在C8000v上使用本地身份验证配置AnyConnect SSL VPN

目录

简介

本文档介绍如何使用本地用户数据库为AnyConnect SSL VPN配置Cisco IOS XE前端C8000v。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科IOS XE
- 思科安全客户端(CSC)
- 常规SSL操作
- 公用密钥基础结构 (PKI)

使用的组件

Th本文档中的信息基于以下软件和硬件版本：

- 运行版本17.16.01a的Cisco Catalyst 8000V(C8000V)
- 思科安全客户端5.1.8.105版
- 安装了Cisco Secure Client的客户端PC

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco IOS XE安全套接字层(SSL)VPN是基于路由器的解决方案，提供SSL VPN远程访问连接，并在融合数据、语音和无线平台上集成了业界领先的安全和路由功能。借助Cisco IOS XE SSL VPN，最终用户可以安全地从家庭或任何支持互联网的位置（如无线热点）进行访问。Cisco IOS XE SSL VPN还使公司能够将公司网络访问扩展到离岸合作伙伴和顾问，同时使公司数据始终受到保护。

以下特定平台支持此功能：

Platform	支持的Cisco IOS XE版本
思科云服务路由器1000V系列	思科IOS XE版本16.9
Cisco Catalyst 8000V	思科IOS XE班加罗尔17.4.1
Cisco 4461 集成业务路由器 Cisco 4451 集成业务路由器 Cisco 4431 集成业务路由器	思科IOS XE Cupertino 17.7.1a

配置

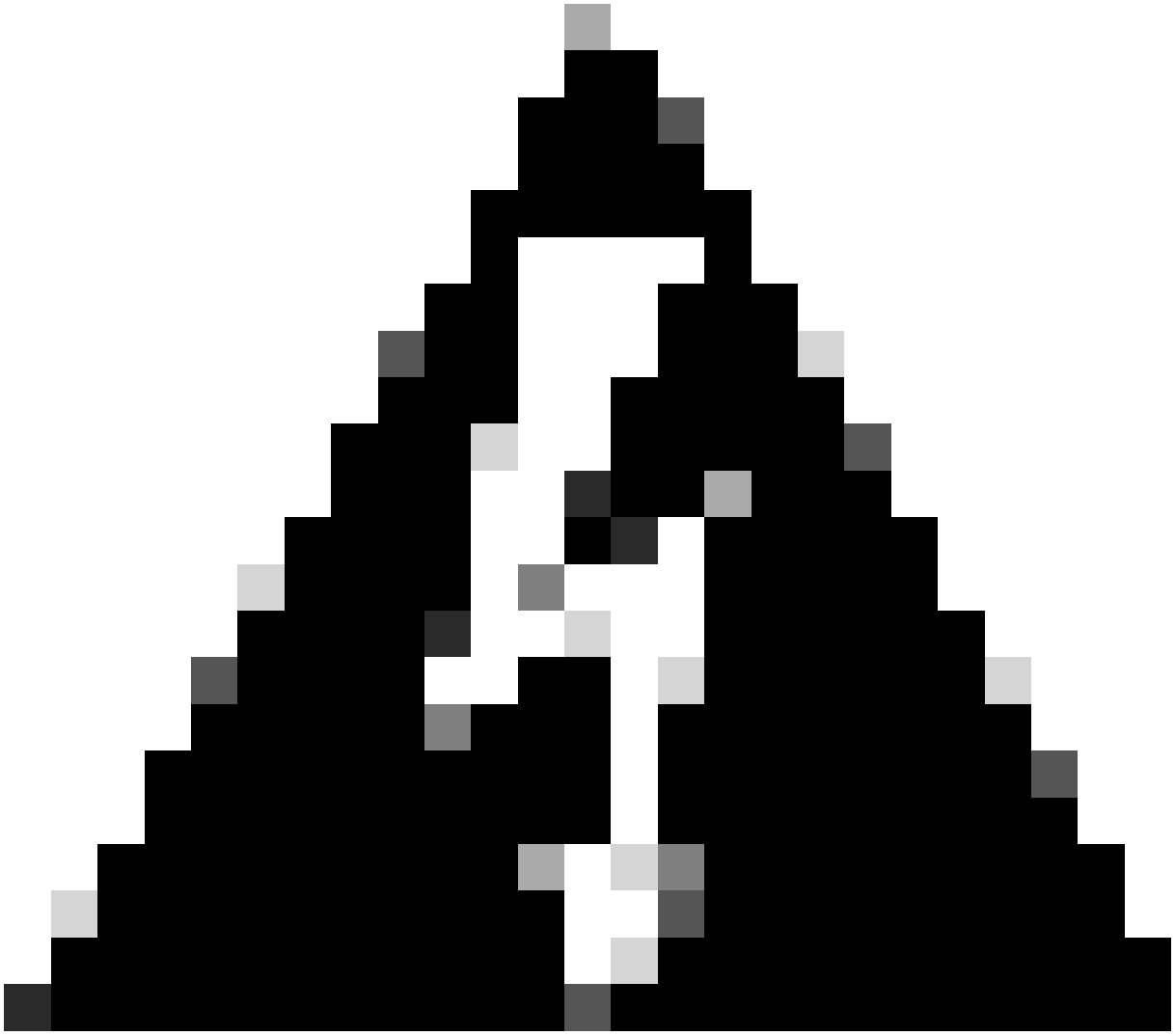
网络图

基本网络图

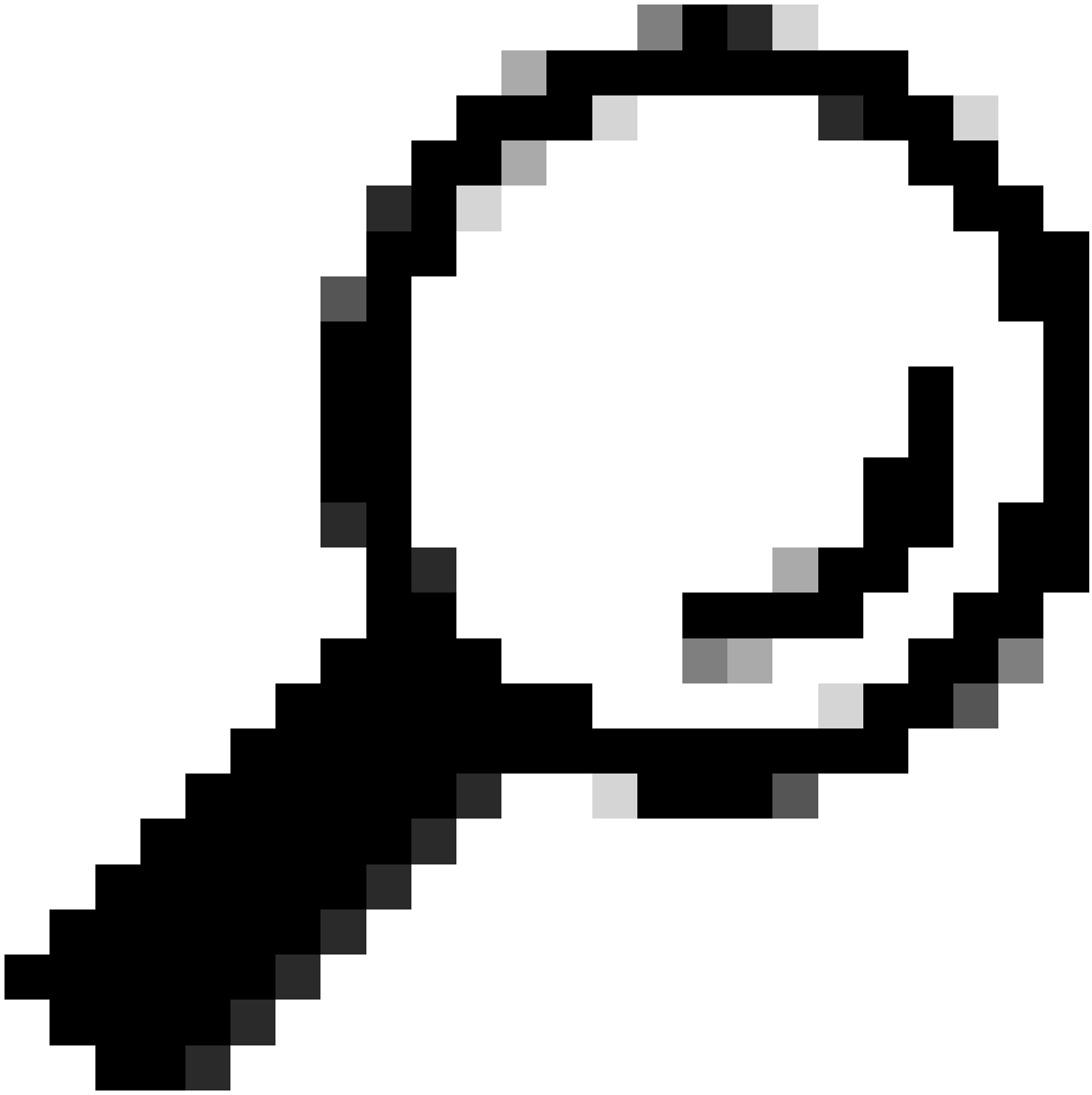
配置

1. 启用AAA，配置身份验证、授权列表，并向本地数据库添加用户名。

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



警告：aaa new-model 命令立即对所有线路和接口（控制台线路 line con 0 除外）应用本地身份验证。 如果在启用此命令后打开了到路由器的telnet会话（或者如果连接超时且必须重新连接），则必须使用路由器的本地数据库对用户进行身份验证。建议在启动AAA配置之前定义路由器的用户名和密码，这样就不会锁定路由器。



提示：在配置AAA命令之前，请保存配置。只有在完成AAA配置后（并确信该配置能正常工作），才能再次保存配置。 这允许您从意外锁定中恢复，因为您可以在重新加载路由器时回滚任何更改。

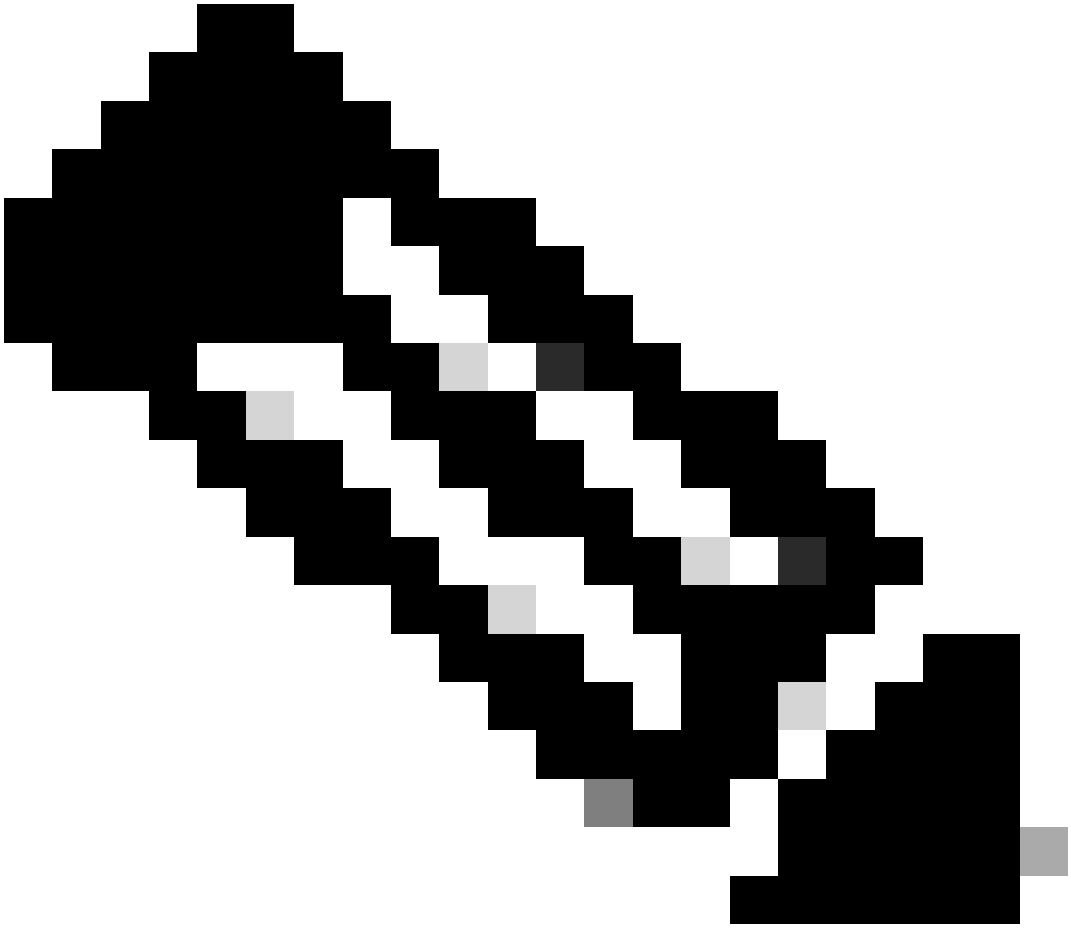
2.生成Rivest-Shamir-Adleman(RSA)密钥对。

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

3.创建信任点以安装路由器的身份证书。有关证书创建的详细信息，请参阅[如何为PKI配置证书注册]

。

```
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
```



注意：使用者名称中的公用名(CN)必须配置有用户用来连接到安全网关(C8000V)的IP地址或完全限定域名(FQDN)。 虽然不是强制性的，但正确输入CN有助于减少用户在登录时遇到的证书错误数量。

---

4. 定义IP本地池以向Cisco安全客户端分配地址。

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

5.（可选）配置用于拆分隧道的标准访问列表。此访问列表包括可通过VPN隧道访问的目标网络。默认情况下，如果未配置拆分隧道，则所有流量都会通过VPN隧道(Full Tunnel)。

```
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安全服务器。

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

7.配置SSL提议。

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

8.配置SSL策略，调用SSL建议和PKI信任点。

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

SSL策略定义在SSL协商期间使用的建议和信任点。它充当SSL协商所涉及的所有参数的容器。策略选择是通过将会话参数与策略下配置的会话参数匹配来进行的。

9.（可选）在思科安全客户端配置文件编辑器Cisco Secure Client Profile Editor的帮助下创建

AnyConnect配置文件。提供了配置文件的XML等效代码段以供参考。

<#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.将创建的XML配置文件上传到路由器的闪存并定义配置文件：

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

11.禁用HTTP安全服务器。

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

12.配置SSL授权策略。

```
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授权策略是推送到远程客户端的授权参数的容器。授权策略是从SSL配置文件引用的。

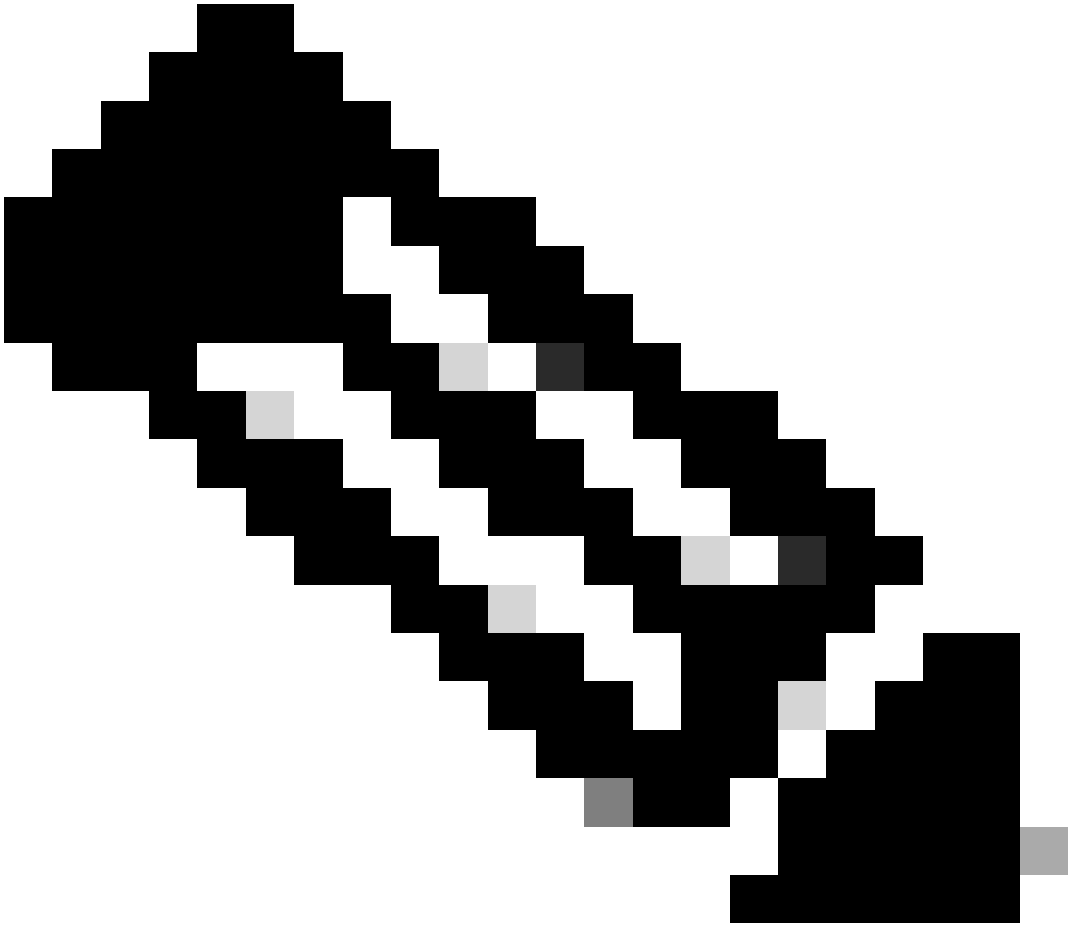
13.配置一个虚拟模板，从其中克隆虚拟访问接口。

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

14.配置SSL配置文件并 定义身份验证、记帐列表和虚拟模板。

```
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
```

配置文件选择取决于策略和URL值。



注意：策略和URL对于SSL VPN配置文件必须是唯一的，并且必须至少指定一个授权方法才能启动会话。

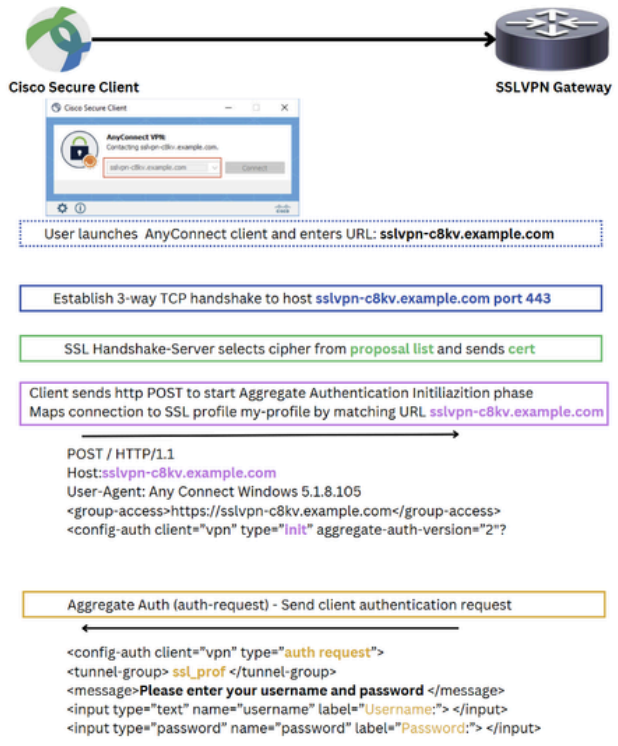
以下内容用于SSL配置文件中：

- match policy - match语句，用于为SSL策略名称ssl_policy上的客户端选择SSL配置文件ssl_prof。
- match url — 匹配语句，以便为URL sslvpn-c8kv.example.com上的客户端选择SSL配置文件ssl_prof。
- aaa authentication user-pass list — 在身份验证期间使用SSLVPN_AUTHEN列表。
- aaa authorization group user-pass list — 在授权过程中，网络列表SSLVPN_AUTHOR与授权策略ssl_author_policy一起使用。
- authentication remote user-pass — 定义远程客户端的身份验证模式基于用户名/密码。
- virtual-template 2 — 定义要克隆的虚拟模板。

连接流

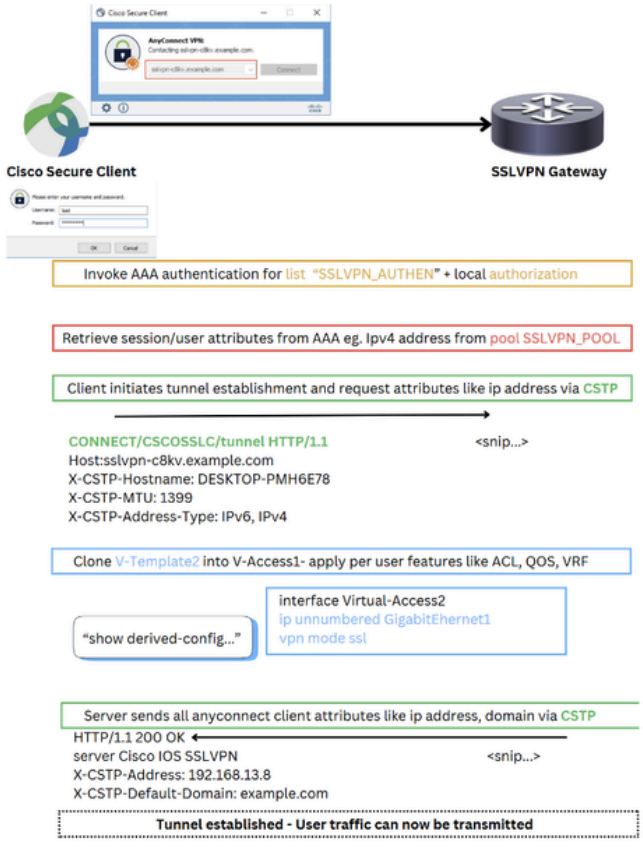
要了解Cisco安全客户端和安全网关在SSL VPN连接建立期间发生的事件，请参阅文档[了解AnyConnect SSL VPN连接流]

Cisco安全客户端(AnyConnect)到C8000v的高级连接流




```
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
```

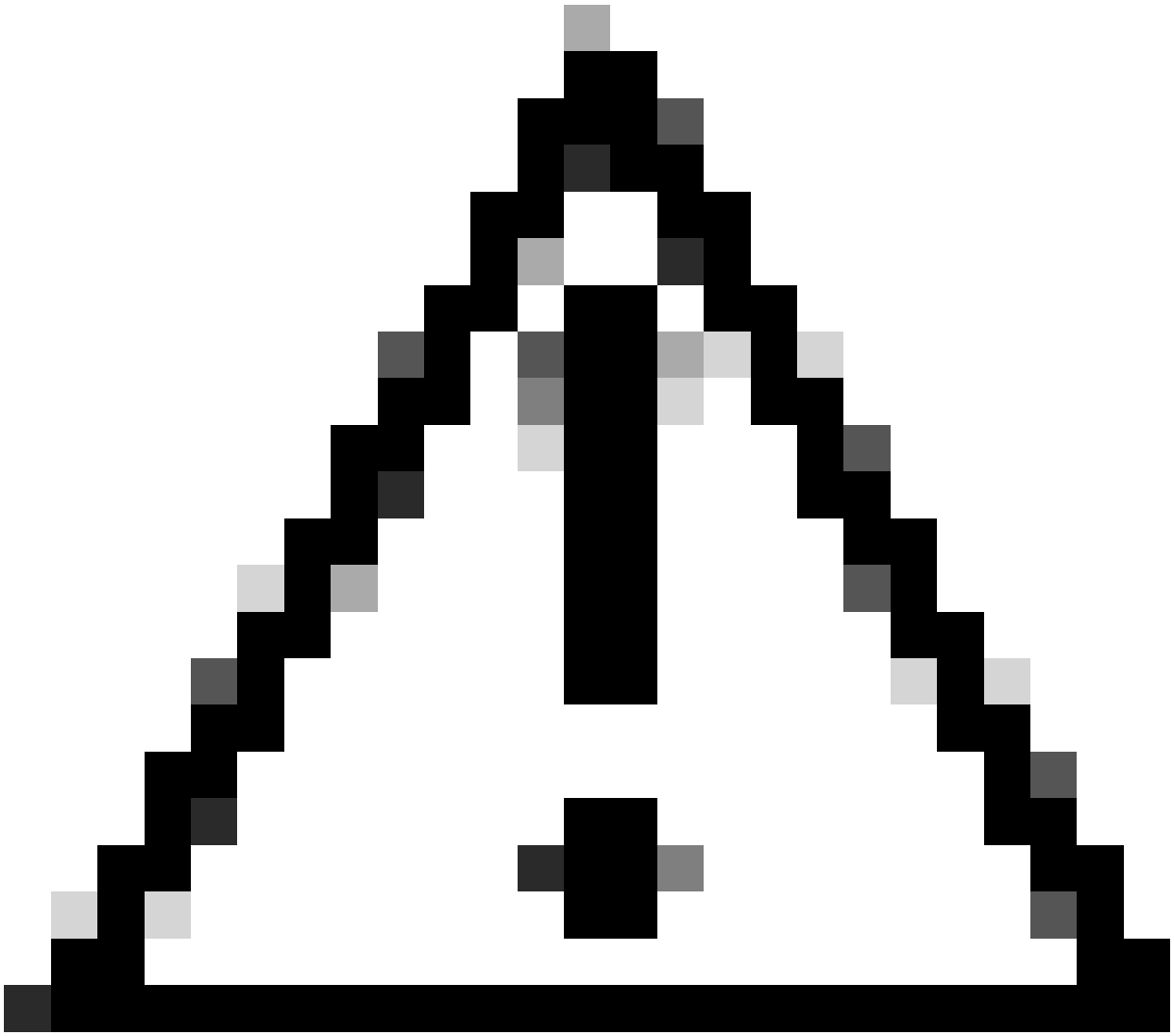
高级连接流1



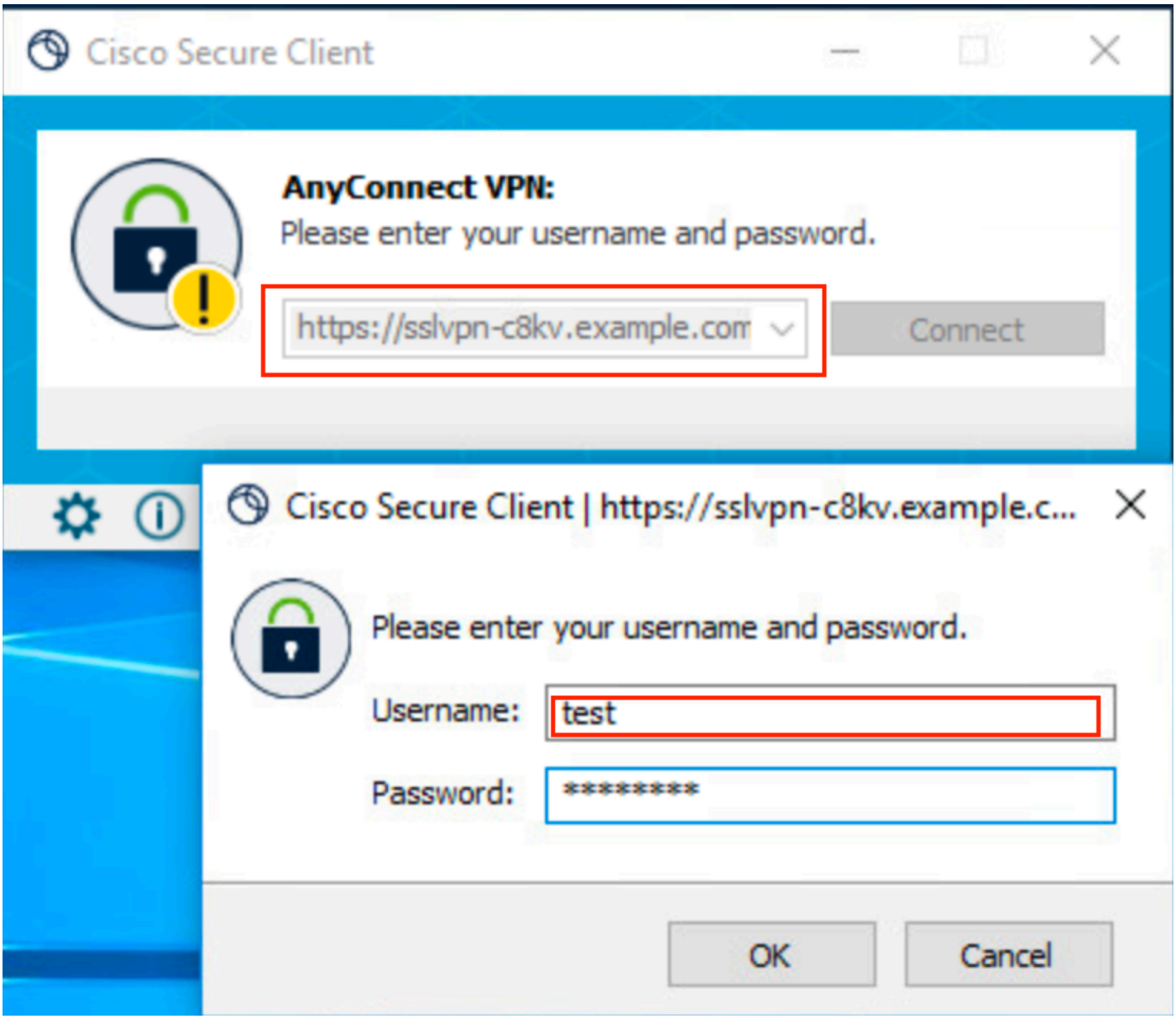

```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443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

验证

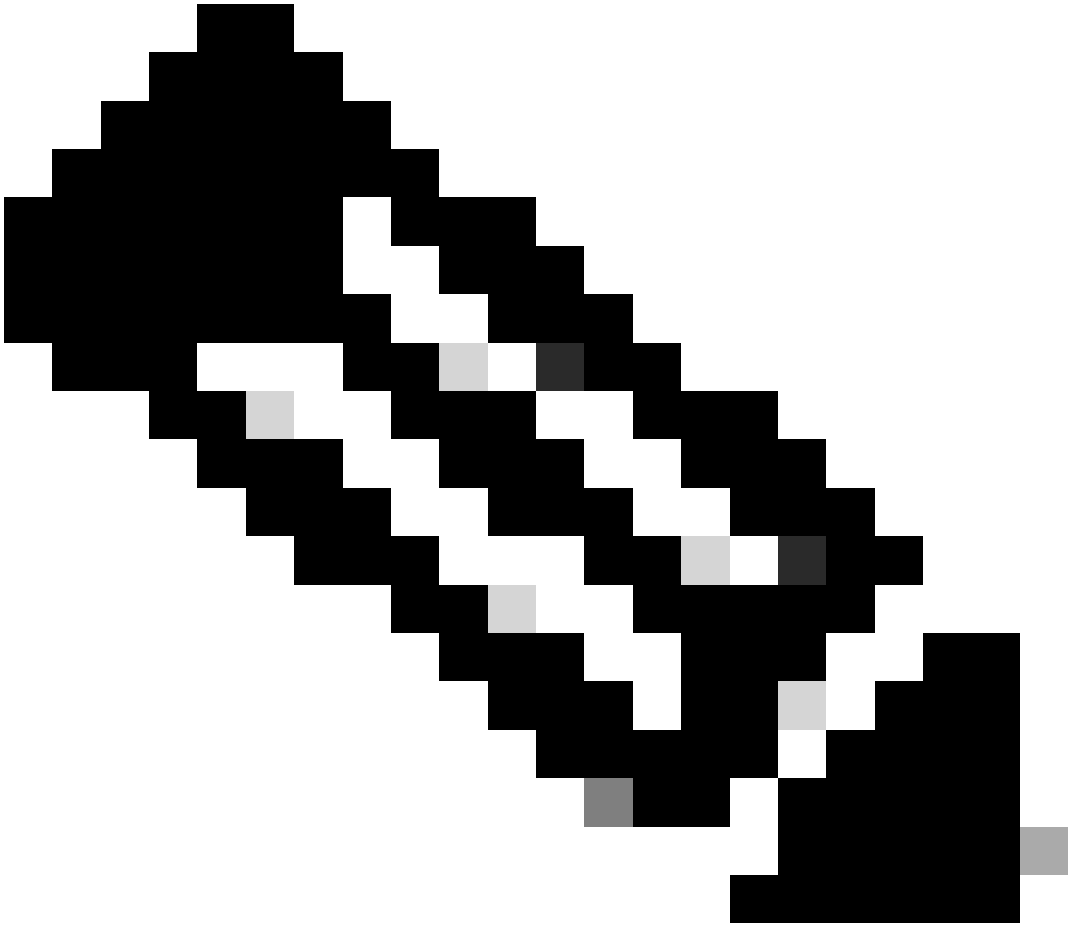
1.为了测试身份验证，请从Cisco安全客户端使用完全限定域名(FQDN)或C8000v的IP地址进行连接，然后输入凭证。



警告：C8000v不支持从头端下载客户端软件。必须在PC上预安装Cisco安全客户端。

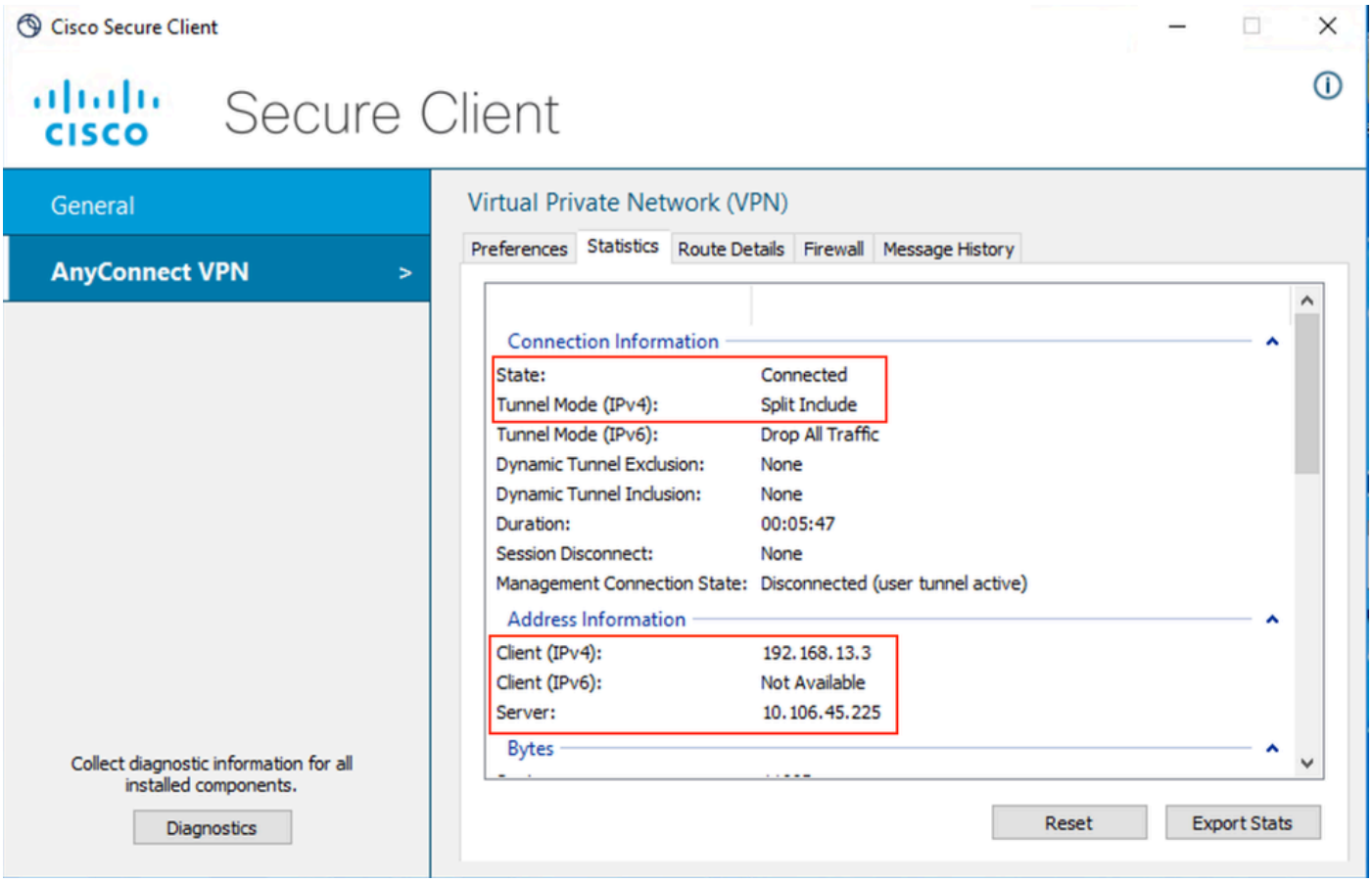


思科安全客户端连接尝试



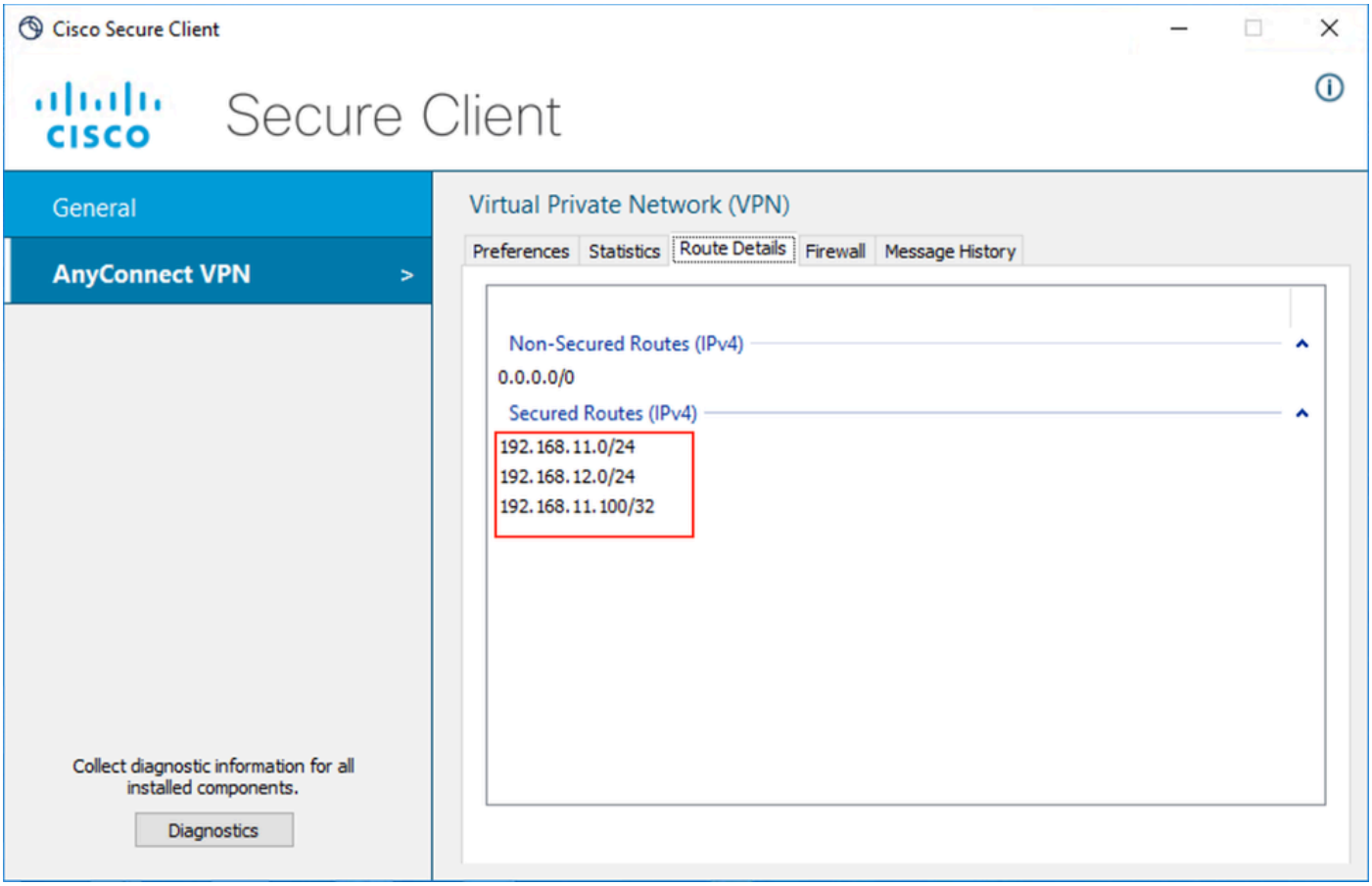
注：通过全新安装思科安全客户端（未添加XML配置文件），用户可以在Cisco安全客户端地址栏中手动输入VPN网关的FQDN。成功登录后，Cisco安全客户端会默认尝试下载XML配置文件。但是，需要重新启动Cisco安全客户端才能在GUI中显示配置文件。仅关闭Cisco Secure Client窗口是不够的。要重新启动该进程，请右键单击Windows任务栏中的Cisco Secure Client图标，然后选择Quit选项。

2.建立连接后，单击左下角的gear图标，然后导航到AnyConnect VPN > Statistics。确认显示的信息与“连接和地址信息”对应。



思科安全客户端(AnyConnect)统计信息

3.导航至 AnyConnectVPN >路由详细信息 并确认所显示的信息对应于安全路由和非安全路由。



思科安全客户端(AnyConnect)路由详细信息

使用此部分可确认您的配置在C8000v上是否正常工作：

1.显示ssl会话信息 — 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.显示ssl vpn统计信息 — 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.检查应用于与客户端关联的虚拟访问接口的实际配置。

<#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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

1. SSL调试，用于验证头端和客户端之间的协商。

<#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. 用于验证SSL配置的几个附加命令。

```
# 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.思科安全客户端的诊断和报告工具(DART)。
要收集DART捆绑包，请执行运行DART以收集数据以进行故障排除中介绍的步骤

成功连接的调试示例：

```
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

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。