AnyConnect SSL VPN op C800v met lokale verificatie configureren

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco IOS XE Head-end C800v voor AnyConnect SSL VPN kunt configureren met een lokale gebruikersdatabase.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco IOS XE
- Cisco Secure-client (CSC)
- Algemene SSL-werking
- Public Key Infrastructure (PKI)

Gebruikte componenten

DeDe informatie in dit document is gebaseerd op deze software- en hardwareversies:

- Cisco Catalyst 8000V (C800V) actieve versie 17.16.01a
- Cisco Secure-clientversie 5.1.8.105
- Clientpc met geïnstalleerde Cisco Secure-client

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Cisco IOS XE Secure Socket Layer (SSL) VPN is een routergebaseerde oplossing die SSL VPN-connectiviteit voor externe toegang biedt die is geïntegreerd met toonaangevende security en routeringsfuncties op een geconvergeerd platform voor gegevens, spraak en draadloze verbindingen. Met Cisco IOS XE SSL VPN krijgen eindgebruikers veilig toegang vanuit huis of elke locatie die voor internet geschikt is, zoals draadloze hotspots. Cisco IOS XE SSL VPN stelt bedrijven ook in staat om de toegang tot het bedrijfsnetwerk uit te breiden naar offshore partners en consultants, waardoor bedrijfsgegevens voortdurend beschermd blijven.

Deze optie wordt ondersteund op de opgegeven platforms:

Platform	Ondersteunde Cisco IOS XE release
Cisco Cloud-services router 1000V Series	Cisco IOS XE release 16.9
Cisco Catalyst 8000V switch	Cisco IOS XE Bengaluru 17.4.1
Cisco 4461 geïntegreerde services router Cisco 4451 geïntegreerde services router Cisco 4431 geïntegreerde services router	Cisco IOS XE-koppeling 17.7.1a

Configureren

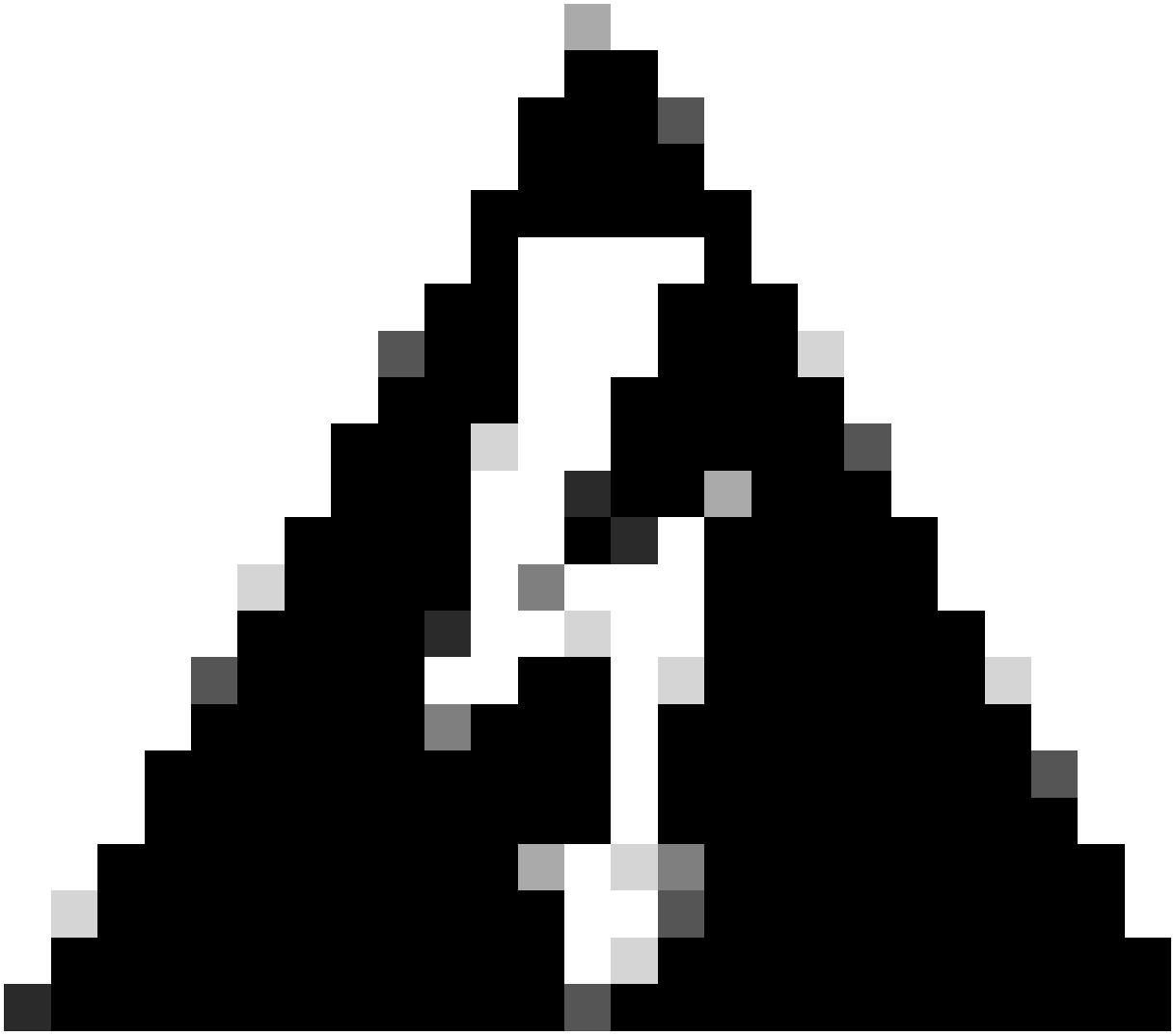
Netwerkdiagram

Basis netwerkdiagram

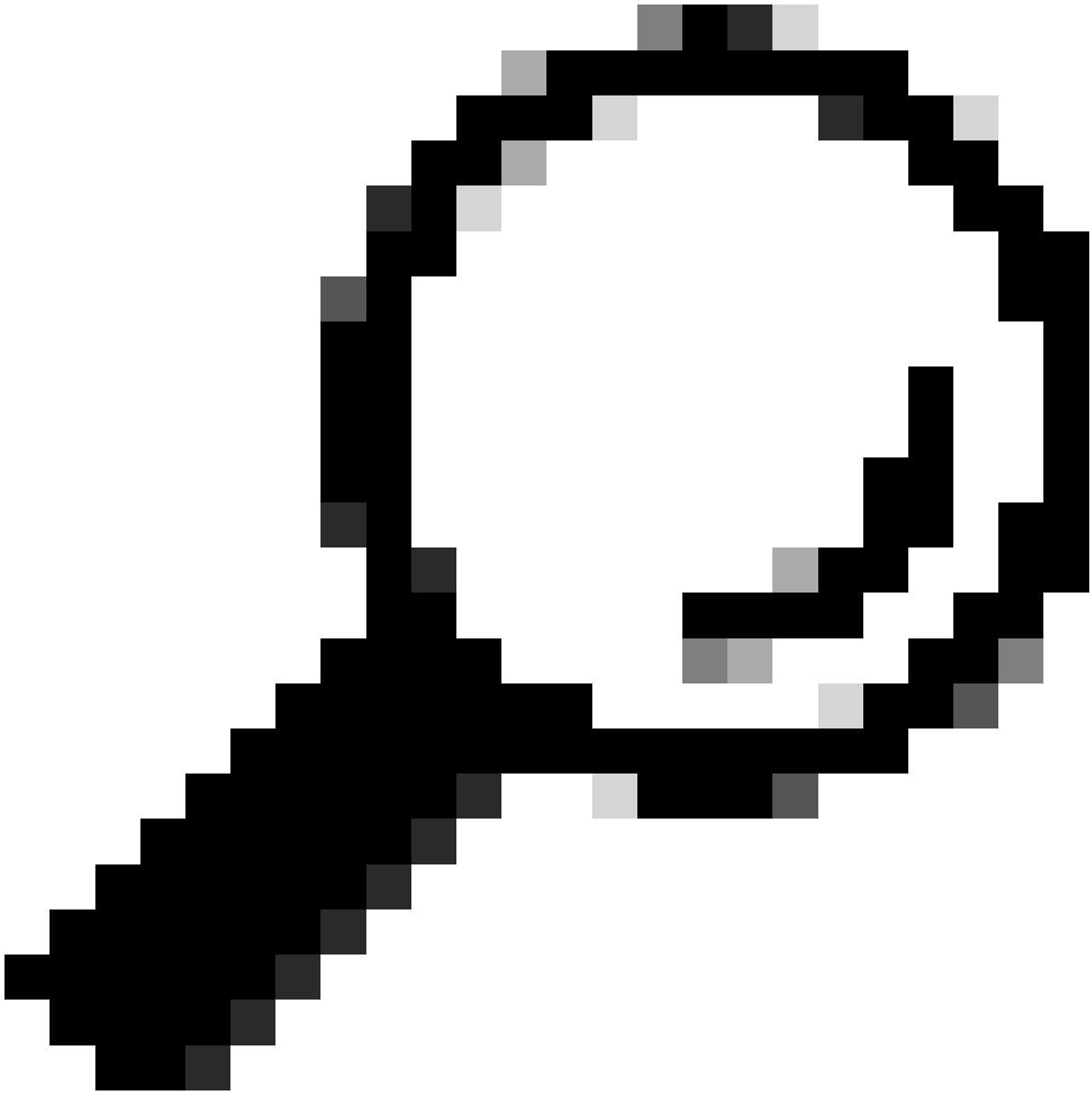
Configuraties

1. Schakel AAA in, configureer verificatie, autorisatielijsten en voeg een gebruikersnaam toe aan de lokale database.

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



Waarschuwing: De opdracht aaa new-model past onmiddellijk lokale verificatie toe op alle lijnen en interfaces (behalve de consolelijn con 0). Als een Telnet-sessie wordt geopend naar de router nadat deze opdracht is ingeschakeld (of als een verbinding wordt uitgezet en opnieuw moet worden verbonden), dan moet de gebruiker worden geverifieerd met de lokale database van de router. Het wordt aanbevolen om een gebruikersnaam en wachtwoord op de router te definiëren voordat u de AAA-configuratie start, zodat u niet uitgesloten bent van de router.



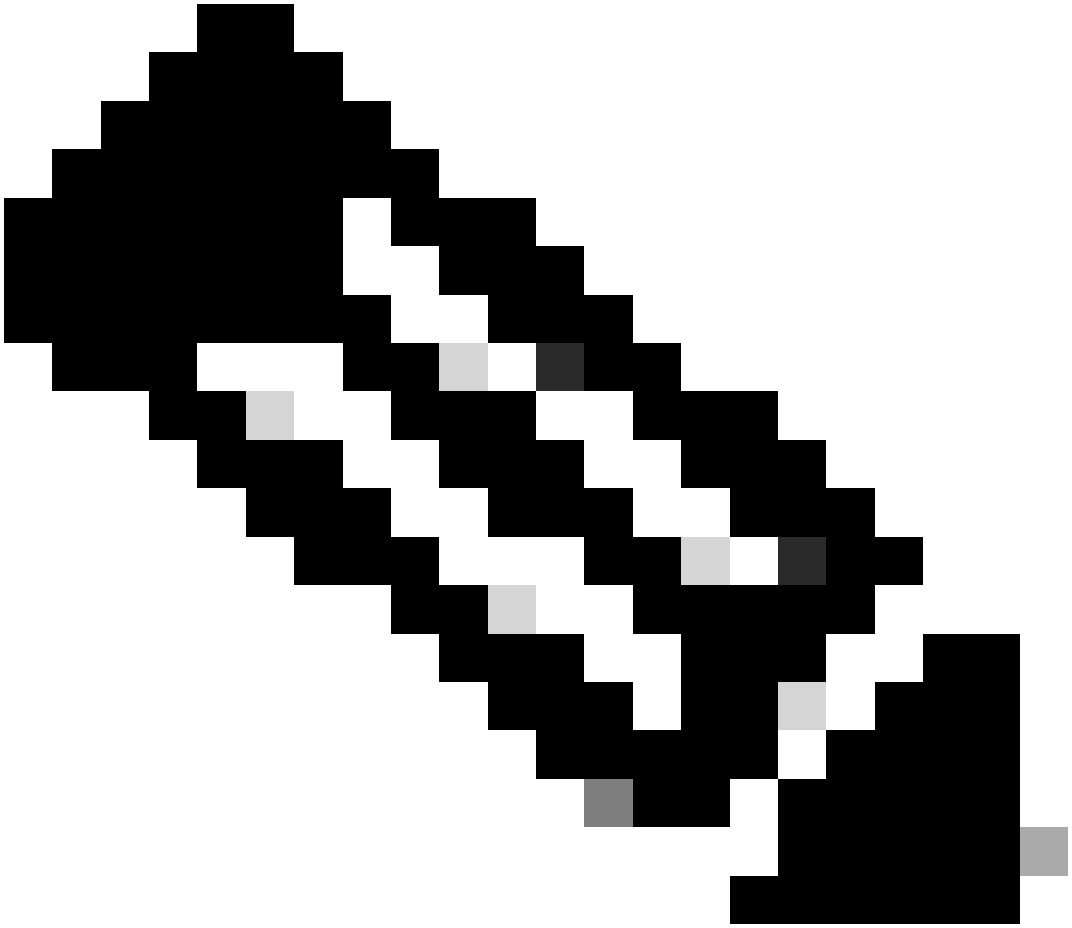
Tip: Voordat u uw AAA-opdrachten configureert, slaat u de configuratie op. U kunt de configuratie alleen opnieuw opslaan nadat u de AAA-configuratie hebt voltooid (en ervan overtuigd bent dat deze correct werkt). Dit staat u toe om van onverwachte lockouts te herstellen aangezien u om het even welke verandering met een herladen van de router kunt terugrollen.

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

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

3. Maak een Trustpoint om het identiteitscertificaat van de router te installeren. U kunt verwijzen naar Hoe te om Certificaatinschrijving voor een PKI te vormen voor meer details op de certificaatverwezenlijking.

```
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
```



Opmerking: De algemene naam (CN) in de onderwerpnaam moet worden geconfigureerd met het IP-adres of de FQDN-naam (Full Qualified Domain Name) die gebruikers gebruiken om verbinding te maken met de beveiligde gateway (C800V). Hoewel niet

---

verplicht, kan het correct invoeren van de GN helpen het aantal certificaatfouten te verminderen die gebruikers tegenkomen bij het inloggen.

4. Definieer een lokale IP-pool om adressen aan Cisco Secure Client toe te wijzen.

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

5. (Optioneel) Configureer een standaard toegangslijst die voor de splitstunnel moet worden gebruikt. Deze toegangslijst bestaat uit de doelnetwerken die toegankelijk zijn via de VPN-tunnel. In de standaardinstelling passeert al het verkeer door de VPN-tunnel (volledige tunnel) als de gesplitste tunnel niet is geconfigureerd.

```
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.Schakel de beveiligde HTTP-server uit.

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

7. Configureer een SSL-voorstel.

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

8. Configureer een SSL-beleid, neem contact op met het SSL-voorstel en het PKI-trustpoint.

```
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
```

```
ip interface GigabitEthernet1 port 443
```

SSL-beleid definieert het voorstel en trustpoint dat tijdens SSL-onderhandeling moet worden gebruikt. Het dient als een container voor alle parameters die betrokken zijn bij de SSL onderhandeling. De beleidsselectie wordt gemaakt door de sessieparameters af te stemmen op die welke onder het beleid zijn geconfigureerd.

9. (Optioneel) Maak een AnyConnect-profiel met behulp van de Cisco Secure Client Profile Editor Cisco Secure Client Profile Editor . Een fragment van XML equivalent van het profiel, wordt gegeven voor uw verwijzing.

<#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

false

false

true

SSL_C8KV

sslvpn-c8kv.example.com

10. Upload het gemaakte XML-profiel naar het flash-geheugen van de router en definieer het profiel:

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

11.Schakel de beveiligde HTTP-server uit.

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

12. Configuratie van SSL-autorisatiebeleid.

```
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
```

Het SSL-autorisatiebeleid is een container met autorisatieparameters die naar een externe client worden geduwd.Het autorisatiebeleid wordt vanuit het SSL-profiel doorverwezen.

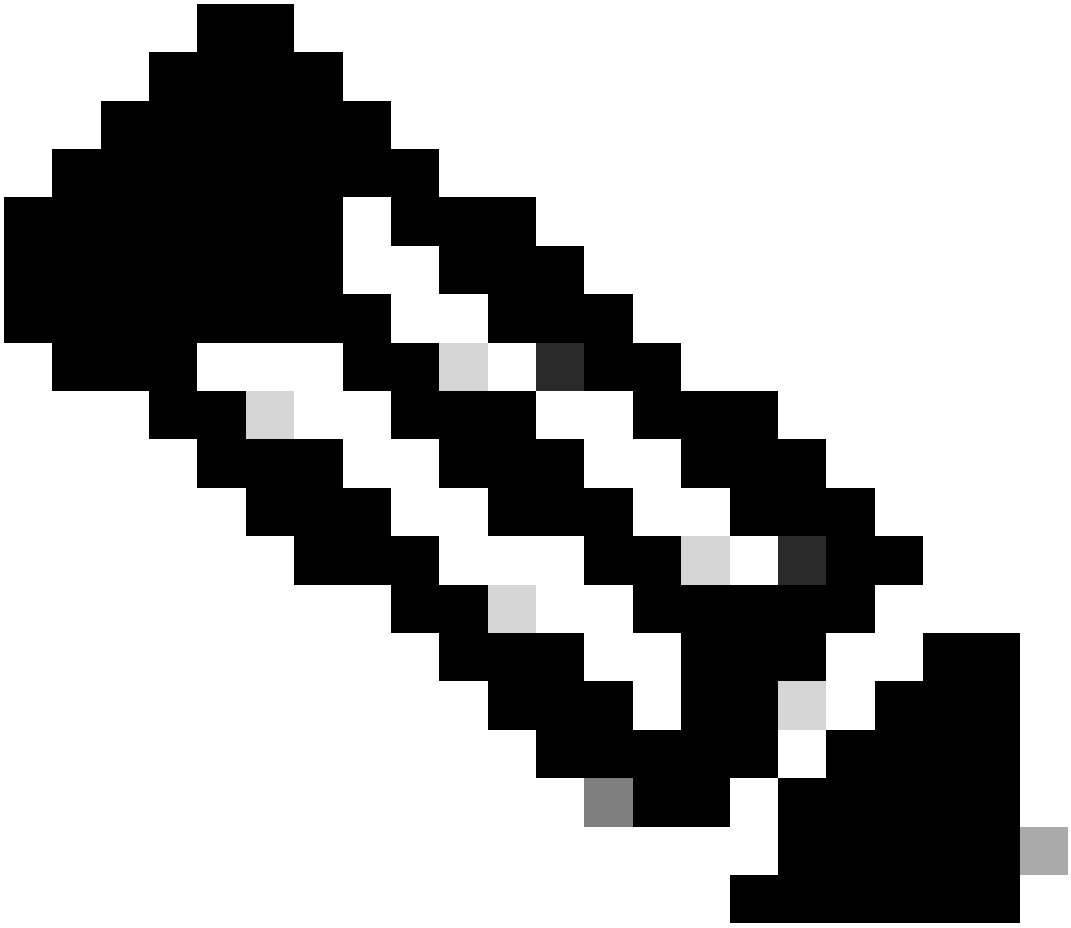
13. Configureer een virtuele sjabloon waaruit de virtuele-toegangsinterfaces worden gekloond.

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

14. Een SSL-profiel configureren en authenticatie, boekhoudlijsten en virtuele template te definiëren.

```
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
```

Een profielselectie hangt af van beleid en URL-waarden.



Opmerking: Het beleid en de URL moeten uniek zijn voor een SSL VPN-profiel en er moet ten minste één autorisatiemethode worden gespecificeerd om de sessie te starten.

Deze worden gebruikt in SSL-profiel:

- match policy - match statement om een SSL profiel ssl_prof te selecteren voor een client onder de SSL beleidsnaam ssl_policy.
- match url - match statements om een SSL profiel ssl_prof te selecteren voor een client op de URL sslvpn-c8kv.example.com.
- aaa verificatie user-pass lijst - Tijdens verificatie wordt de SSLVPN_AUTHEN lijst gebruikt.
- aaa autorisatiegroep user-pass lijst - Tijdens de autorisatie wordt de netwerklijst SSLVPN_AUTHOR gebruikt met het autorisatiebeleid ssl_auteur_policy.
- verificatie externe user-pass - definieert de verificatiemodus van de externe client is gebaseerd op gebruikersnaam/wachtwoord.
- virtual-template 2 - definieert welke virtuele template moet worden gekloond.

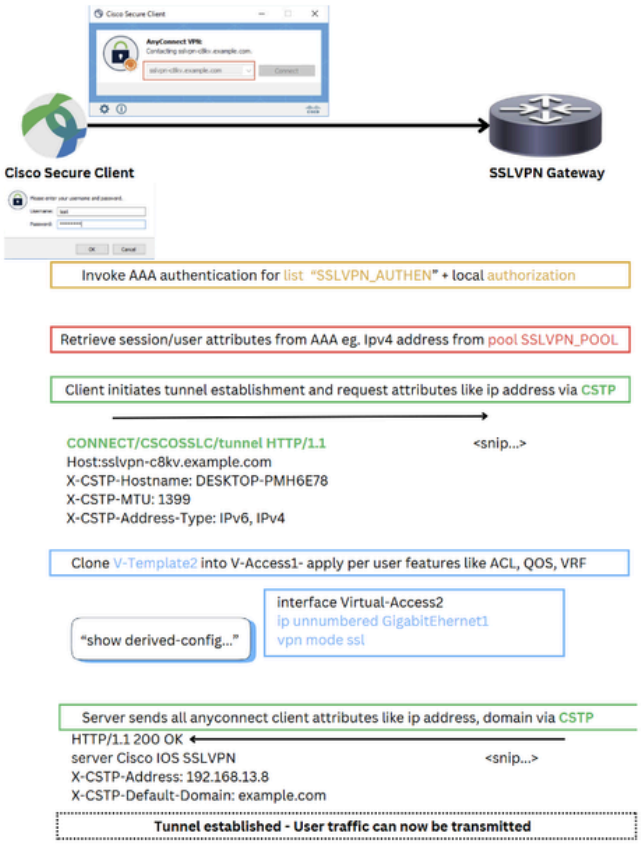
Verbindingsstroom

Als u de gebeurtenissen wilt begrijpen die plaatsvinden tussen Cisco Secure Client en de beveiligde gateway tijdens een SSL VPN-verbindingsbedrijf, raadpleegt u Document [Understanding the AnyConnect SSL VPN Connection Flow]

Cisco Secure Client (AnyConnect) voor C800v-verbindingsstroom op hoog niveau


```
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
```

Verbindingsstroom op hoog niveau 1

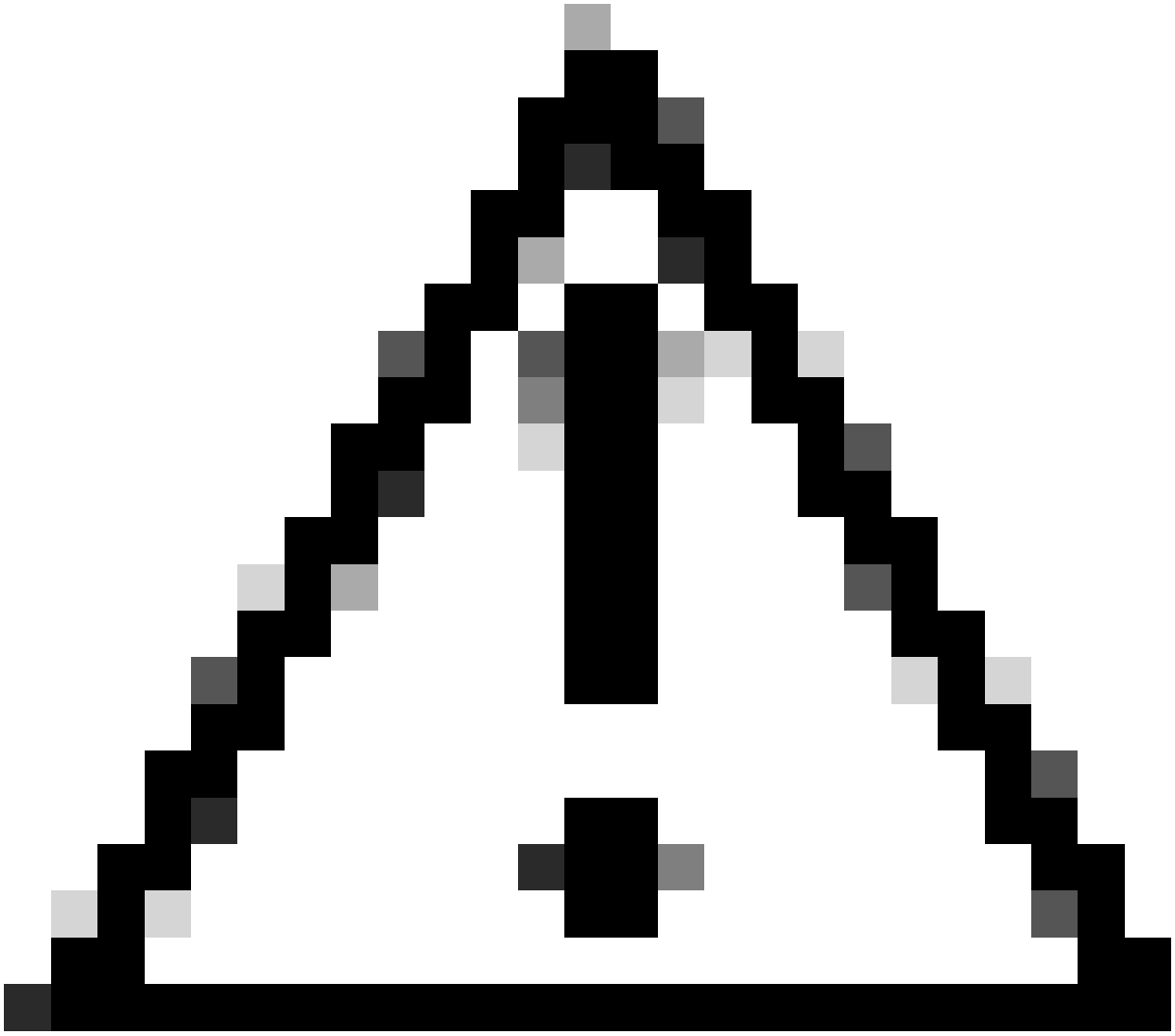



```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
!
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
```

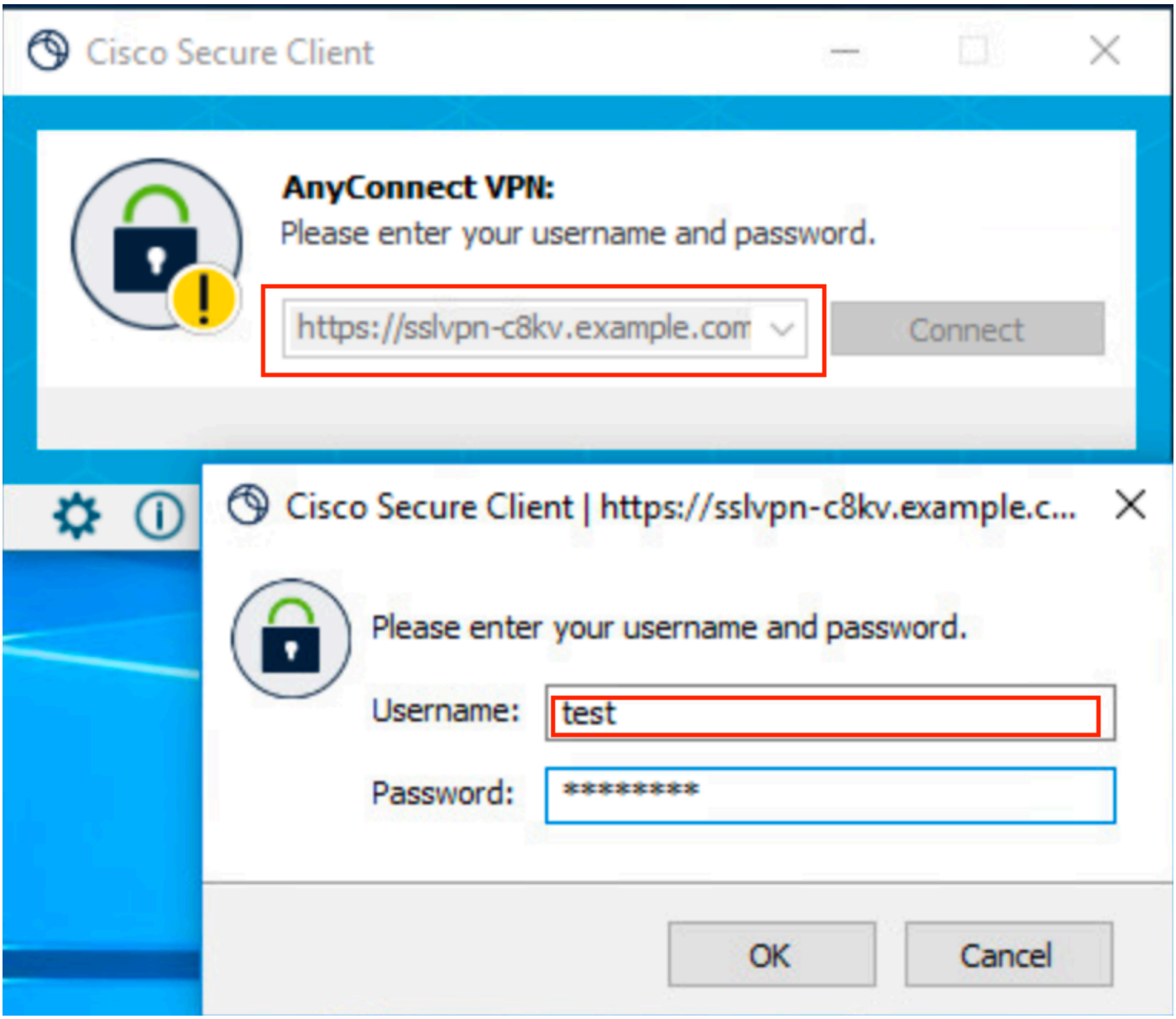
Verbindingsstroom op hoog niveau 2

Verifiëren

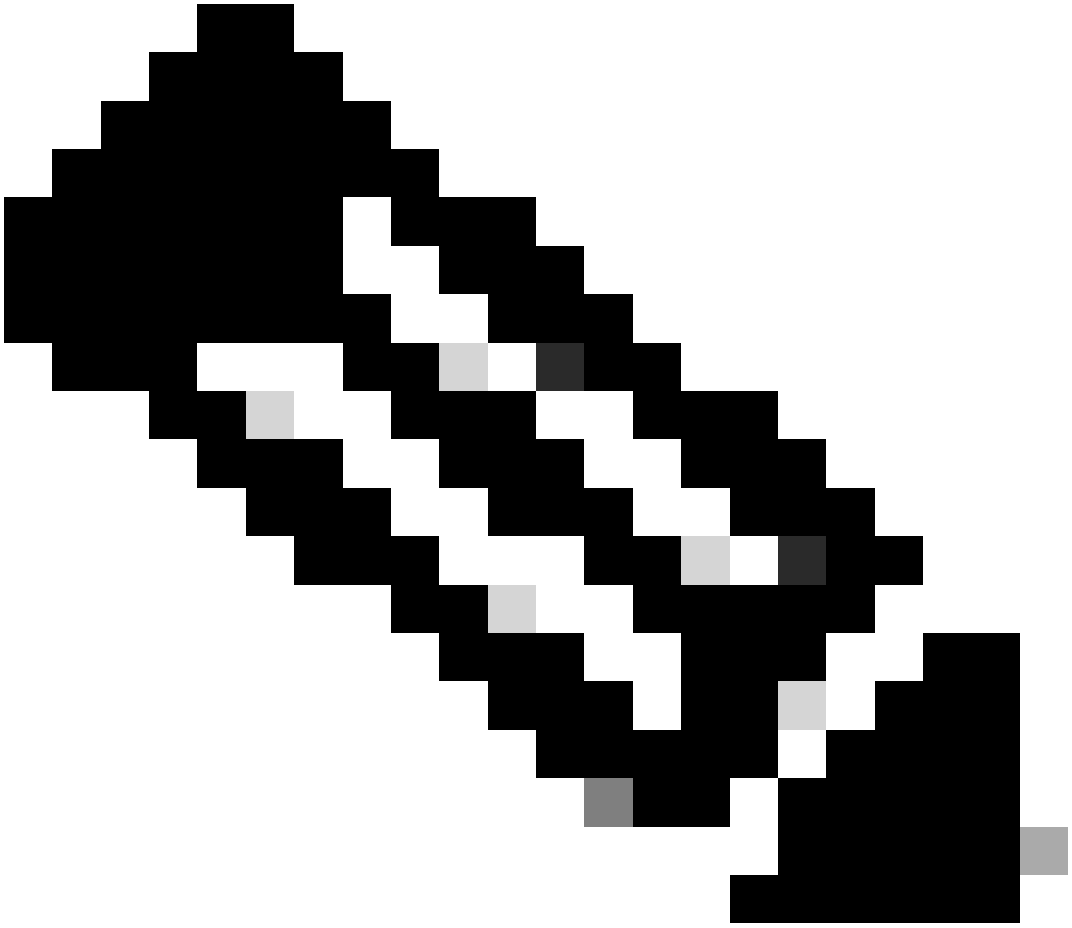
1. Om de verificatie te testen, maakt u verbinding vanuit de Cisco Secure Client met Fully Qualified Domain Name (FQDN) of IP-adres van C800v en voert u de referenties in.



Voorzichtig: C800v ondersteunt het downloaden van clientsoftware vanaf head-end niet. Cisco Secure-client moet vooraf op de pc zijn geïnstalleerd.



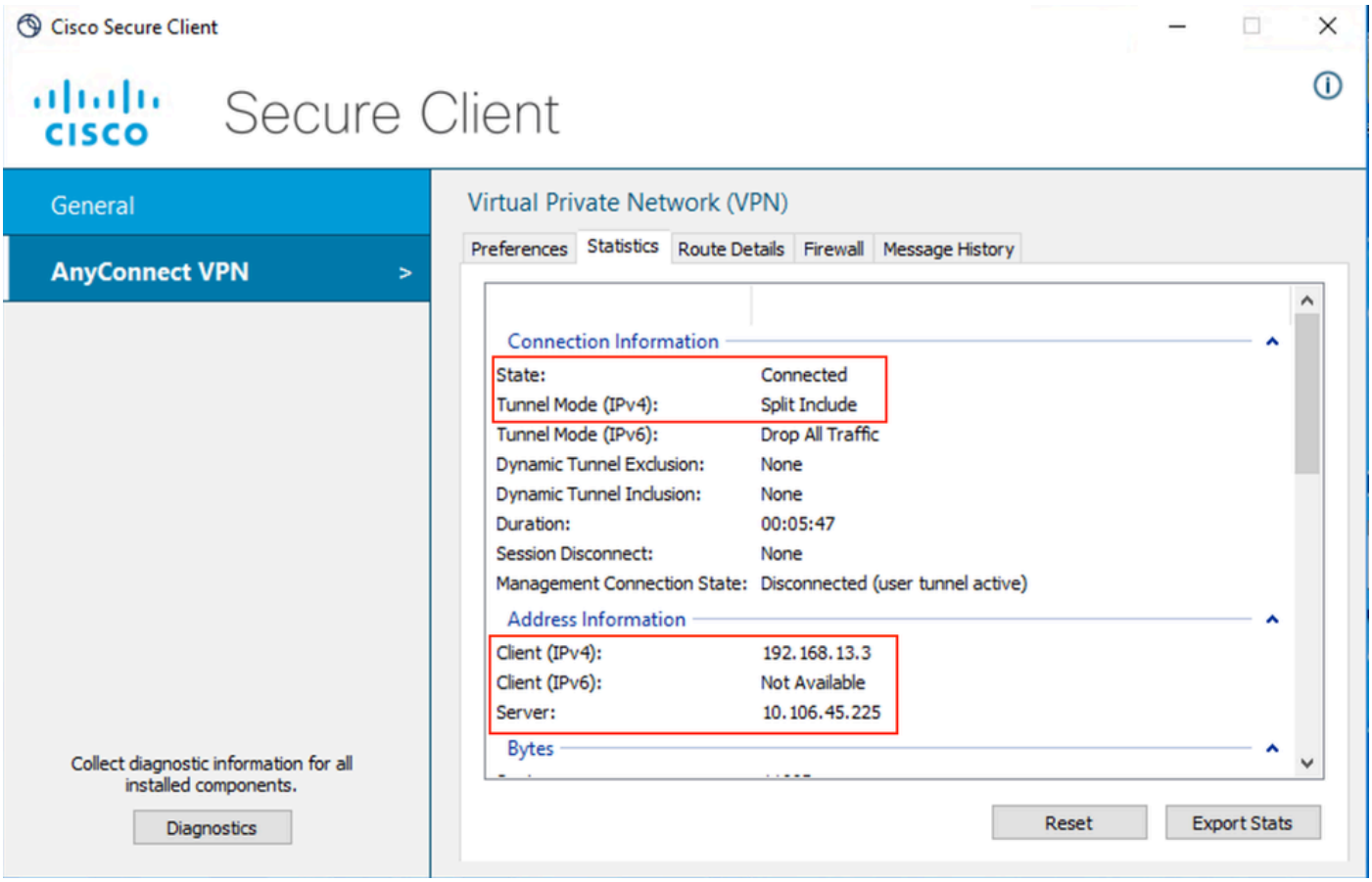
Cisco Secure-clientverbindingspoging



Opmerking: met een nieuwe installatie van de beveiligde client voor Cisco (zonder XML-profielen toegevoegd) kan de gebruiker handmatig de FQDN van de VPN-gateway invoeren in de adresbalk van Cisco Secure Client. Na een succesvolle aanmelding probeert de Cisco Secure-client standaard het XML-profiel te downloaden. Cisco Secure-client moet echter worden herstart om het profiel in de GUI te kunnen weergeven. Het eenvoudigweg sluiten van het venster voor Cisco Secure Client is niet voldoende. Om het proces opnieuw te starten, klikt u met de rechtermuisknop op het pictogram Cisco Secure Client in het Windows-vak en selecteert u de optie Ophouden.

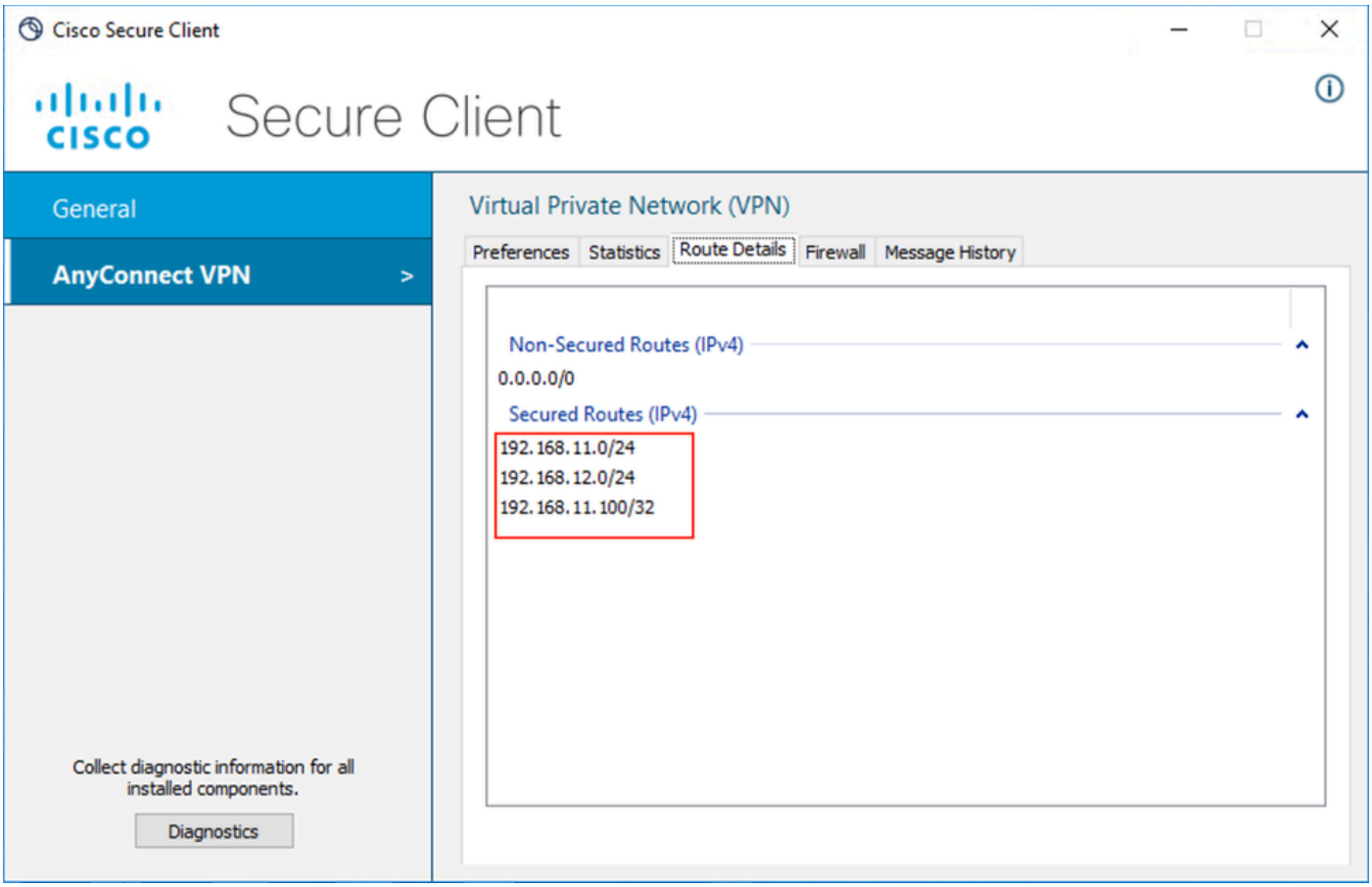
---

2. Zodra de verbinding tot stand is gebracht, klikt u op het pictogram van de versnelling in de linkerbenedenhoek en navigeert u naar AnyConnect VPN > Statistics. Bevestig dat de weergegeven informatie overeenkomt met de informatie over de verbinding en het adres.



Cisco Secure Client (AnyConnect)-statistieken

3. Navigeer naar AnyConnectVPN > Routegegevens en bevestigen dat de weergegeven informatie overeenstemt met de beveiligde routes en niet beveiligde routes.



Cisco Secure Client (AnyConnect)-routegegevens

Gebruik dit gedeelte om te bevestigen dat uw configuratie correct werkt op C8000v:

1. Om ssl sessieinformatie weer te geven - toon crypto ssl sessie{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. Om ssl vpn statistieken weer te geven - toon crypto sssl 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. Om de feitelijke configuratie te controleren die is toegepast voor de Virtual-Access-interface die aan de client is gekoppeld.

<#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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

1. SSL debugt om de onderhandeling tussen de head-end en de client te verifiëren.

<#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. Een paar extra opdrachten om SSL-configuratie te verifiëren.

```
# 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. Diagnostische en rapportage-tool (DART) voor de Cisco Secure-client.
Om de DART-bundel te verzamelen, voert u de stappen uit die in de Run DART worden beschreven om gegevens te verzamelen voor probleemoplossing.

Het voorbeeld van debugs van een succesvolle verbinding:

```
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

Gerelateerde informatie

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.