在C8000v上使用本地身份驗證配置AnyConnect SSL VPN

目錄

簡介

本文檔介紹如何使用本地使用者資料庫為AnyConnect SSL VPN配置Cisco IOS XE頭端C8000v。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS XE
- 思科安全使用者端(CSC)
- 常規SSL操作
- 公開金鑰基礎架構 (PKI)

採用元件

Th本檔案中的資訊是根據以下軟體和硬體版本：

- 運行版本17.16.01a的Cisco Catalyst 8000V(C8000V)
- 思科安全使用者端版本5.1.8.105
- 安裝了Cisco Secure Client的客戶端PC

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco IOS XE安全套接字層(SSL)VPN是一種基於路由器的解決方案，可在融合資料、語音和無線平台上提供SSL VPN遠端訪問連線，並與業界領先的安全性和路由功能整合。藉助Cisco IOS XE SSL VPN，終端使用者可以安全地從家庭或任何啟用網際網路的位置（如無線熱點）訪問資料。Cisco IOS XE SSL VPN還使公司能夠將公司網路訪問擴展到離岸合作夥伴和顧問，同時保護公司資料。

以下指定平台支援此功能：

平台	支援的Cisco IOS XE版本
Cisco Cloud Services Router 1000V系列	Cisco IOS XE版本16.9
Cisco Catalyst 8000V	Cisco IOS XE班加羅爾17.4.1
思科4461整合式服務路由器 思科4451整合式服務路由器 思科4431整合式服務路由器	Cisco IOS XE Cupertino 17.7.1a

設定

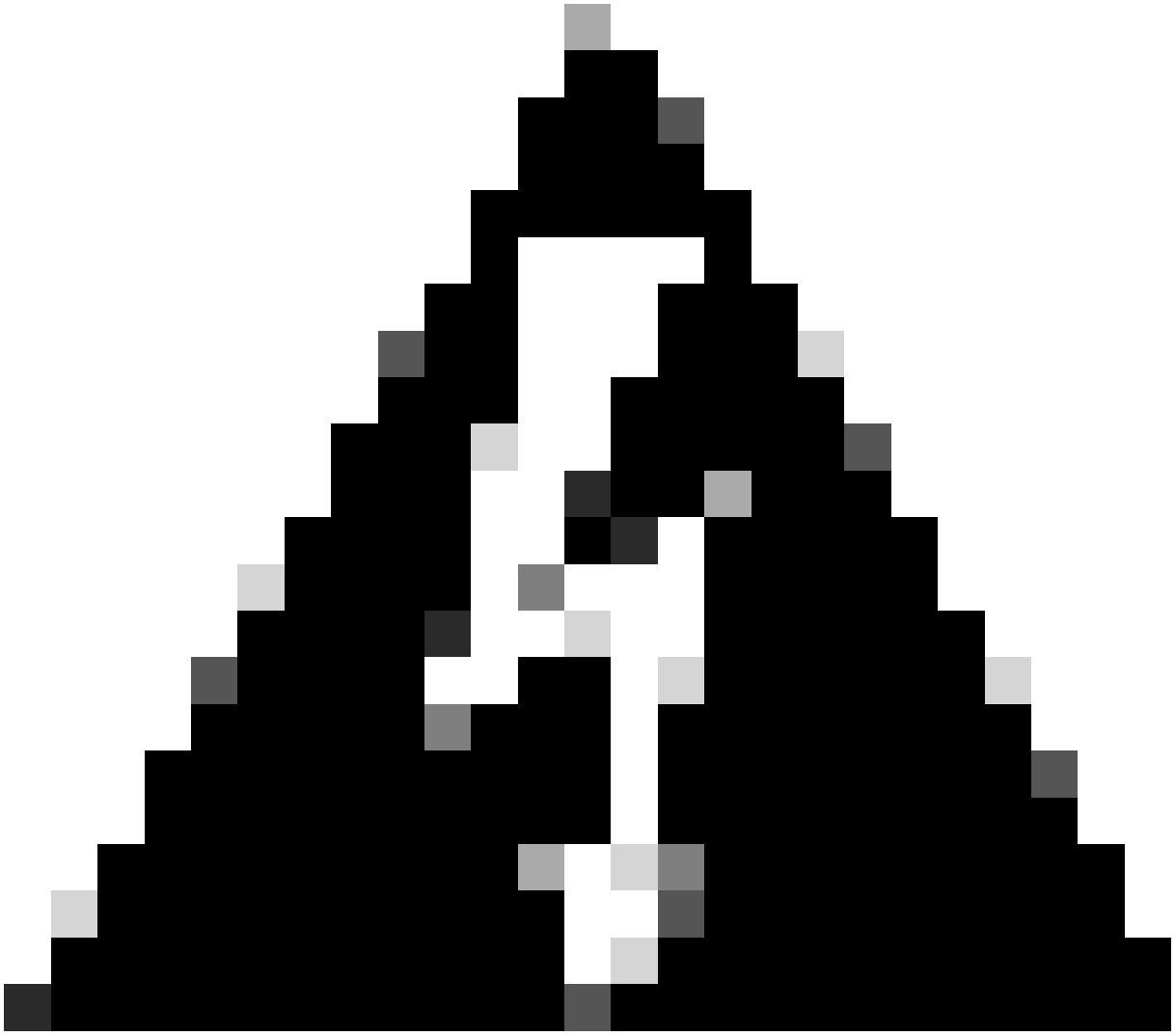
網路圖表

基本網路圖

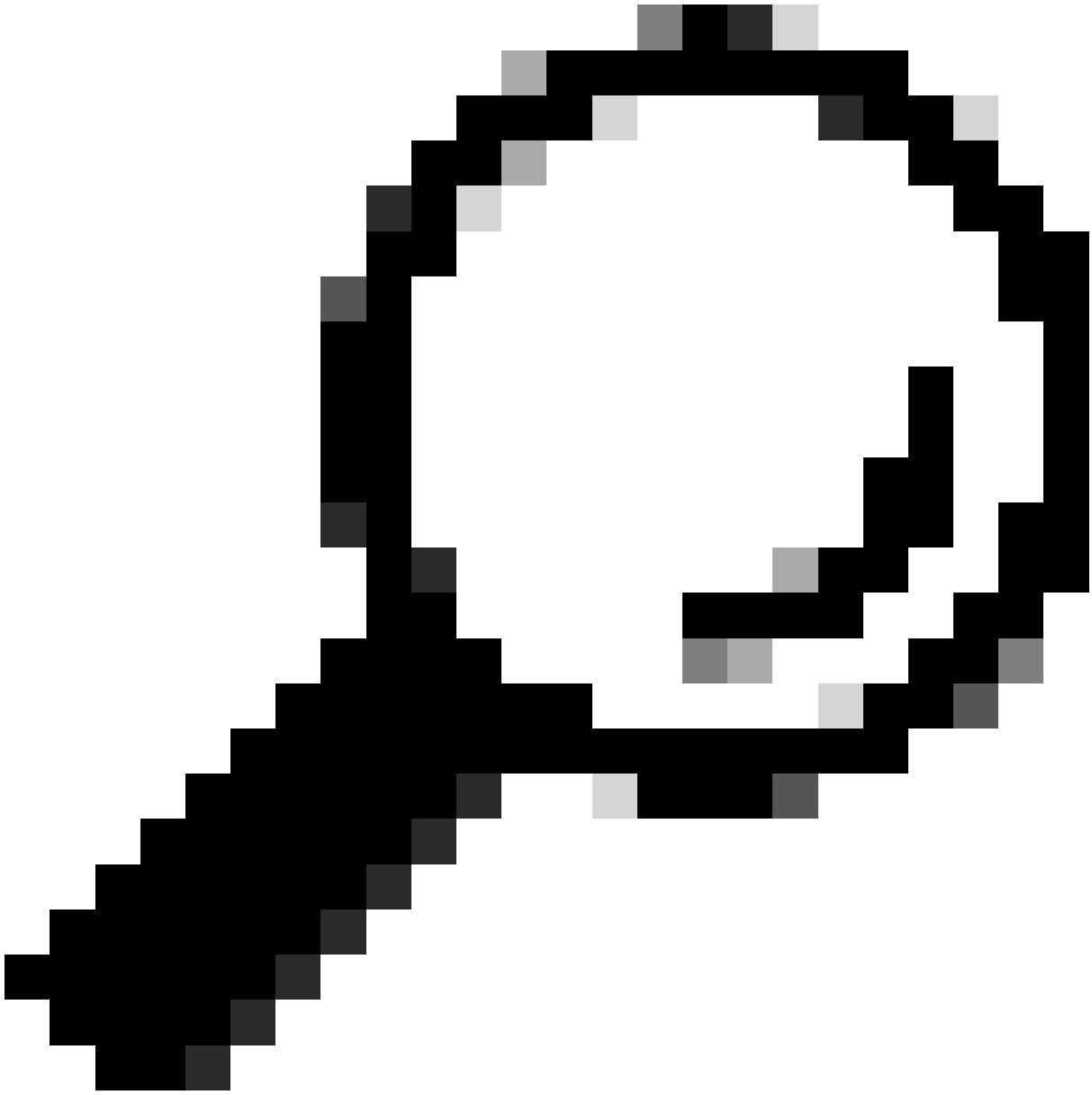
組態

1. 啟用AAA，配置身份驗證、授權清單，並向本地資料庫新增使用者名稱。

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



警告：aaa new-model命令立即將本地身份驗證應用到所有線路和介面（控制檯線路連線0除外）。 如果 Telnet 工作階段在命令啟用（或連線逾時且必須重新連線）後向路由器開放，則使用者必須使用路由器的本機資料庫進行驗證。建議在開始AAA設定之前，在路由器上定義使用者名稱和密碼，以免您鎖定在路由器之外。



提示：在配置AAA命令之前，請儲存配置。只有在完成AAA配置後（並且確信配置工作正常），才能再次儲存配置。 這可讓您從非預期的鎖定中復原，只要重新載入路由器就能復原任何變更。

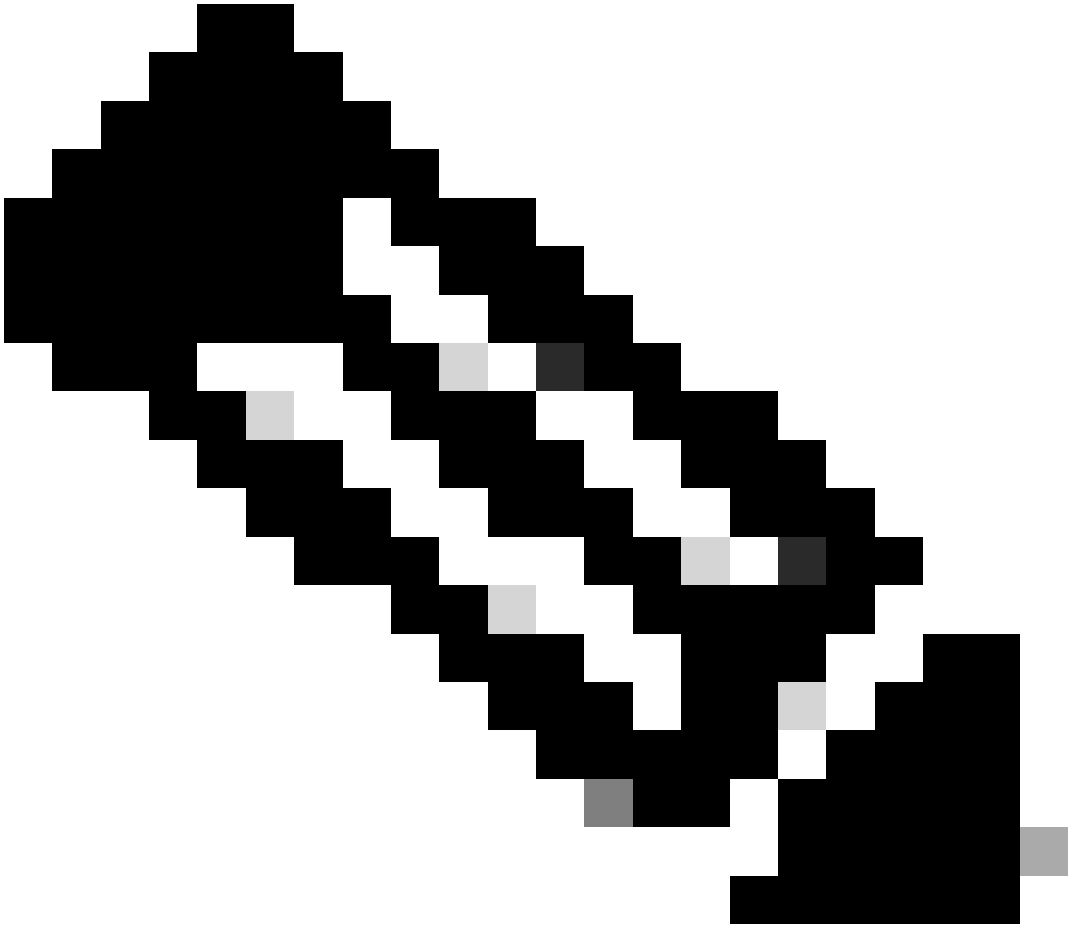
2.生成Rivest-Shamir-Adleman(RSA)金鑰對。

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

3.建立信任點以安裝路由器的身份證書。有關證書建立的詳細資訊，請參閱如何為PKI配置證書註冊

。

```
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
```



附註：使用者名稱中的公用名稱(CN)必須配置有使用者用來連線到安全閘道(C8000V)的IP位址或完全限定網域名稱(FQDN)。 雖然並非強制輸入，但正確輸入CN有助於減少使用者在登入時遇到的證書錯誤數量。

---

4. 定義IP本地池以向Cisco安全客戶端分配地址。

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

5.（可選）配置要用於拆分隧道的標準訪問清單。此訪問清單包括可通過VPN隧道訪問的目標網路。預設情況下，如果沒有配置拆分隧道，則所有流量都會通過VPN隧道（全隧道）。

```
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.禁用HTTP安全伺服器。

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

7.配置SSL方案。

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

8.配置SSL策略，呼叫SSL建議和PKI信任點。

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

SSL策略定義在SSL協商期間要使用的提議和信任點。它充當SSL協商中涉及的所有引數的容器。策略選擇是通過將會話引數與策略下配置的引數匹配來進行的。

9.（可選）在思科安全客戶端配置檔案編輯器Cisco Secure Client Profile Editor的幫助下建立

AnyConnect配置檔案。下面是配置檔案的XML等效代碼段，供您參考。

<#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.將建立的XML配置檔案上傳到路由器的快閃記憶體並定義配置檔案：

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

11.禁用HTTP安全伺服器。

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

12.配置SSL授權策略。

```
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
```

SSL授權策略是推送到遠端客戶端的授權引數的容器。授權策略是從SSL配置檔案引用的。

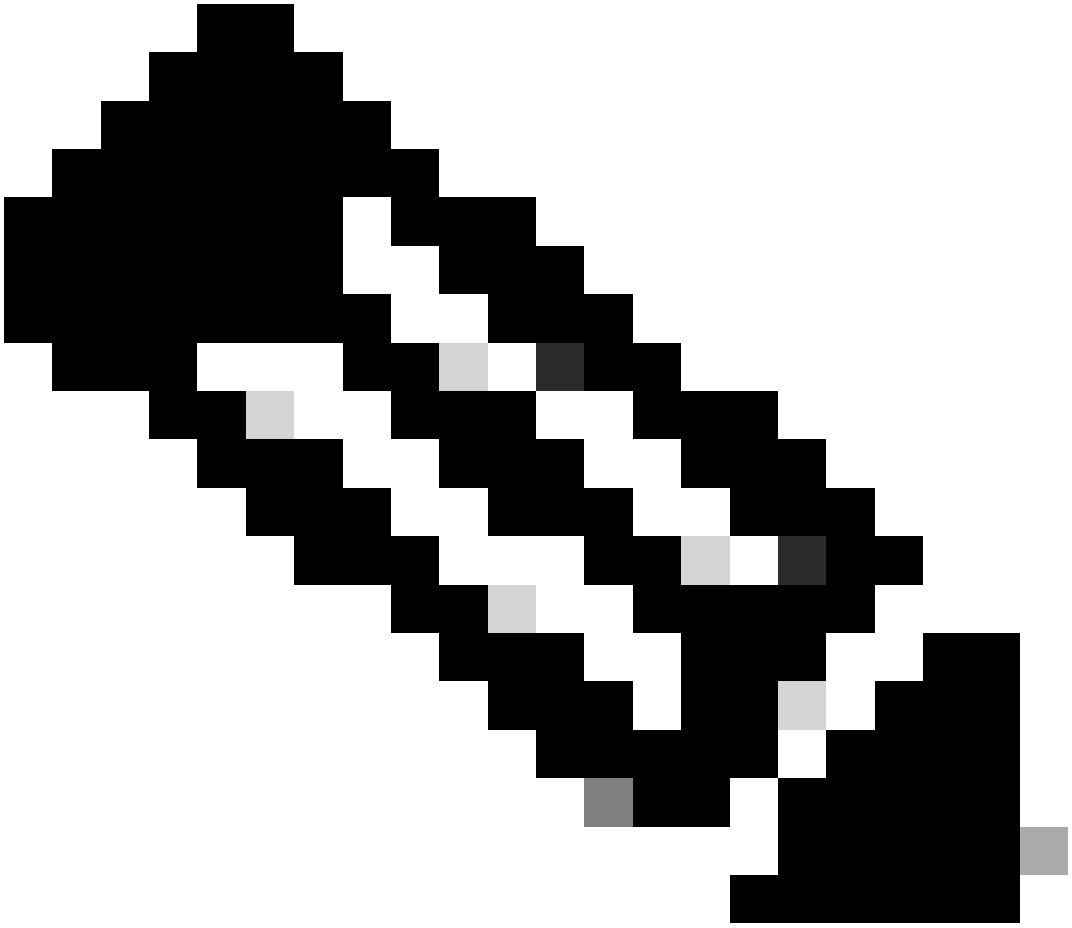
13.配置從中克隆虛擬訪問介面的虛擬模板。

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

14.配置SSL配置檔案並 定義身份驗證、記帳清單和虛擬模板。

```
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
```

配置檔案選擇取決於策略和URL值。



附註：策略和URL對於SSL VPN配置檔案必須是唯一的，並且必須至少指定一個授權方法才能啟動會話。

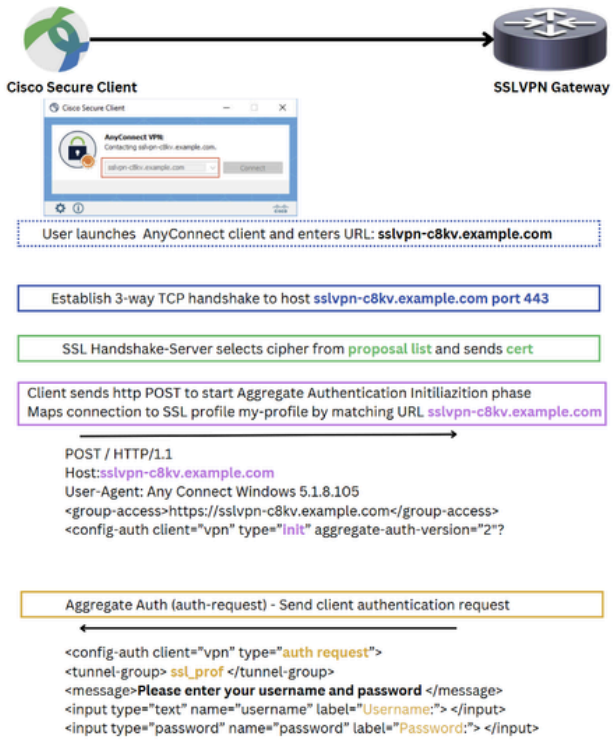
以下內容用於SSL配置檔案：

- match policy - match語句，用於為SSL策略名稱ssl_policy上的客戶端選擇SSL配置檔案ssl_prof。
- match url - match語句為URL sslvpn-c8kv.example.com上的客戶端選擇SSL配置檔案ssl_prof。
- aaa authentication user-pass list — 身份驗證期間使用SSLVPN_AUTHEN清單。
- aaa authorization group user-pass list — 在授權過程中，網路清單SSLVPN_AUTHOR與授權策略ssl_author_policy一起使用。
- authentication remote user-pass — 定義遠端客戶端的身份驗證模式基於使用者名稱/密碼。
- virtual-template 2 — 定義要克隆的虛擬模板。

連線流

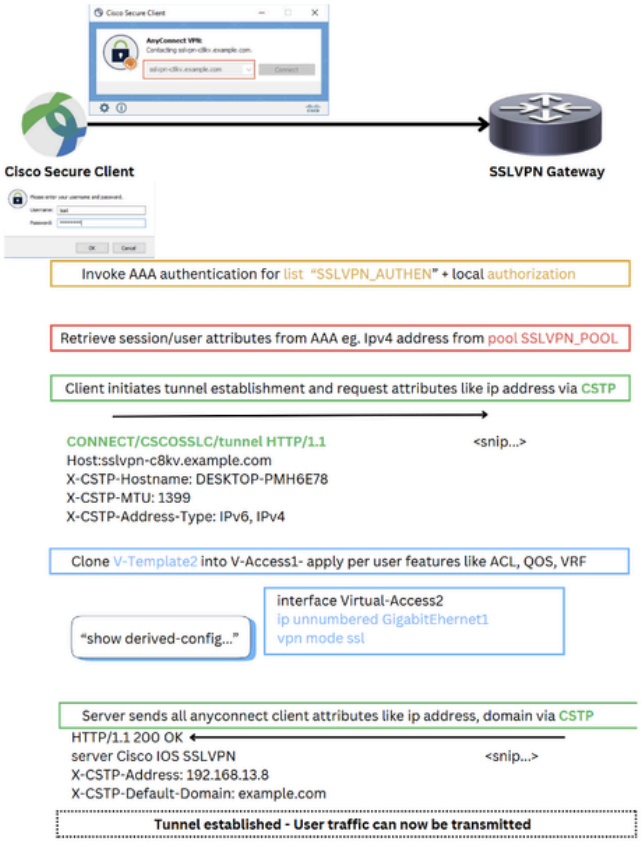
要瞭解在SSL VPN連線建立期間Cisco安全客戶端和安全網關之間發生的事件，請參閱[瞭解AnyConnect SSL VPN連線流的文檔]

思科安全客戶端(AnyConnect)到C8000v的高級別連線流




```
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
```

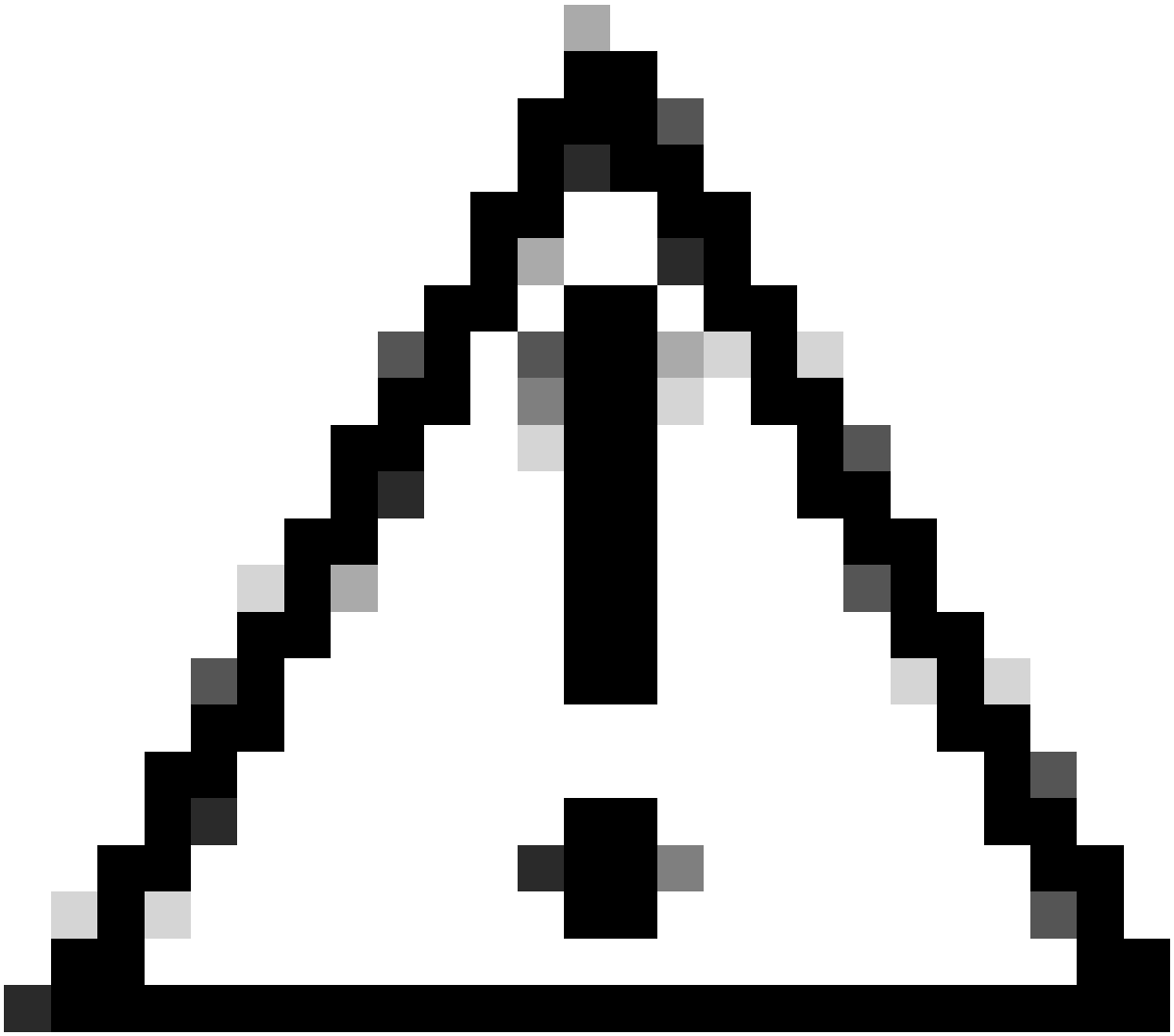
高級連線流1



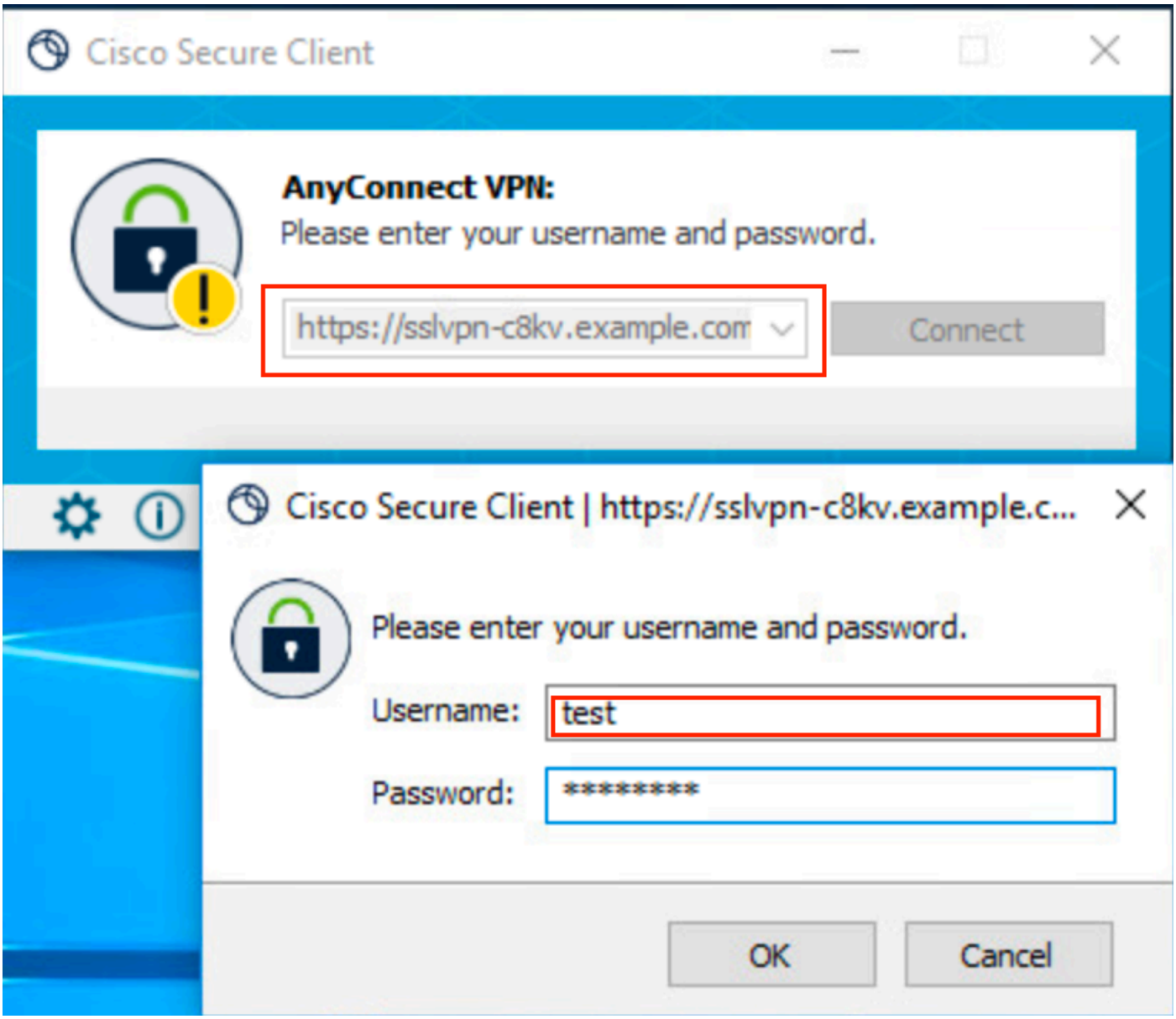

```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443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

驗證

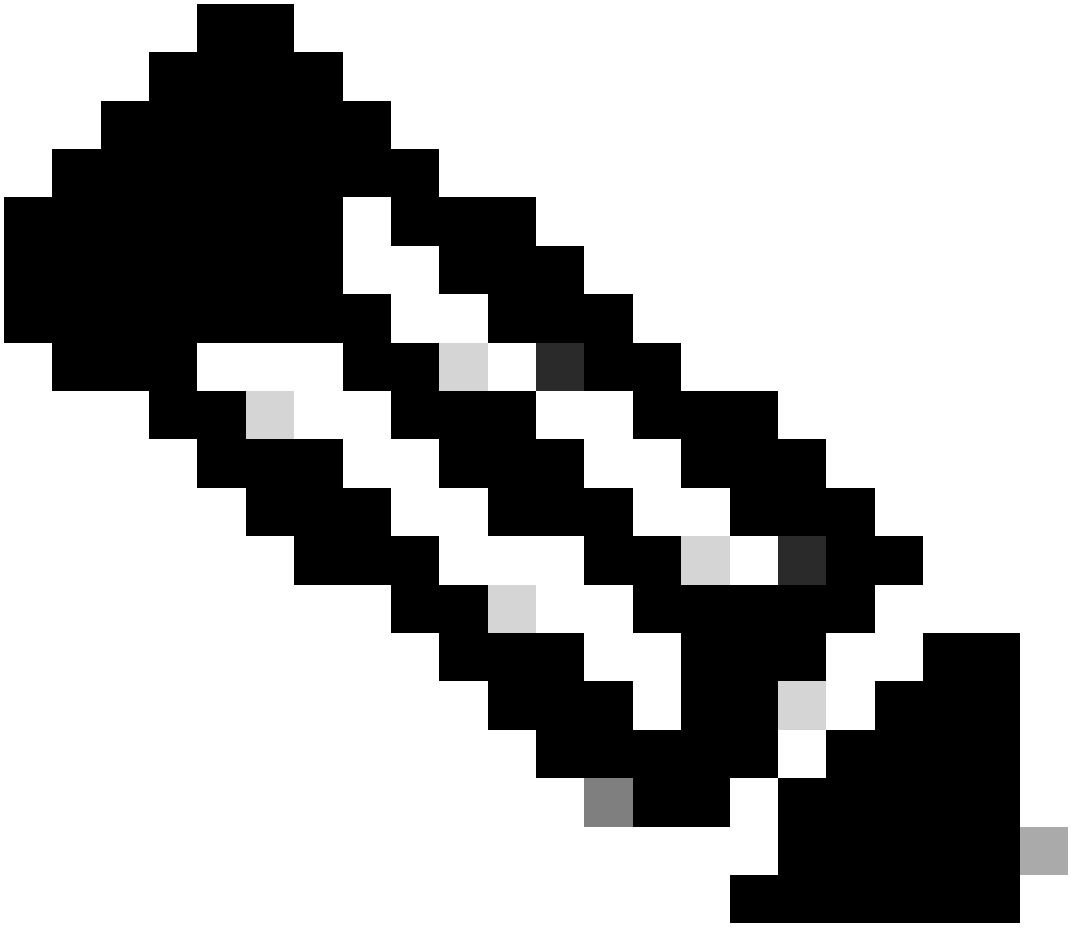
1.為了測試身份驗證，請從具有完全限定域名(FQDN)或C8000v IP地址的思科安全客戶端連線，然後輸入憑據。



注意：C8000v不支援從頭端下載客戶端軟體。Cisco Secure Client必須預先安裝在PC上。

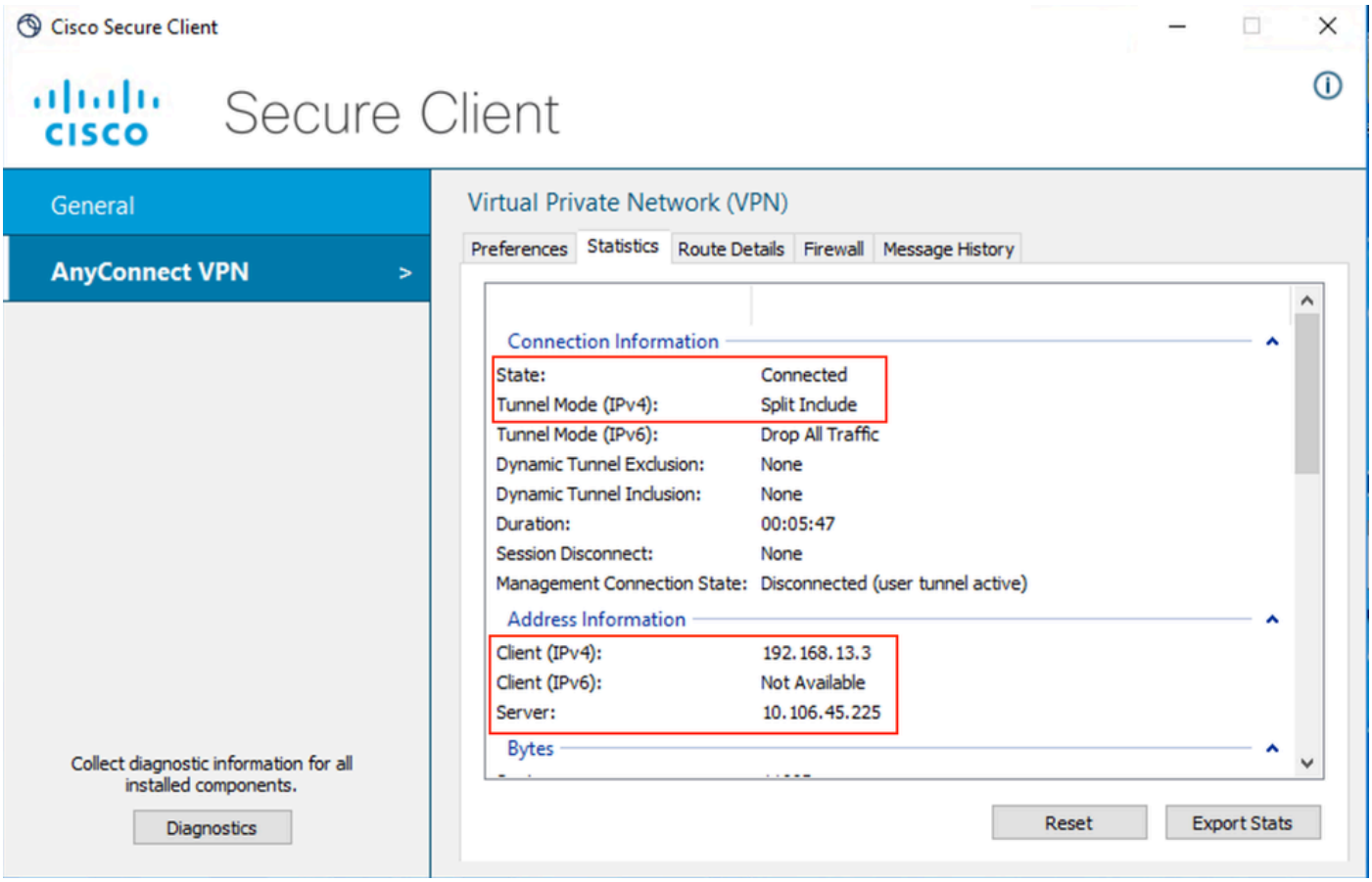


思科安全使用者端連線嘗試



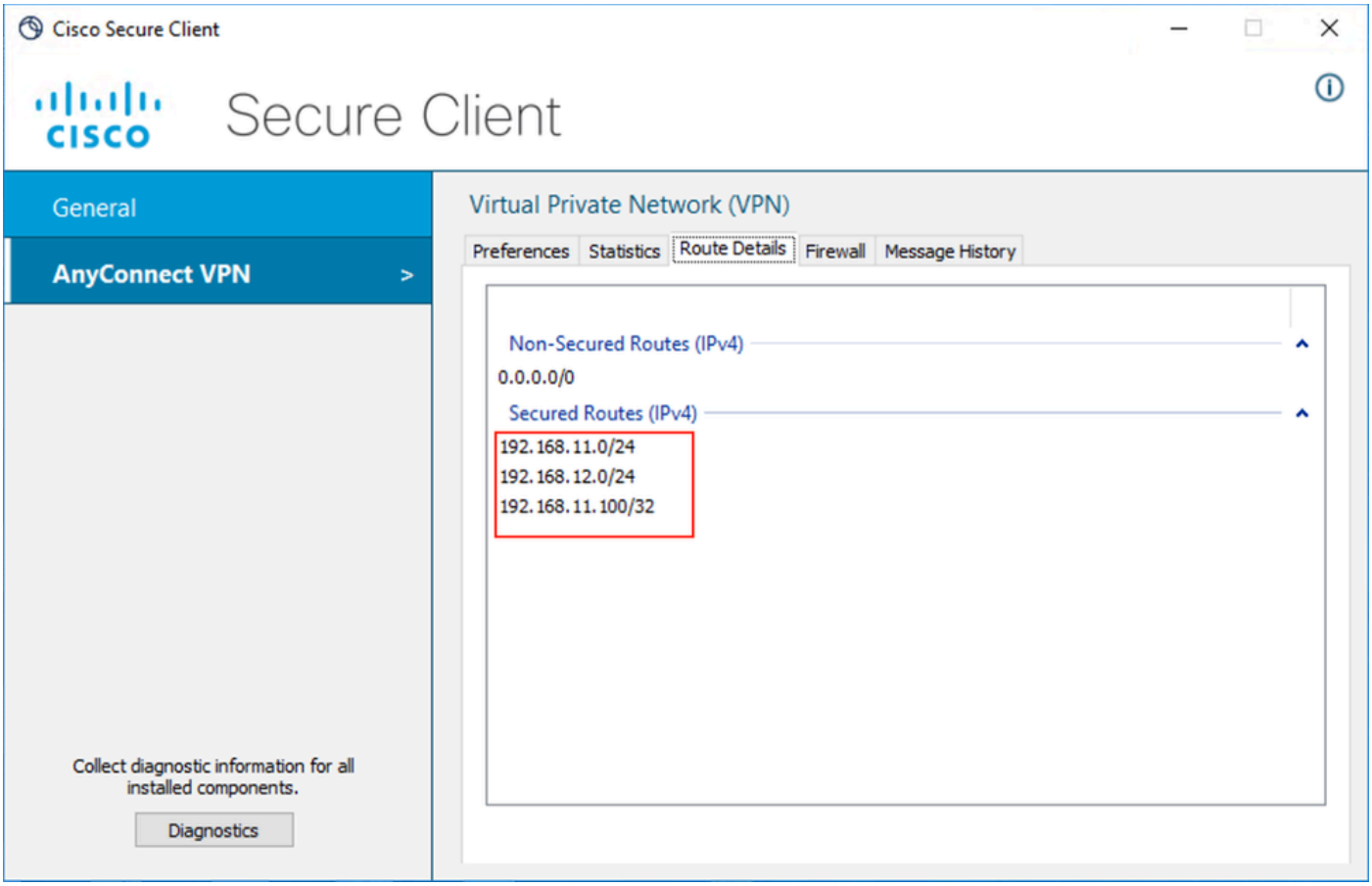
注意：全新安裝思科安全客戶端（未新增XML配置檔案）後，使用者可以在思科安全客戶端位址列中手動輸入VPN網關的FQDN。成功登入後，思科安全客戶端會預設嘗試下載XML配置檔案。但是，需要重新啟動Cisco Secure Client才能在GUI中顯示配置檔案。僅關閉Cisco Secure Client視窗是不夠的。要重新啟動該進程，請按一下右鍵Windows工作列中的Cisco Secure Client圖示，然後選擇Quit選項。

2.建立連線後，按一下左下角的gear圖示，然後導覽至AnyConnect VPN > Statistics。確認顯示的資訊與「連線和地址資訊」相對應。



Cisco Secure Client(AnyConnect)統計資訊

3.導航至 AnyConnectVPN >路由詳細資訊 並確認所顯示的資訊對應於安全路由和非安全路由。



思科安全客戶端(AnyConnect)路由詳細資訊

使用本節內容，確認您的組態是否在C8000v上正常運作：

1.顯示ssl會話資訊 — 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.顯示ssl vpn統計資訊 — 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.檢查應用於與客戶端關聯的虛擬訪問介面的實際配置。

<#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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. SSL調試，驗證頭端和客戶端之間的協商。

<#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. 一些用於驗證SSL配置的附加命令。

```
# 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.思科安全客戶端的診斷和報告工具(DART)。
要收集DART捆綁包，請執行運行DART以收集資料以進行故障排除中介紹的步驟

成功連線的調試示例：

```
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

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。