Konfigurieren von AnyConnect SSL VPN auf C8000v mit lokaler Authentifizierung

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des Cisco IOS XE Headend C8000v für AnyConnect SSL VPN mit einer lokalen Benutzerdatenbank beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco IOS XE
- Cisco Secure Client (CSC)
- Allgemeiner SSL-Betrieb
- Public Key Infrastructure (PKI)

Verwendete Komponenten

DoDie Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Catalyst 8000V (C8000V) mit Version 17.16.01a
- Cisco Secure Client Version 5.1.8.105
- Client-PC mit installiertem Cisco Secure Client

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Cisco IOS XE SSL VPN (Secure Socket Layer) ist eine routerbasierte Lösung, die SSL VPN-Verbindungen für den Remote-Zugriff bietet und mit branchenführenden Sicherheits- und Routing-Funktionen auf einer konvergenten Daten-, Sprach- und Wireless-Plattform integriert ist. Mit Cisco IOS XE SSL VPN erhalten Endbenutzer sicheren Zugriff von zu Hause oder von einem beliebigen internetfähigen Standort aus, z. B. von Wireless-Hotspots. Mit Cisco IOS XE SSL VPN können Unternehmen den Zugriff auf das Unternehmensnetzwerk auf Offshore-Partner und -Berater erweitern und gleichzeitig die Unternehmensdaten schützen.

Diese Funktion wird auf den folgenden Plattformen unterstützt:

Plattform	Unterstützte Cisco IOS XE-Version
Cisco Cloud Services Router der Serie 1000V	Cisco IOS XE Version 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bengaluru 17.4.1
Cisco Integrated Services Router 4461 Cisco Integrated Services Router 4451 Cisco Integrated Services Router 4431	Cisco IOS XE Cupertino 17.7.1a

Konfigurieren

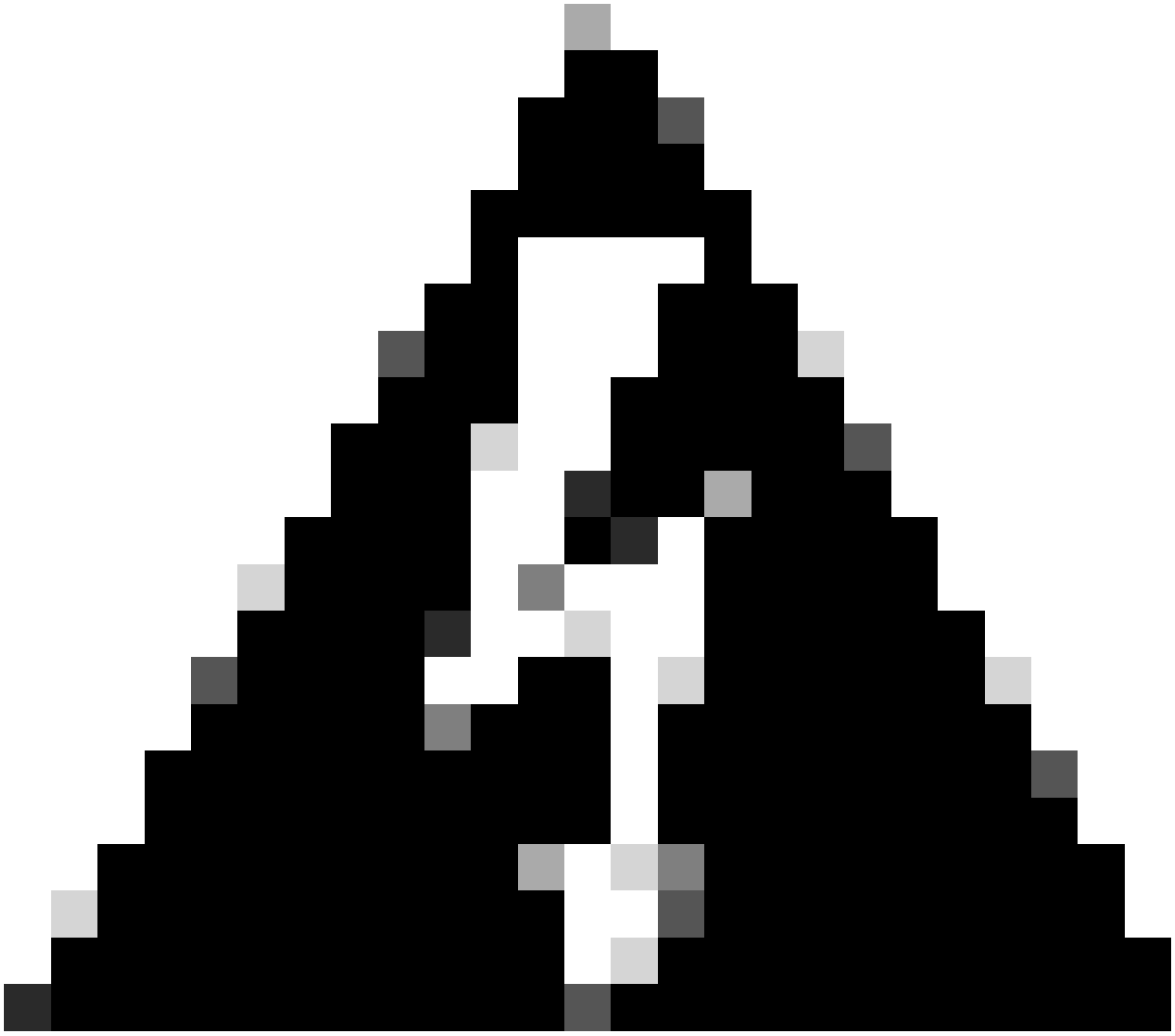
Netzwerkdiagramm

Grundlegendes Netzwerkdiagramm

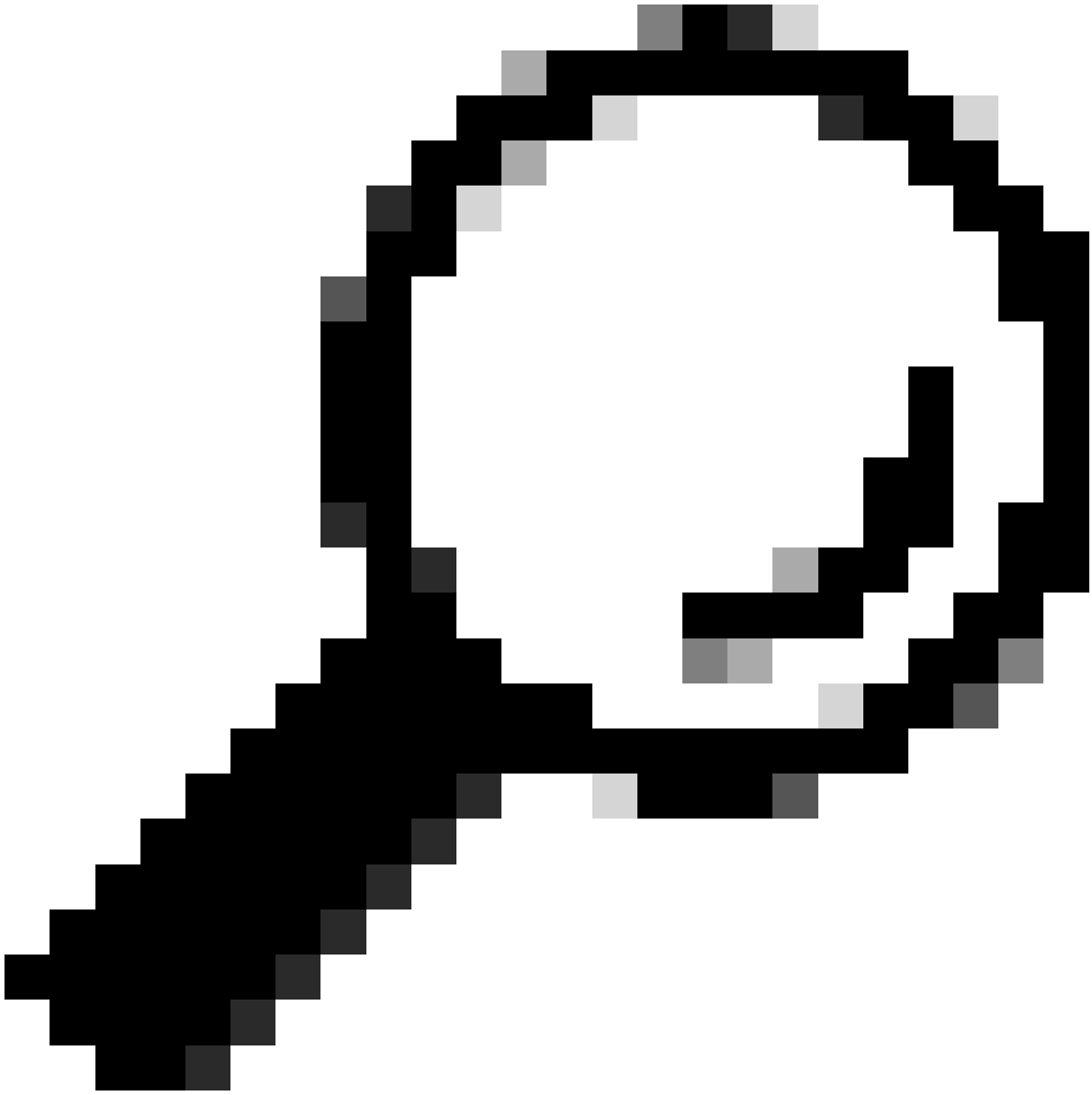
Konfigurationen

1. Aktivieren Sie AAA, konfigurieren Sie Authentifizierung, Autorisierungslisten, und fügen Sie einen Benutzernamen zur lokalen Datenbank hinzu.

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



Warnung: Mit dem Befehl aaa new-model wird sofort die lokale Authentifizierung auf alle Leitungen und Schnittstellen angewendet (mit Ausnahme der Konsolenzeile line con 0). Wenn eine Telnet-Sitzung zum Router geöffnet wird, nachdem dieser Befehl aktiviert wurde (oder wenn bei einer Verbindung die Zeit überschritten wird und die Verbindung wiederhergestellt werden muss), muss der Benutzer über die lokale Datenbank des Routers authentifiziert werden. Es wird empfohlen, vor dem Starten der AAA-Konfiguration einen Benutzernamen und ein Kennwort für den Router zu definieren, damit Sie nicht vom Router ausgeschlossen werden.



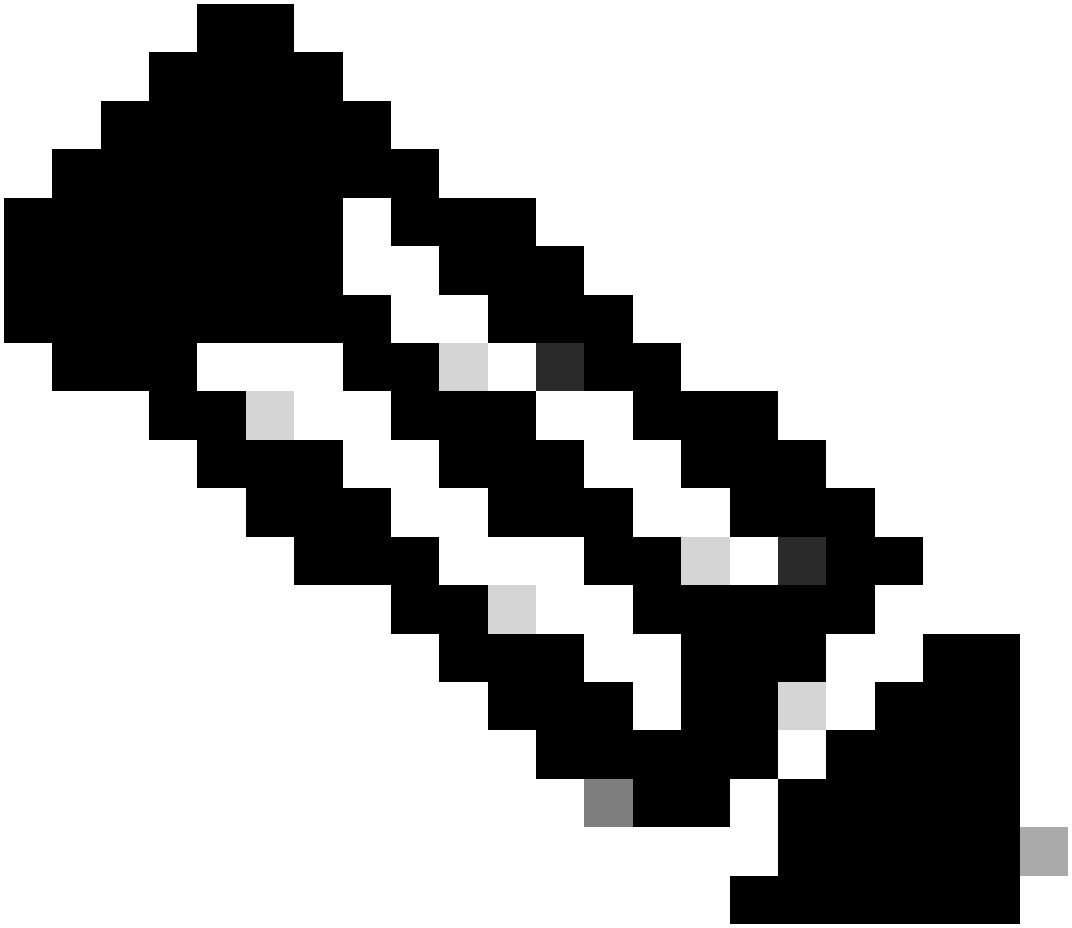
Tipp: Speichern Sie Ihre Konfiguration, bevor Sie die AAA-Befehle konfigurieren. Sie können die Konfiguration erst erneut speichern, nachdem Sie Ihre AAA-Konfiguration abgeschlossen haben (und sich davon überzeugt haben, dass sie ordnungsgemäß funktioniert). Auf diese Weise können Sie den Zustand nach unerwarteten Sperrungen wiederherstellen, da Sie jede Änderung durch ein Neuladen des Routers zurücksetzen können.

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

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

3. Erstellen Sie einen Vertrauenspunkt, um das Identitätszertifikat des Routers zu installieren. Weitere Informationen zur Zertifikaterstellung finden Sie unter How to Configure Certificate Enrollment for a PKI (Konfigurieren der Zertifikatregistrierung für eine PKI).

```
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
```



Anmerkung: Der Common Name (CN) im Subject Name (Antragstellername) muss mit der IP-Adresse oder dem vollqualifizierten Domänennamen (FQDN) konfiguriert werden, die bzw. den Benutzer verwenden, um eine Verbindung mit dem Secure Gateway (C8000V)

---

herzustellen. Die korrekte Eingabe der CN ist zwar nicht obligatorisch, kann jedoch dazu beitragen, die Anzahl der Zertifikatfehler zu reduzieren, die Benutzer bei der Anmeldung feststellen.

4. Definieren Sie einen lokalen IP-Pool, um dem Cisco Secure Client Adressen zuzuweisen.

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

5. (Optional) Konfigurieren Sie eine Standard-Zugriffsliste für den Split-Tunnel. Diese Zugriffsliste besteht aus den Zielnetzwerken, auf die über den VPN-Tunnel zugegriffen werden kann. Standardmäßig durchläuft der gesamte Datenverkehr den VPN-Tunnel (vollständiger Tunnel), wenn der Split-Tunnel nicht konfiguriert ist.

```
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.Deaktivieren Sie den sicheren HTTP-Server.

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

7. Konfigurieren Sie ein SSL-Angebot.

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

8. Konfigurieren Sie eine SSL-Richtlinie, und rufen Sie das SSL-Angebot und den PKI-Vertrauenspunkt auf.

```
crypto ssl policy ssl_policy
```

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

Die SSL-Richtlinie definiert den Vorschlag und den Vertrauenspunkt, der während der SSL-Aushandlung verwendet werden soll. Er dient als Container für alle Parameter, die an der SSL-Aushandlung beteiligt sind. Die Richtlinienauswahl erfolgt durch Abgleich der Sitzungsparameter mit den in der Richtlinie konfigurierten Parametern.

9. (Optional) Erstellen Sie mithilfe des Cisco Secure Client Profile Editor Cisco Secure Client Profile Editor ein AnyConnect-Profil. Ein Ausschnitt aus XML-Äquivalent des Profils wird als Referenz angegeben.

<#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. Laden Sie das erstellte XML-Profil in den Flash-Speicher des Routers hoch, und definieren Sie das Profil:

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

11.Deaktivieren Sie den sicheren HTTP-Server.

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

12. Konfigurieren der SSL-Autorisierungsrichtlinie

```
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
```

Die SSL-Autorisierungsrichtlinie ist ein Container mit Autorisierungsparametern, die an den Remote-Client gesendet werden.Die Autorisierungsrichtlinie wird vom SSL-Profil aus referenziert.

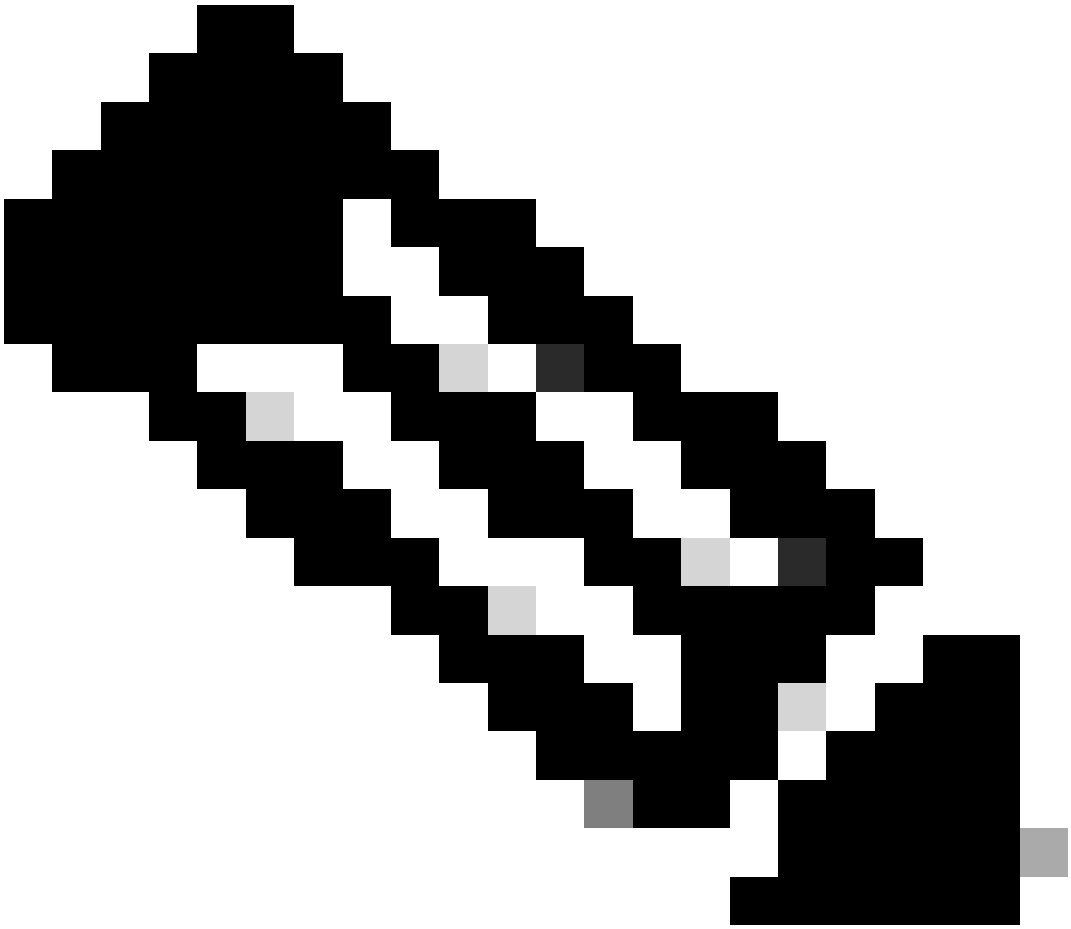
13. Konfigurieren Sie eine virtuelle Vorlage, aus der die Schnittstellen für den virtuellen Zugriff geklont werden.

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

14. Konfigurieren Sie ein SSL-Profil und Definieren Sie Authentifizierung, Abrechnungslisten und virtuelle Vorlage.

```
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
```

Eine Profilauswahl hängt von Richtlinien- und URL-Werten ab.



Anmerkung: Die Richtlinie und die URL müssen für ein SSL VPN-Profil eindeutig sein, und es muss mindestens eine Autorisierungsmethode zum Starten der Sitzung angegeben werden.

Diese werden im SSL-Profil verwendet:

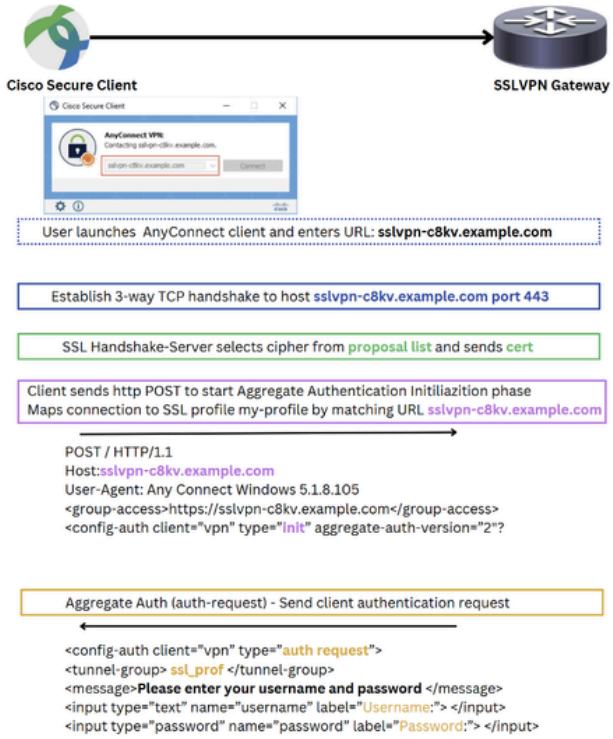
- match policy - match-Anweisung zur Auswahl eines SSL-Profils ssl_prof für einen Client mit dem SSL-Richtliniennamen ssl_policy.
- match url - match-Anweisungen zur Auswahl eines SSL-Profils ssl_prof für einen Client im Verzeichnis URL sslvpn-c8kv.example.com.
- aaa authentication user-pass list - Während der Authentifizierung wird die SSL VPN_AUTHEN-Liste verwendet.
- aaa authentication group user-pass list - Während der Autorisierung wird die Netzwerkliste SSLVPN_AUTHOR mit der Autorisierungsrichtlinie ssl_author_policy verwendet.
- authentication remote user-pass - Definiert den Authentifizierungsmodus des Remote-

Clients, der auf Benutzername/Kennwort basiert.
- virtual-template 2 - Definiert, welche virtuelle Vorlage geklont werden soll.

Verbindungsfluss

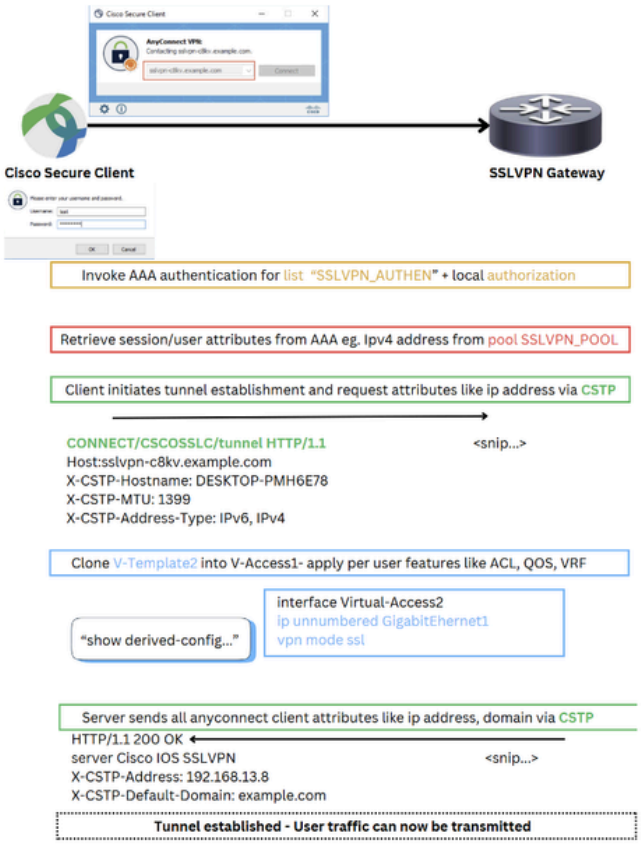
Informationen zu den Ereignissen, die während der Herstellung einer SSL VPN-Verbindung zwischen dem Cisco Secure Client und dem Secure Gateway auftreten, finden Sie im Dokument [Understanding the AnyConnect SSL VPN Connection Flow.]

High-Level-Verbindungsfluss von Cisco Secure Client (AnyConnect) zu 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
```

High-Level-Verbindungsablauf 1

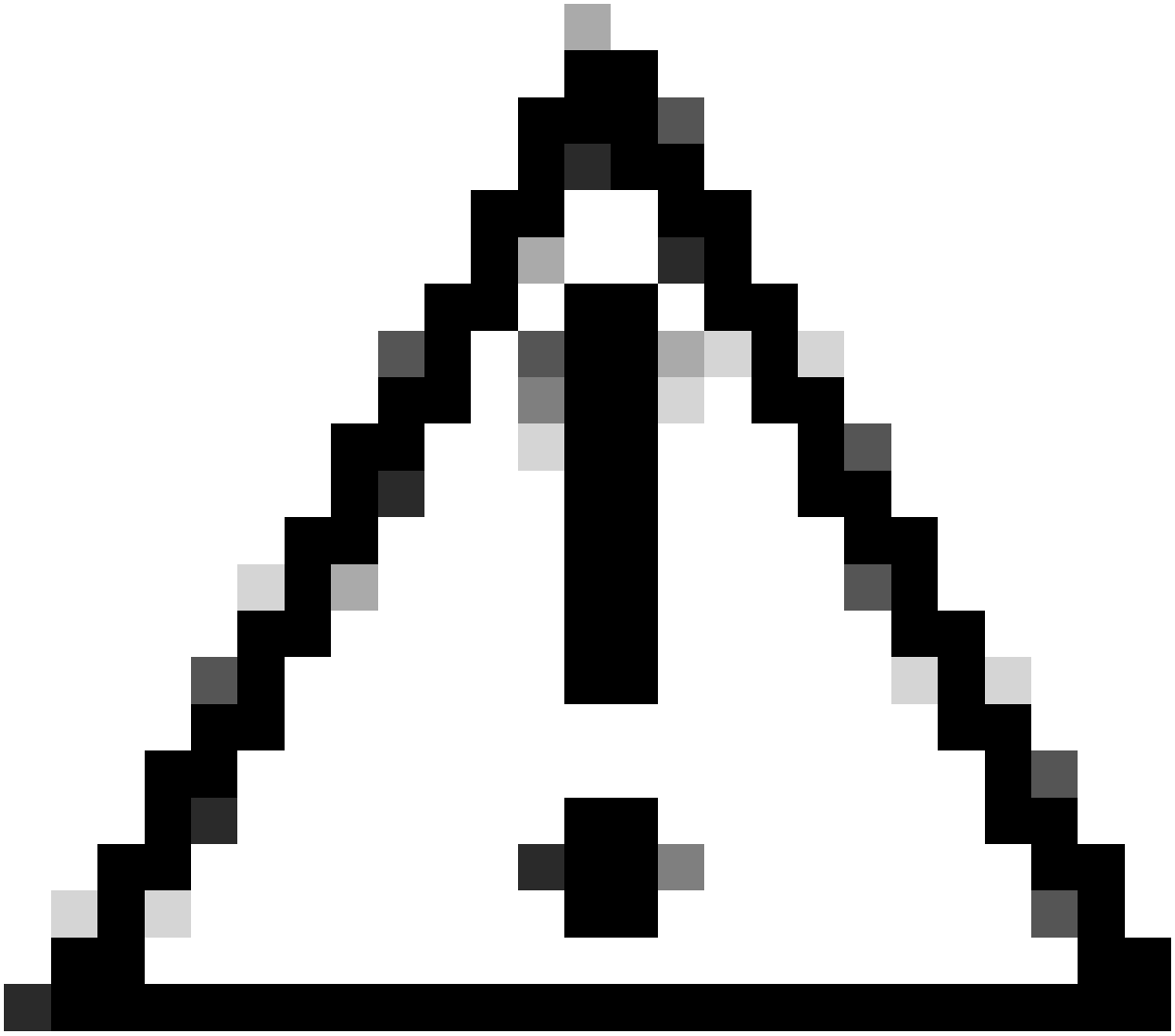



```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443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

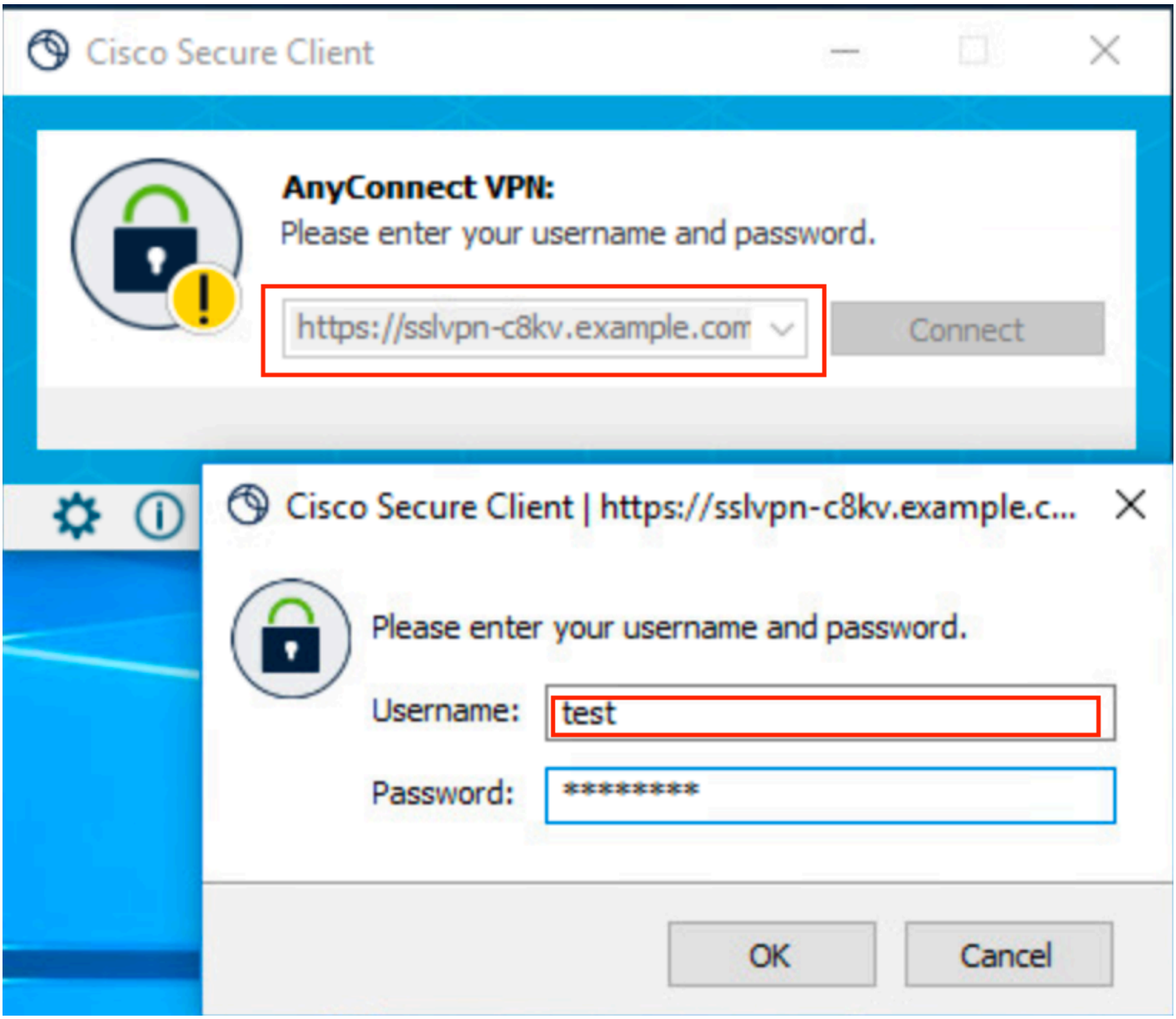
High-Level-Verbindungsablauf 2

Überprüfung

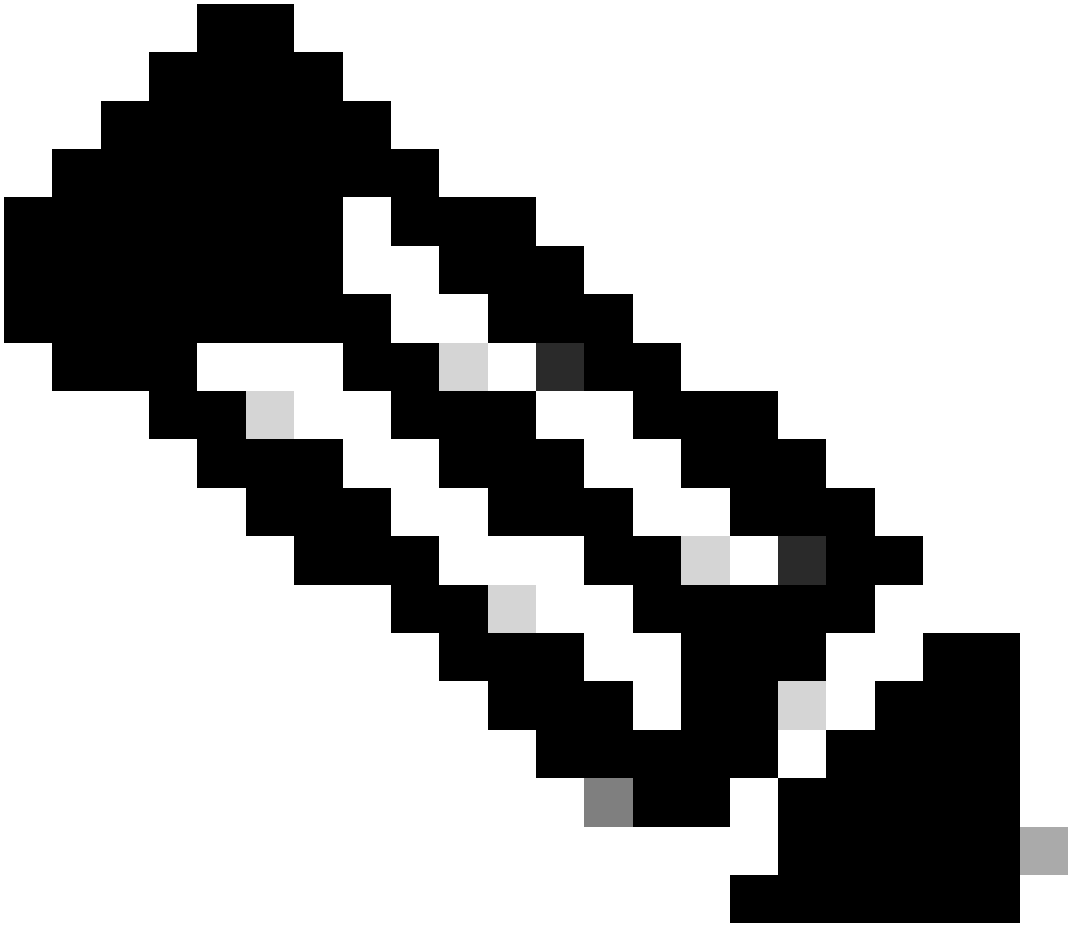
1. Stellen Sie zum Testen der Authentifizierung eine Verbindung vom Cisco Secure Client mit dem vollqualifizierten Domänennamen (FQDN) oder der IP-Adresse von C8000v her, und geben Sie die Anmeldeinformationen ein.



Vorsicht: C8000v unterstützt kein Herunterladen von Client-Software vom Headend. Cisco Secure Client muss auf dem PC vorinstalliert sein.



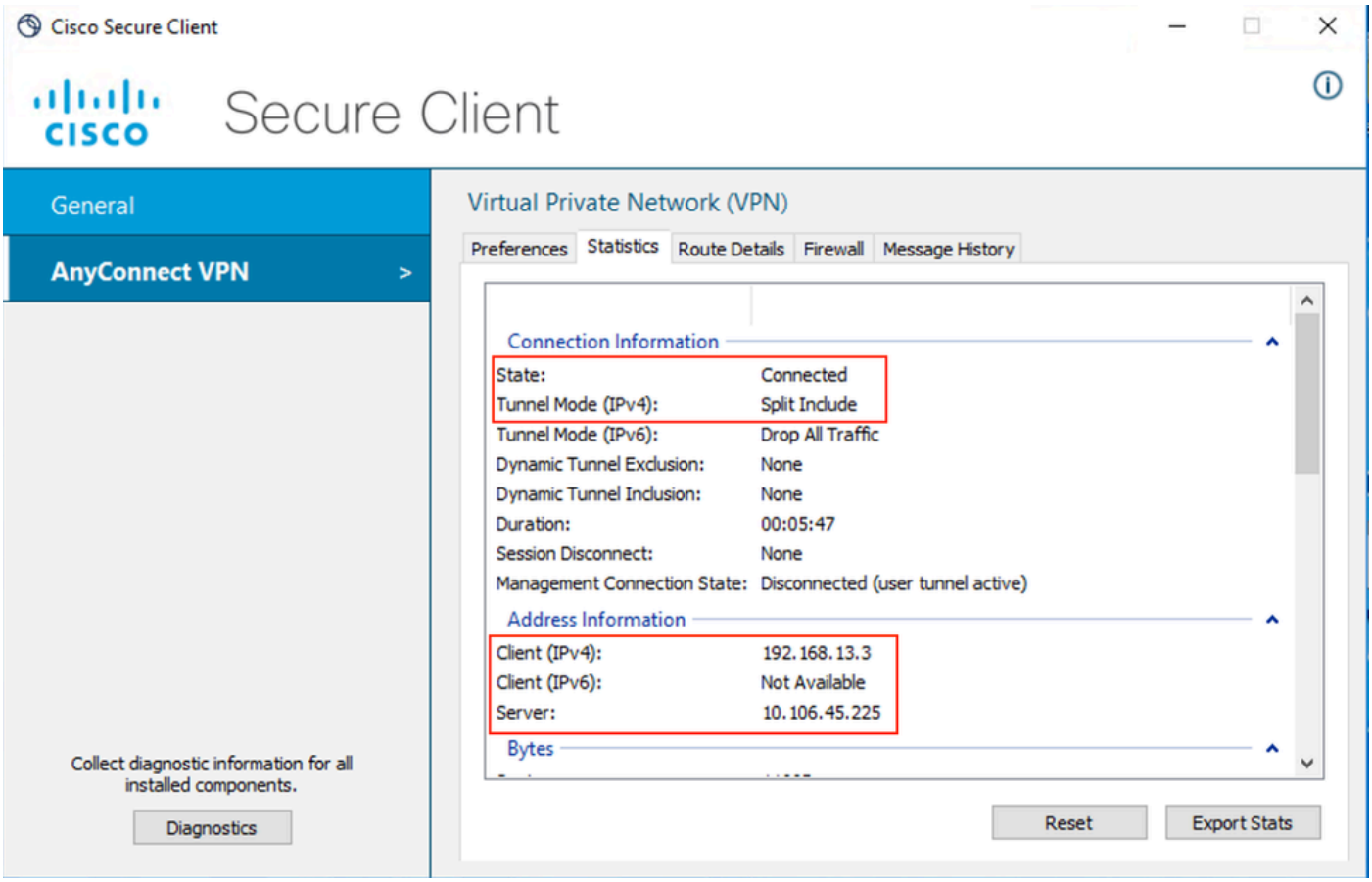
Verbindungsversuch mit Cisco Secure Client



Hinweis: Nach einer Neuinstallation des Cisco Secure Client (ohne Hinzufügen von XML-Profilen) kann der Benutzer den FQDN des VPN-Gateways manuell in der Adressleiste des Cisco Secure Client eingeben. Nach erfolgreicher Anmeldung versucht der Cisco Secure Client standardmäßig, das XML-Profil herunterzuladen. Der Cisco Secure Client muss jedoch neu gestartet werden, damit das Profil in der GUI angezeigt wird. Das Schließen des Fensters "Cisco Secure Client" reicht nicht aus. Um den Prozess neu zu starten, klicken Sie mit der rechten Maustaste auf das Symbol Cisco Secure Client in der Windows-Taskleiste, und wählen Sie die Option Beenden.

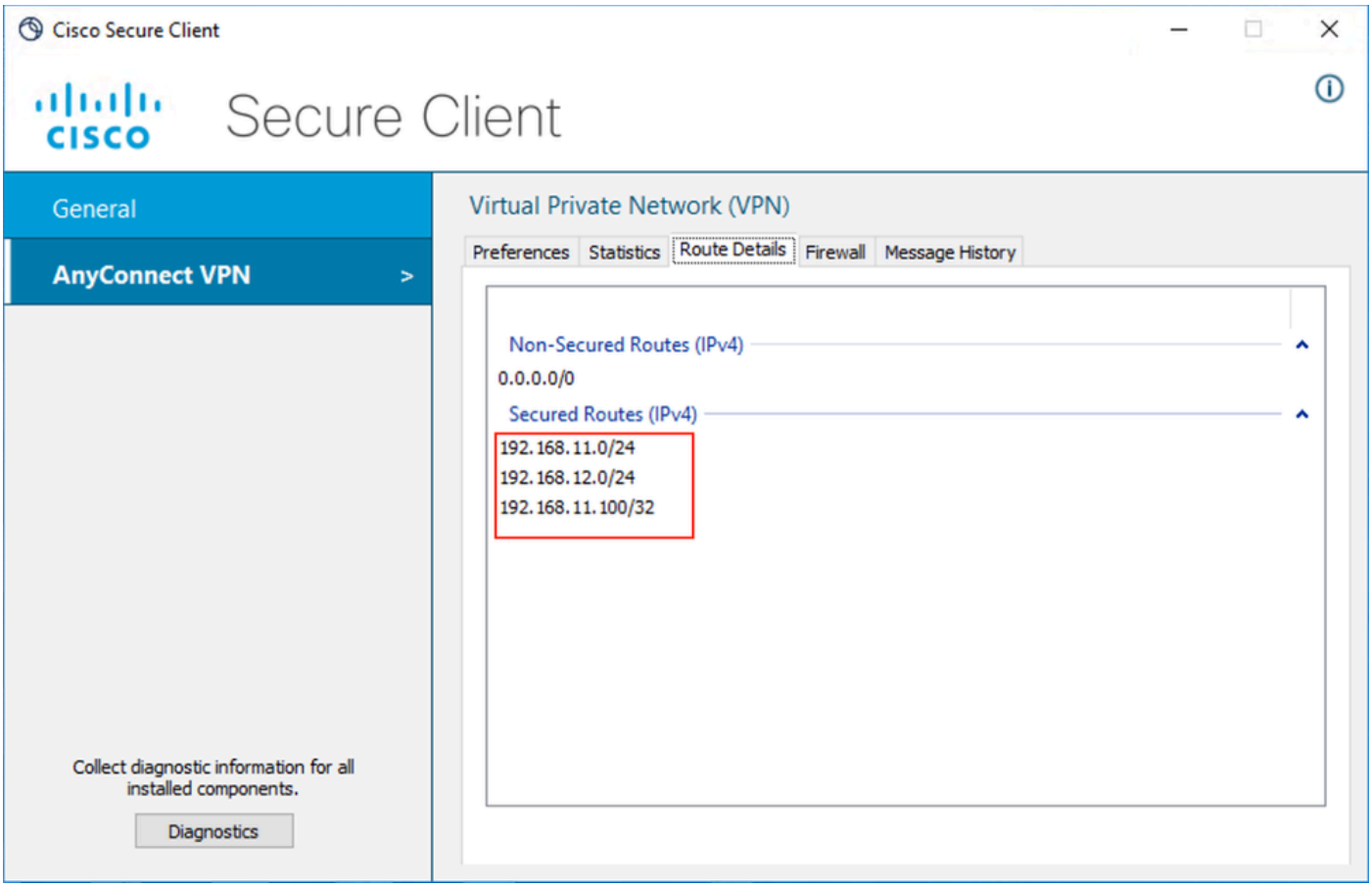
---

2. Nachdem die Verbindung hergestellt wurde, klicken Sie auf das Zahnrad-Symbol in der linken unteren Ecke und navigieren Sie zu AnyConnect VPN > Statistics. Bestätigen Sie, dass die angezeigten Informationen den Verbindungs- und Adressinformationen entsprechen.



Cisco Secure Client (AnyConnect)-Statistiken

3. Navigieren Sie zu AnyConnectVPN > Routendetails und bestätigen Sie, dass die angezeigten Informationen den gesicherten und nicht gesicherten Routen entsprechen.



Routendetails für Cisco Secure Client (AnyConnect)

Verwenden Sie diesen Abschnitt, um sicherzustellen, dass Ihre Konfiguration auf C8000v ordnungsgemäß funktioniert:

1. So zeigen Sie SSL-Sitzungsinformationen an: 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. Um SSL VPN-Statistiken anzuzeigen - 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. Um die tatsächliche Konfiguration zu überprüfen, die für die dem Client zugeordnete Virtual-Access-Schnittstelle angewendet wurde.

<#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
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

1. SSL-Debugging-Verfahren zur Überprüfung der Aushandlung zwischen Headend und 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. Einige zusätzliche Befehle zum Überprüfen der SSL-Konfiguration.

```
# 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. Diagnostic and Reporting Tool (DART) für den Cisco Secure Client
Führen Sie zum Sammeln des DART-Pakets die unter DART ausführen beschriebenen Schritte aus, um Daten zur Fehlerbehebung zu sammeln.

Beispiel für das Debuggen einer erfolgreichen Verbindung:

```
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

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.