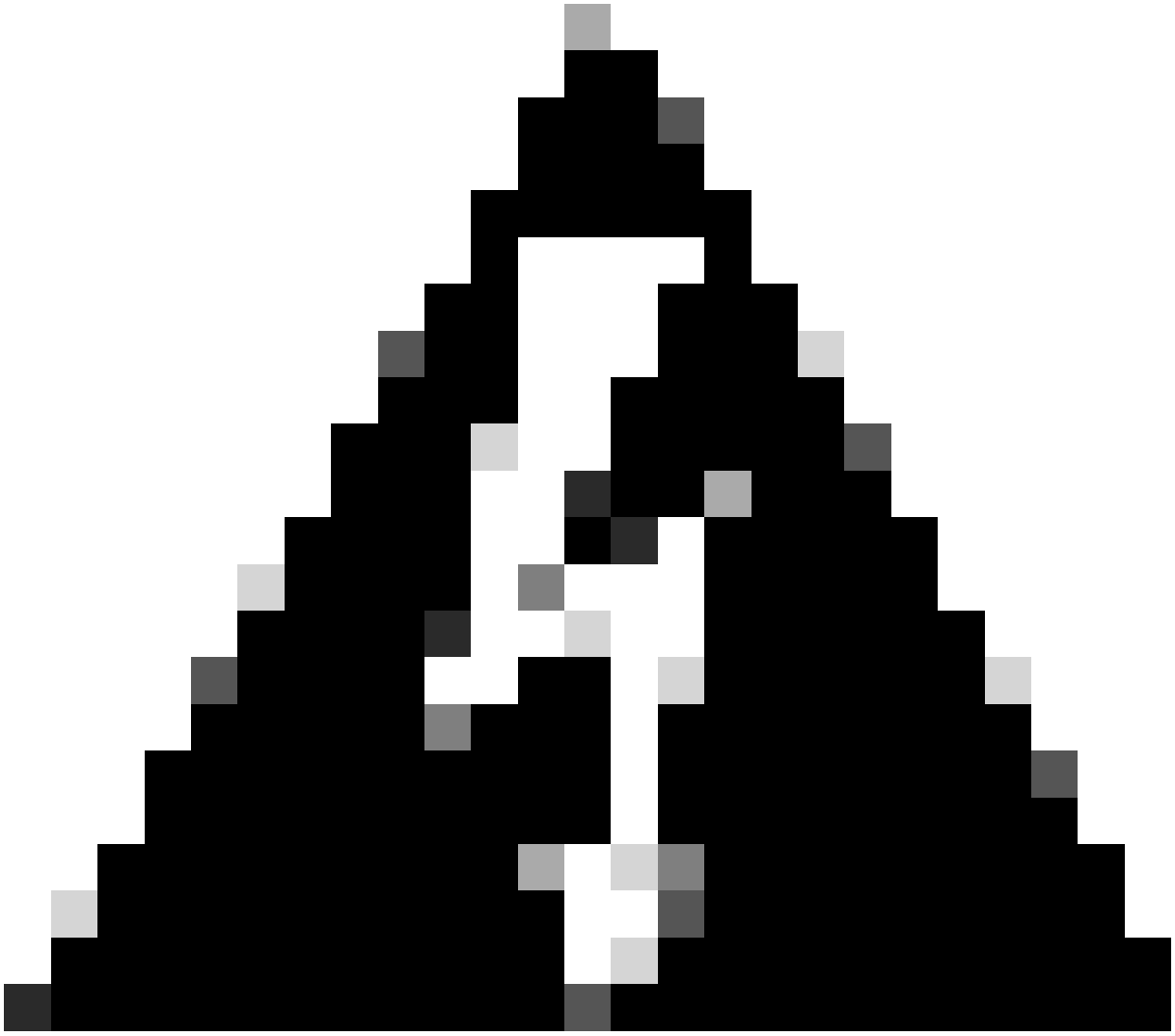
Diagramme du réseau

Schéma de réseau de base

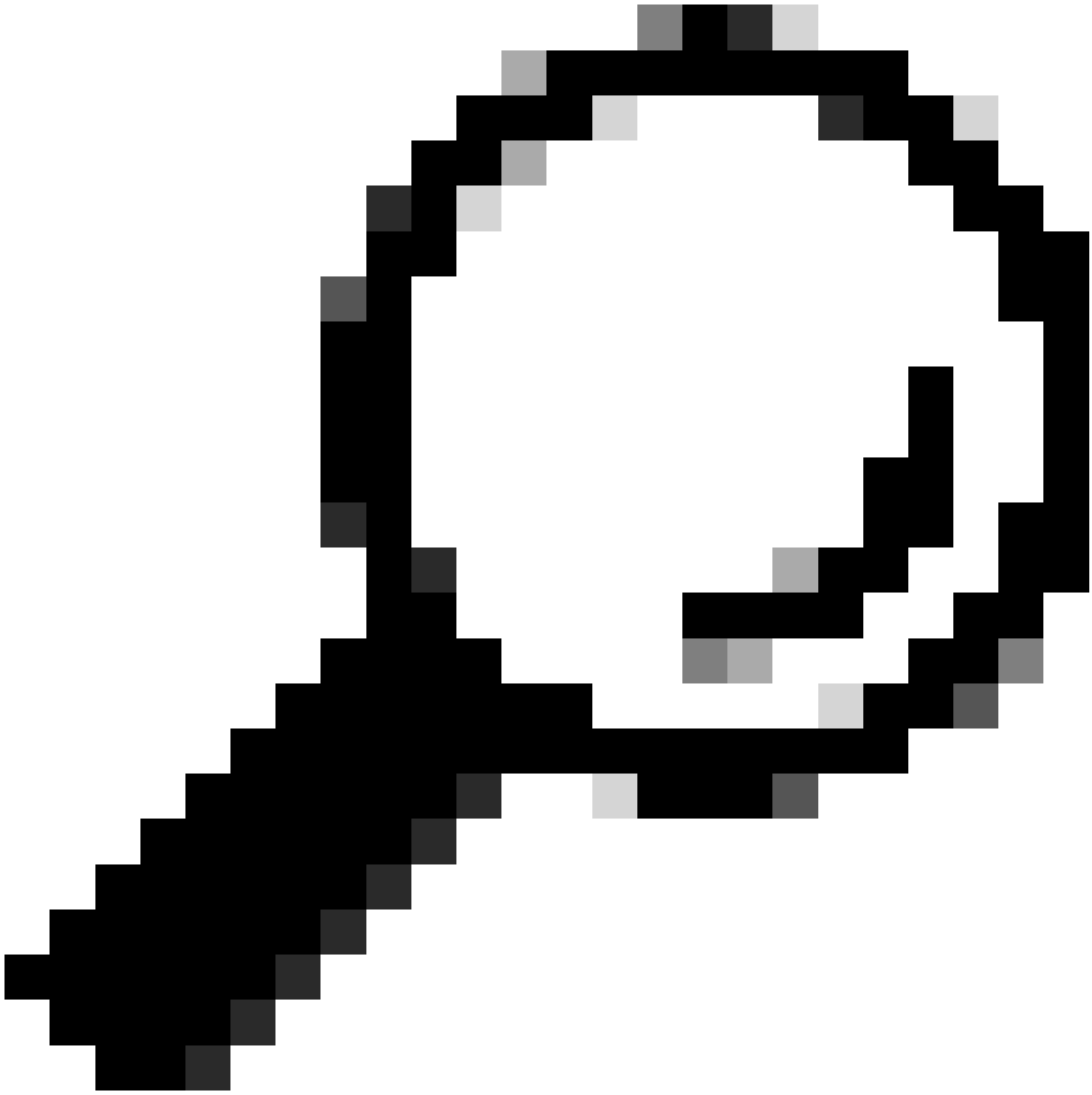
Configurations

1. Activez AAA, configurez l'authentification, les listes d'autorisation et ajoutez un nom d'utilisateur à la base de données locale.

```
aaa new-model
!
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
!
username test password cisco123
```



Avertissement : La commande aaa new-model applique immédiatement l'authentification locale à toutes les lignes et interfaces (excepté la ligne de console line con 0). Si une session Telnet est ouverte vers le routeur après l’activation de cette commande (ou si une connexion expire et doit être reconnectée), l’utilisateur doit s’authentifier avec la base de données locale du routeur. Il est recommandé de définir un nom d'utilisateur et un mot de passe sur le routeur avant de commencer la configuration AAA, afin de ne pas être verrouillé hors du routeur.



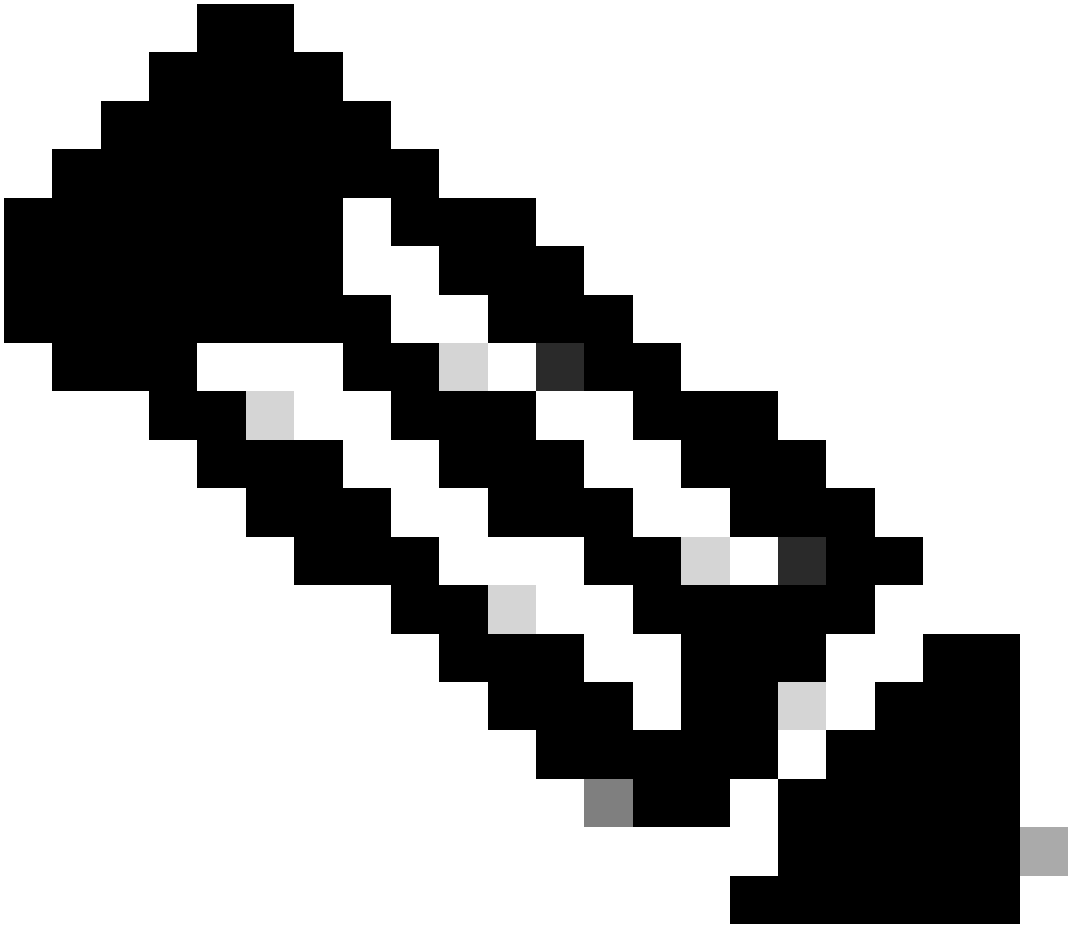
Conseil : Avant de configurer vos commandes AAA, enregistrez votre configuration. Vous pouvez enregistrer à nouveau la configuration après avoir terminé votre configuration du protocole AAA (et vous être assuré qu'elle fonctionne correctement). Cela vous permet de vous rétablir d'un verrouillage inattendu, car vous pouvez annuler toute modification en rechargeant le routeur.

2.Generate Rivest-Shamir-Adleman (RSA) Keypair.

```
crypto key generate rsa label AnyConnect modulus 2048 exportable
```

3. Créez un point de confiance pour installer le certificat d'identité du routeur. Vous pouvez consulter la section Comment configurer l'inscription de certificat pour une ICP pour plus de détails sur la création du certificat.

```
crypto pki trustpoint TP_AnyConnect
enrollment terminal
fqdn sslvpn-c8kv.example.com
subject-name cn=sslvpn-c8kv.example.com
subject-alt-name sslvpn-c8kv.example.com
revocation-check none
rsakeypair AnyConnect
```



Remarque : Le nom commun (CN) du nom de l'objet doit être configuré avec l'adresse IP ou le nom de domaine complet (FQDN) que les utilisateurs utilisent pour se connecter à la passerelle sécurisée (C8000V). Bien que ce ne soit pas obligatoire, la saisie correcte du

---

CN peut aider à réduire le nombre d'erreurs de certificat rencontrées par les utilisateurs lors de la connexion.

4. Définissez un pool local IP pour attribuer des adresses au client sécurisé Cisco.

```
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
```

5. (Facultatif) Configurez une liste d'accès standard à utiliser pour le split-tunnel. Cette liste d'accès comprend les réseaux de destination accessibles via le tunnel VPN. Par défaut, tout le trafic passe par le tunnel VPN (Full Tunnel) si le tunnel partagé n'est pas configuré.

```
ip access-list standard split-tunnel-acl
10 permit 192.168.11.0 0.0.0.255
20 permit 192.168.12.0 0.0.0.255
```

6.Désactivez le serveur sécurisé HTTP.

```
no ip http secure-server
```

7. Configurez une proposition SSL.

```
crypto ssl proposal ssl_proposal
protection rsa-aes128-sha1 rsa-aes256-sha1
```

8. Configurez une stratégie SSL, appelez la proposition SSL et le point de confiance PKI.

```
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
```

La stratégie SSL définit la proposition et le point de confiance à utiliser lors de la négociation SSL. Il sert de conteneur pour tous les paramètres impliqués dans la négociation SSL. La sélection de stratégie est effectuée en comparant les paramètres de session à ceux configurés sous la stratégie.

9. (Facultatif) Créez un profil AnyConnect à l'aide de l'Éditeur de profil client sécurisé Cisco [Éditeur de profil client sécurisé Cisco](#) . Un extrait de l'équivalent XML du profil est fourni à titre de référence.

<#root>

```
        true

        true

        false
```

All

All

All

false

Native

```
true
```

```
30
```

```
false
```

```
true
```

false

false

true

IPv4,IPv6

true

ReconnectAfterResume

false

true

Automatic

SingleLocalLogon

SingleLocalLogon

AllowRemoteUsers

LocalUsersOnly

false

Disable

false

false

20

4

```
false
```

```
false
```

```
true
```

SSL_C8KV

sslvpn-c8kv.example.com

10. Téléchargez le profil XML créé dans la mémoire flash du routeur et définissez le profil :

```
crypto vpn anyconnect profile acvpn bootflash:/acvpn.xml
```

11.Désactivez le serveur sécurisé HTTP.

```
no ip http secure-server
```

12. Configurez la stratégie d'autorisation SSL.

```
crypto ssl authorization policy ssl_author_policy
client profile acvpn
pool SSLVPN_POOL
dns 192.168.11.100
banner Welcome to C8kv SSLVPN
def-domain example.com
route set access-list split-tunnel-acl
```

La stratégie d'autorisation SSL est un conteneur de paramètres d'autorisation qui sont transmis au client distant.La stratégie d'autorisation est référencée à partir du profil SSL.

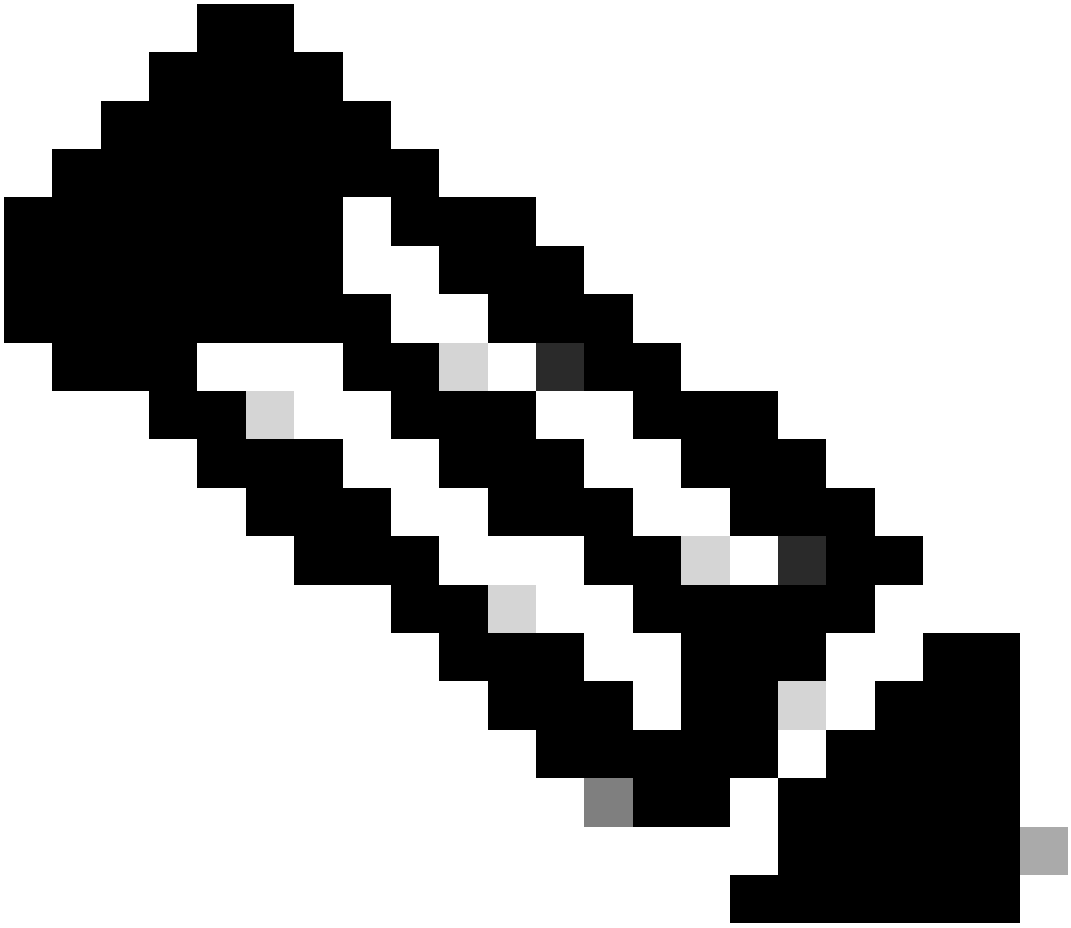
13. Configurez un modèle virtuel à partir duquel les interfaces d’accès virtuel sont clonées.

```
interface Virtual-Template2 type vpn
ip unnumbered GigabitEthernet1
ip mtu 1400
ip tcp adjust-mss 1300
```

14. Configurez un profil SSL et définissez l'authentification , les listes de gestion et le modèle virtuel.

```
crypto ssl profile ssl_prof
match policy ssl_policy
match url https://sslvpn-c8kv.example.com
aaa authentication user-pass list SSLVPN_AUTHEN
aaa authorization group user-pass list SSLVPN_AUTHOR ssl_author_policy
authentication remote user-pass
virtual-template 2
```

La sélection d'un profil dépend de la stratégie et des valeurs d'URL.



Remarque : La stratégie et l'URL doivent être uniques pour un profil VPN SSL, et au moins une méthode d'autorisation doit être spécifiée pour ouvrir la session.

Ils sont utilisés dans le profil SSL :

- match policy - instruction match pour sélectionner un profil SSL ssl_prof pour un client sur le nom de stratégie SSL ssl_policy.
- match url : faites correspondre les instructions pour sélectionner un profil SSL ssl_prof pour un client sur le URL sslvpn-c8kv.example.com.
- aaa authentication user-pass list : pendant l'authentification, la liste SSLVPN_AUTHEN est utilisée.
- aaa authorization group user-pass list - Pendant l'autorisation, la liste réseau SSLVPN_AUTHOR est utilisée avec la politique d'autorisation ssl_author_policy.
- authentication remote user-pass : définit le mode d'authentification du client distant en fonction du nom d'utilisateur et du mot de passe.
- virtual-template 2 : définit le modèle virtuel à cloner.

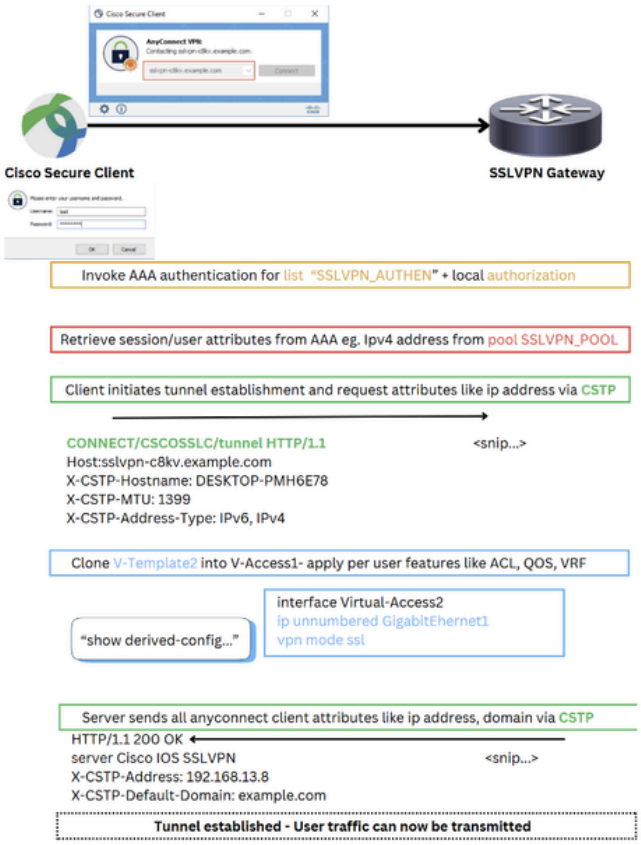
Flux de connexion

Pour comprendre les événements qui se produisent entre le client sécurisé Cisco et la passerelle sécurisée au cours de l'établissement d'une connexion VPN SSL, référez-vous au document [Présentation du flux de connexion VPN SSL AnyConnect]

Flux de connexion de haut niveau Cisco Secure Client (AnyConnect) vers C8000v


```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
!
crypto ssl profile my-profile
match policy ssl_policy
match url https://sslvpn-c8kv.example.com
aaa authentication user-pass list SSLVPN_AUTHEN
aaa authorization group user-pass list SSLVPN_AUTHOR ssl_author_policy
authentication remote user-pass
virtual-template 2
!
crypto ssl authorization policy ssl_author_policy
pool SSLVPN_POOL
def domain example.com
!
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
interface Virtual-Template2 type vpn
  ip unnumbered GigabitEthernet1
  ip mtu 1400
  vpn mode ssl
```

Flux de connexion de haut niveau 1

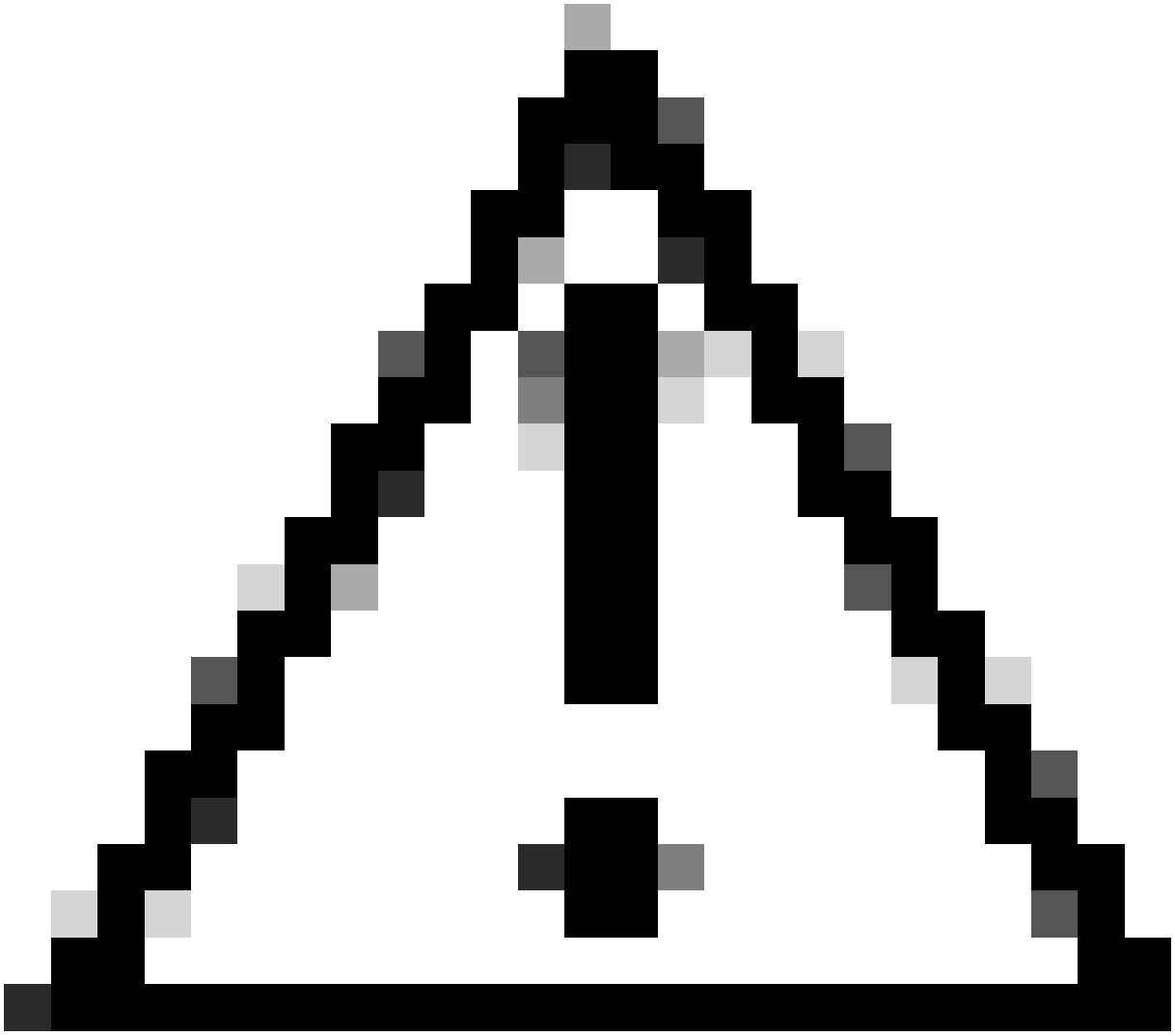



```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
!
crypto ssl profile my-profile
match policy ssl_policy
match url https://sslvpn-c8kv.example.com
aaa authentication user-pass list SSLVPN_AUTHEN
aaa authorization group user-pass list SSLVPN_AUTHOR ssl_author_policy
authentication remote user-pass
virtual-template 2
!
crypto ssl authorization policy ssl_author_policy
pool SSLVPN_POOL
def domain example.com
!
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
interface Virtual-Template2 type vpn
  ip unnumbered GigabitEthernet1
  ip mtu 1400
  vpn mode ssl
```

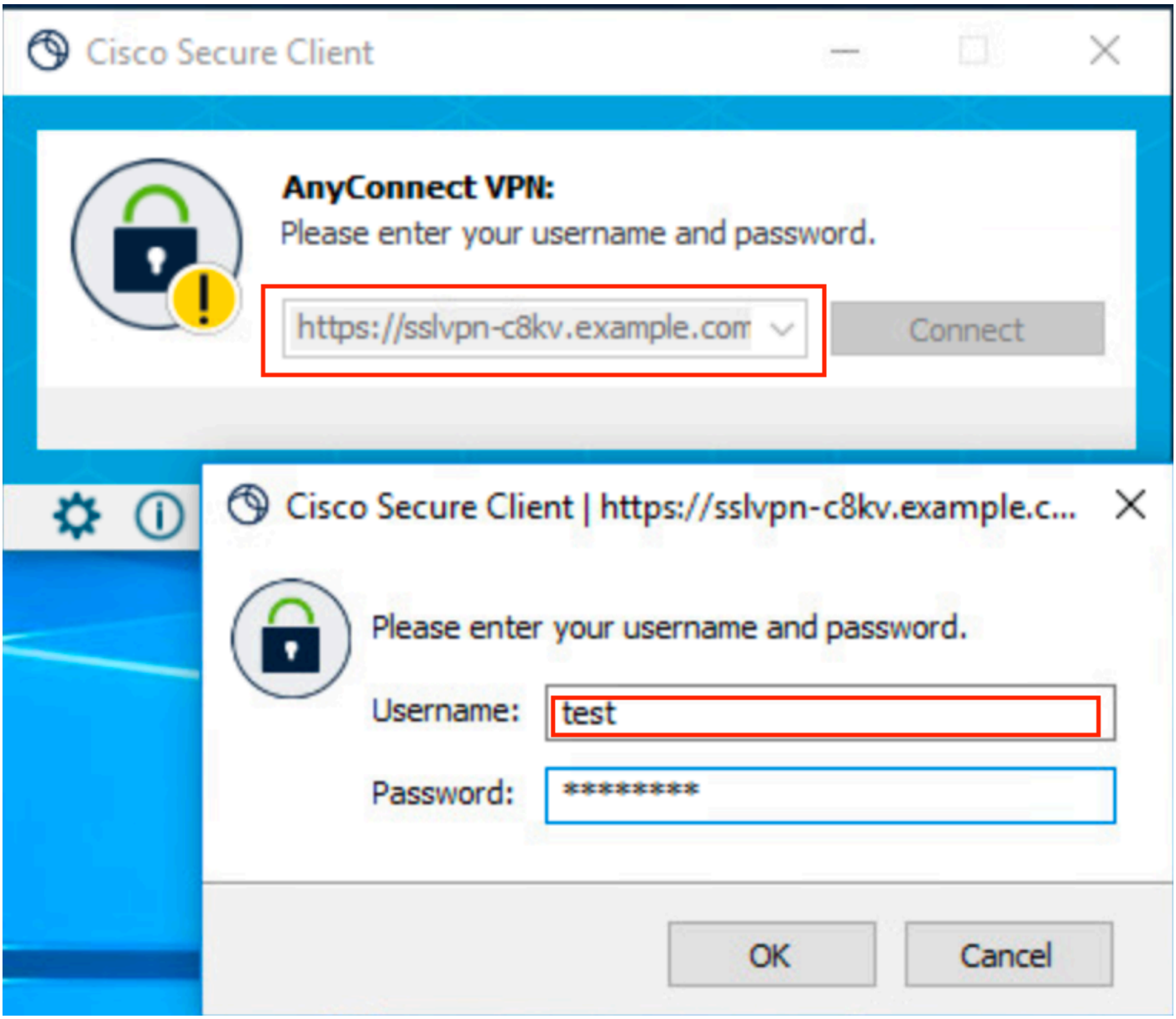
Flux de connexion de haut niveau 2

Vérifier

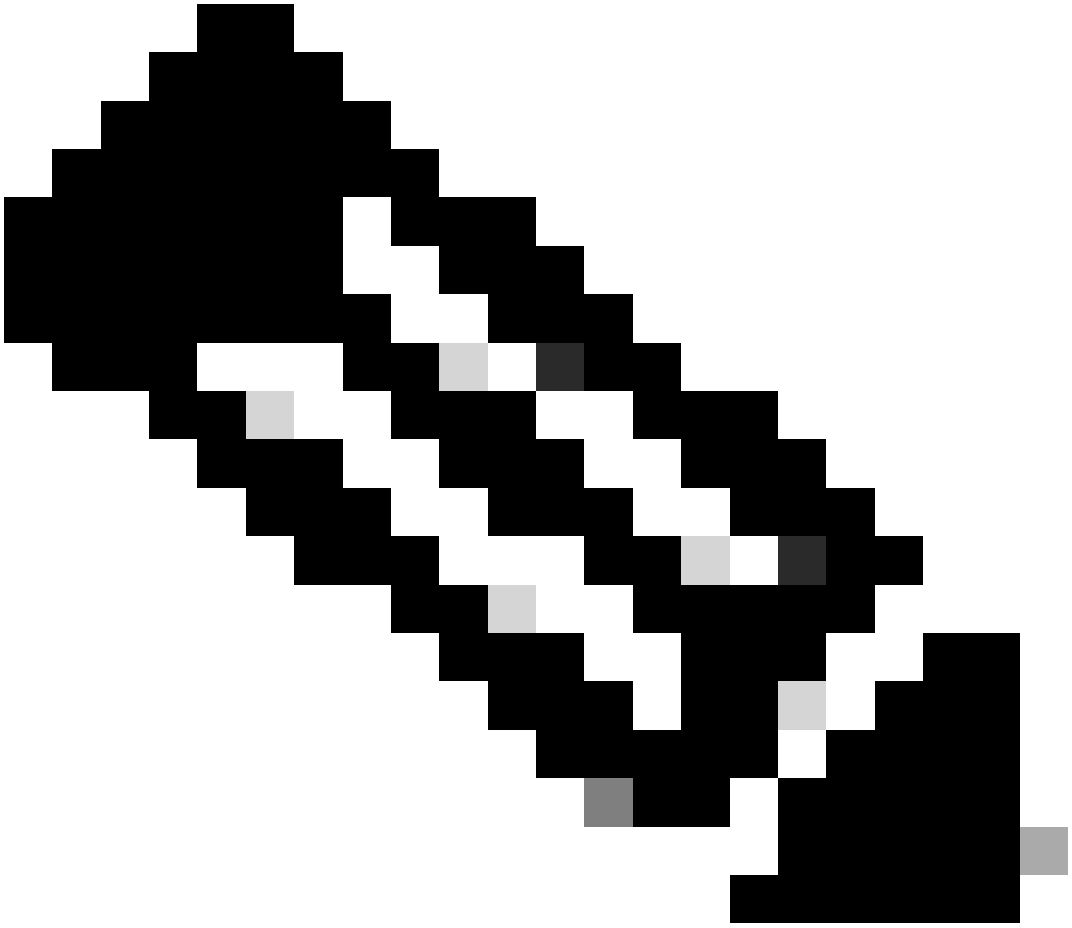
1. Afin de tester l'authentification, connectez-vous à partir du client sécurisé Cisco avec le nom de domaine complet (FQDN) ou l'adresse IP C8000v, et entrez les informations d'identification.



Mise en garde : C8000v ne prend pas en charge le téléchargement de logiciels clients depuis la tête de réseau. Cisco Secure Client doit être préinstallé sur l'ordinateur.



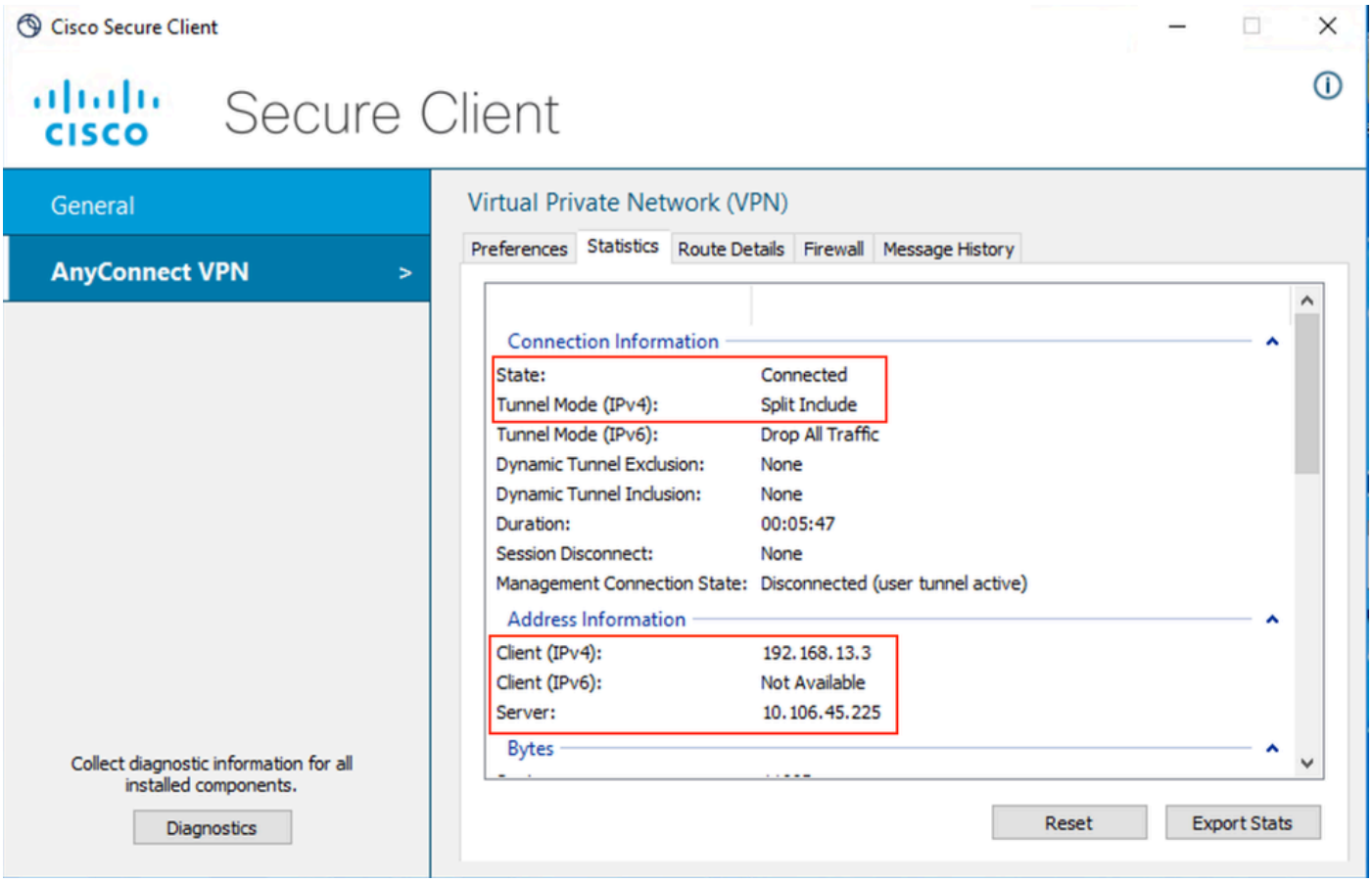
Tentative de connexion du client sécurisé Cisco



Remarque : avec une nouvelle installation du client sécurisé Cisco (sans ajout de profils XML), l'utilisateur peut entrer manuellement le nom de domaine complet de la passerelle VPN dans la barre d'adresse du client sécurisé Cisco. Après une connexion réussie, le client sécurisé Cisco tente de télécharger le profil XML par défaut. Cependant, Cisco Secure Client doit être redémarré pour que le profil apparaisse dans l'interface utilisateur graphique. La simple fermeture de la fenêtre Cisco Secure Client ne suffit pas. Pour redémarrer le processus, cliquez avec le bouton droit sur l'icône Cisco Secure Client dans la barre d'état système de Windows et sélectionnez l'option Quit.

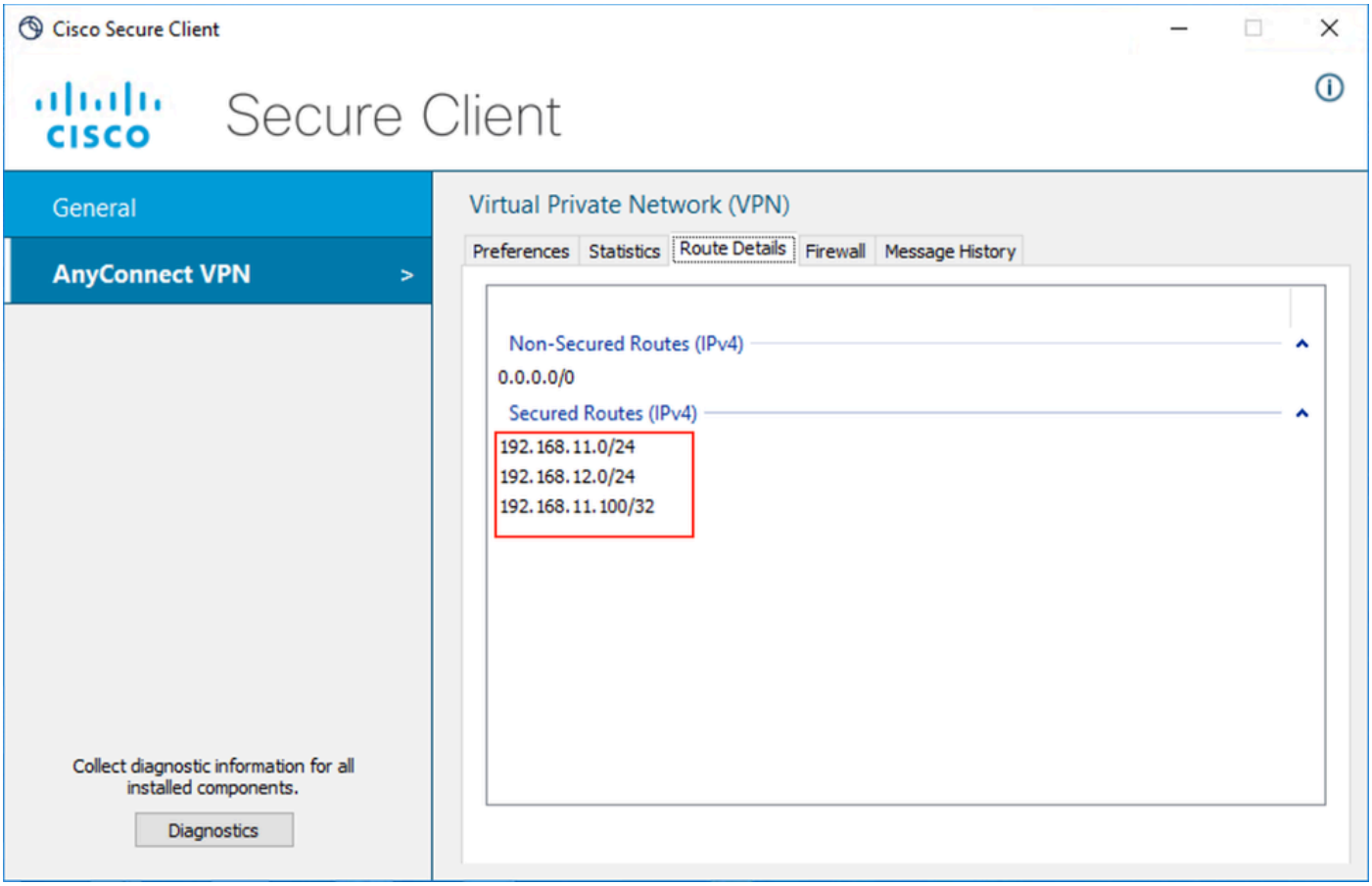
---

2. Une fois la connexion établie, cliquez sur l'icône engrenage dans le coin inférieur gauche et accédez à AnyConnect VPN > Statistics. Vérifiez que les informations affichées correspondent aux informations de connexion et d'adresse.



Statistiques Cisco Secure Client (AnyConnect)

3. Accédez à AnyConnect VPN > Détails de la route et confirmer que les informations affichées correspondent aux routes sécurisées et aux routes non sécurisées.



Détails de la route Cisco Secure Client (AnyConnect)

Utilisez cette section afin de confirmer que votre configuration fonctionne correctement sur C8000v :

1. Pour afficher les informations de session SSL - show crypto ssl session{user user-name |profile profile-name}

<#root>

```
sal_c8kv#show crypto ssl session user test


Interface :
Virtual-Access1

Session Type : Full Tunnel
Client User-Agent : AnyConnect Windows 5.1.8.105

Username : test                         Num Connection : 1
Public IP : 10.106.69.69
Profile :
ssl_prof

Policy :
```

```
ssl_policy


Last-Used : 00:41:40                    Created : *15:25:47.618 UTC Mon Mar 3 2025
Tunnel IP : 192.168.13.3                Netmask : 0.0.0.0
Rx IP Packets : 542                     Tx IP Packets : 410


sal_c8kv#show crypto ssl session profile ssl_prof


SSL profile name: ssl_prof
Client_Login_Name  Client_IP_Address No_of_Connections Created   Last_Used
cisco                10.106.69.69             1        00:49:41  00:49:41
```

2. Pour afficher les statistiques ssl vpn - show crypto ssl stats [profile profile-name] [tunnel] [detail]

<#root>

```
sal_c8kv#show crypto ssl stats tunnel profile ssl_prof


SSLVPN Profile name : ssl_prof

Tunnel Statistics:

    Active connections       : 1
    Peak connections         : 1          Peak time               : 1d23h
    Connect succeed          : 13         Connect failed          : 0
    Reconnect succeed        : 0          Reconnect failed        : 0
    IP Addr Alloc Failed     : 0          VA creation failed      : 0
    DPD timeout              : 0

  Client

    in  CSTP frames          : 23         in  CSTP control        : 23
    in  CSTP data            : 0          in  CSTP bytes          : 872
    out CSTP frames          : 11         out CSTP control        : 11
    out CSTP data            : 0          out CSTP bytes          : 88
    cef in  CSTP data frames : 0          cef in  CSTP data bytes : 0
    cef out CSTP data frames : 0          cef out CSTP data bytes : 0

  Server

    In  IP pkts              : 0          In  IP bytes            : 0
    In  IP6 pkts             : 0          In  IP6 bytes           : 0
    Out IP pkts              : 0          Out IP bytes            : 0
    Out IP6 pkts             : 0          Out IP6 bytes           : 0
```

3. Pour vérifier la configuration réelle appliquée pour l'interface d'accès virtuel associée au client.

<#root>

sal_c8kv#show derived-config interface Virtual-Access1

```
Building configuration...

Derived configuration : 143 bytes
!
interface Virtual-Access1
description ***Internally created by SSLVPN context ssl_prof***
ip unnumbered GigabitEthernet1
ip mtu 1400
end
```

Dépannage

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

1. Débogages SSL pour vérifier la négociation entre la tête de réseau et le client.

<#root>

debug crypto ssl condition client username

```
debug crypto ssl aaa
debug crypto ssl aggr-auth message
debug crypto ssl aggr-auth packets
debug crypto ssl tunnel errors
debug crypto ssl tunnel events
debug crypto ssl tunnel packets
debug crypto ssl package
```

2. Quelques commandes supplémentaires pour vérifier la configuration SSL.

```
# show crypto ssl authorization policy
# show crypto ssl diagnose error
# show crypto ssl policy
# show crypto ssl profile
# show crypto ssl proposal
# show crypto ssl session profile <profile_name>
```

```
# show crypto ssl session user <username> detail
# show crypto ssl session user <username> platform detail
```

3. Outil DART (Diagnostic and Reporting Tool) pour le client sécurisé Cisco.
Pour collecter l'ensemble DART, exécutez les étapes décrites dans la section Exécuter DART pour collecter des données pour le dépannage

Exemples de débogages d'une connexion réussie :

```
debug crypto ssl
debug crypto ssl tunnel events
debug crypto ssl tunnel errors
```

<#root>

```
*Mar 3 16:47:11.141: CRYPTO-SSL: sslvpn process rcvd context queue event
*Mar 3 16:47:14.149: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891B8 total_len=621 bytes=621 tcb=0x0
*Mar 3 16:47:15.948: %SSLVPN-5-LOGIN_AUTH_PASSED: vw_ctx: ssl_prof vw_gw: ssl_policy remote_ip: 10.106.
*Mar 3 16:47:15.948: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: cisco] [Source: LOCAL] [localport
*Mar 3 16:47:15.949: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891E0 total_len=912 bytes=912 tcb=0x0
*Mar 3 16:47:17.698: CRYPTO-SSL: sslvpn process rcvd context queue event
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] CSTP Version recd , using 1
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-ERR]: IPv6 local addr pool not found
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] No free IPv6 available, disabling IPv6
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0]
SSLVPN reuqesting a VA creation
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Per Tunnel Vaccess cloning 2 request sent
*Mar 3 16:47:20.760: %SYS-5-CONFIG_P: Configured programmatically by process VTEMPLATE Background Mgr f
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[0] VACCESS: Received VACCESS PER TUNL EVENT response.
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Received vaccess Virtual-Access1 fro
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Cloning Per Tunnel Vaccess
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Interface Vi1 assigned to Session Us
*Mar 3 16:47:20.761: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Allocating IP 192.168.13.4 from address-pool
*Mar 3 16:47:20.761: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Using new allocated IP 192.168.13.4 0.0.0.0
*Mar 3 16:47:20.761: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Mar 3 16:47:20.763: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Full Tunnel CONNECT request processed, HTTP r
*Mar 3 16:47:20.763: HTTP/1.1 200 OK
*Mar 3 16:47:20.763: Server: Cisco IOS SSLVPN
*Mar 3 16:47:20.763: X-CSTP-Version: 1
*Mar 3 16:47:20.763: X-CSTP-Address: 192.168.13.4
*Mar 3 16:47:20.763: X-CSTP-Netmask: 0.0.0.0
*Mar 3 16:47:20.763: X-CSTP-DNS: 192.168.11.100
*Mar 3 16:47:20.764: X-CSTP-Lease-Duration: 43200
*Mar 3 16:47:20.764: X-CSTP-MTU: 1406
*Mar 3 16:47:20.764: X-CSTP-Default-Domain: example.com
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.11.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.12.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.11.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.12.0/255.255.255.0
*Mar 3 16:47:20.765: X-CSTP-Rekey-Time: 3600
*Mar 3 16:47:20.765: X-CSTP-Rekey-Method: new-tunnel
```

```
*Mar 3 16:47:20.765: X-CSTP-DPD: 300
*Mar 3 16:47:20.765: X-CSTP-Disconnected-Timeout: 0
*Mar 3 16:47:20.765: X-CSTP-Idle-Timeout: 1800
*Mar 3 16:47:20.765: X-CSTP-Session-Timeout: 43200
*Mar 3 16:47:20.765: X-CSTP-Keepalive: 30
*Mar 3 16:47:20.765: X-CSTP-Smartcard-Removal-Disconnect: false
*Mar 3 16:47:20.766: X-CSTP-Include-Local_LAN: false
*Mar 3 16:47:20.766: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] For User cisco, DPD timer started for 300 sec
*Mar 3 16:47:20.766: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891E0 total_len=693 bytes=693 tcb=0x0
*Mar 3 16:47:21.762:
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up

Informations connexes

- Assistance technique de Cisco et téléchargements

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.