Configurar o AnyConnect SSL VPN no C8000v com autenticação local

Contents

Introdução

Este documento descreve como configurar o Cisco IOS XE Headend C8000v para AnyConnect SSL VPN com um banco de dados de usuário local.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco IOS XE
- Cisco Secure Client (CSC)
- Operação geral de SSL
- Public Key Infrastructure (PKI)

Componentes Utilizados

OAs informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Catalyst 8000V (C8000V) executando a versão 17.16.01a
- Cisco Secure Client versão 5.1.8.105
- PC cliente com Cisco Secure Client instalado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A VPN Secure Socket Layer (SSL) do Cisco IOS XE é uma solução baseada em roteador que oferece conectividade de acesso remoto VPN SSL integrada com recursos de segurança e roteamento líderes do setor em uma plataforma convergente de dados, voz e sem fio. Com a VPN SSL do Cisco IOS XE, os usuários finais obtêm acesso com segurança de casa ou de qualquer local habilitado para Internet, como hotspots sem fio. A VPN SSL do Cisco IOS XE também permite que as empresas estendam o acesso à rede corporativa para parceiros e consultores no exterior, mantendo os dados corporativos protegidos o tempo todo.

Este recurso é suportado nas seguintes plataformas:

Platform	Versão suportada do Cisco IOS XE
Roteador de serviços em nuvem Cisco 1000V Series	Cisco IOS XE versão 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bengaluru 17.4.1
Roteador de serviços integrados Cisco 4461 Roteador de serviços integrados Cisco 4451 Roteador de serviços integrados Cisco 4431	Cisco IOS XE Cupertino 17.7.1a

Configurar

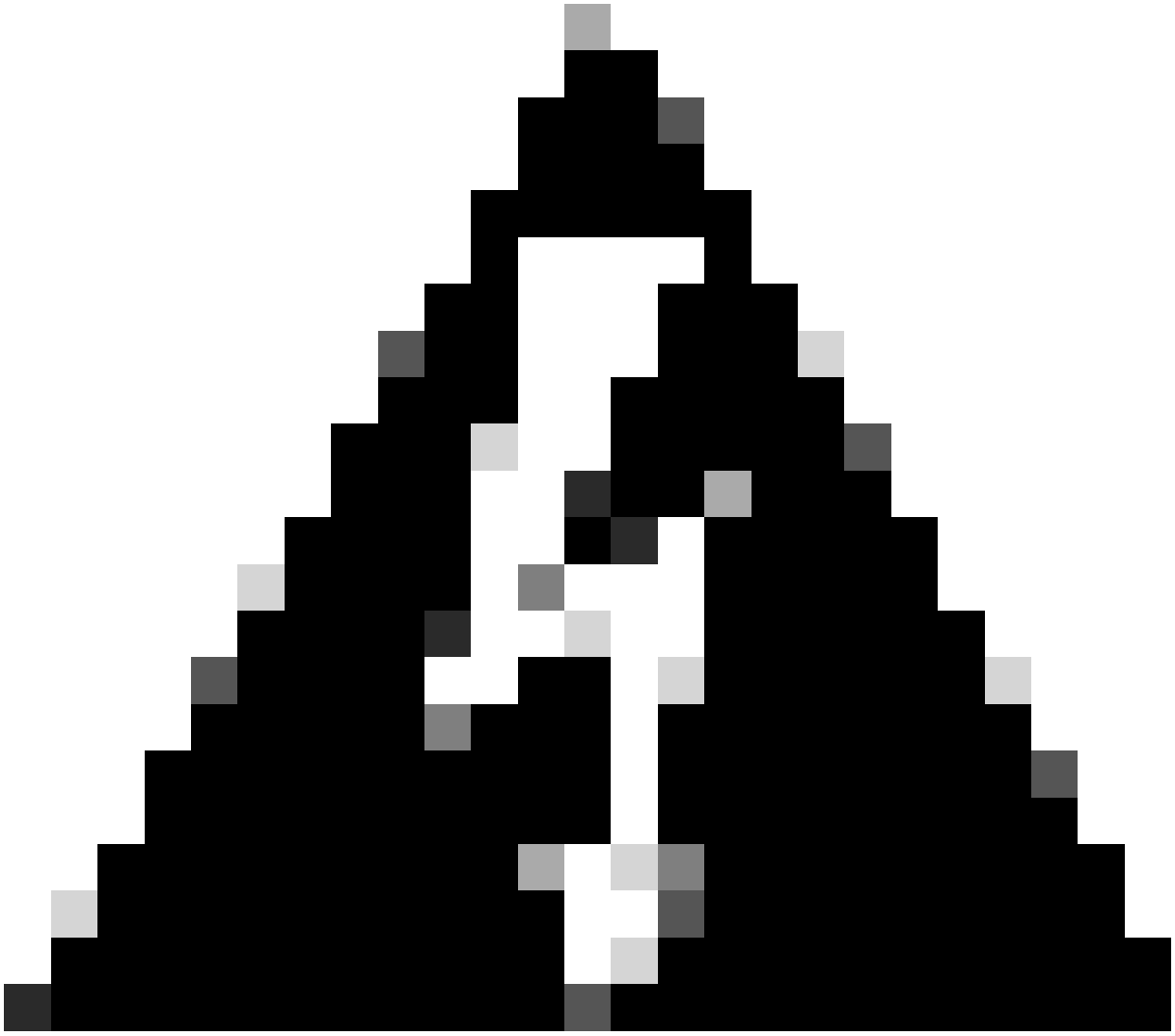
Diagrama de Rede

Diagrama básico de rede

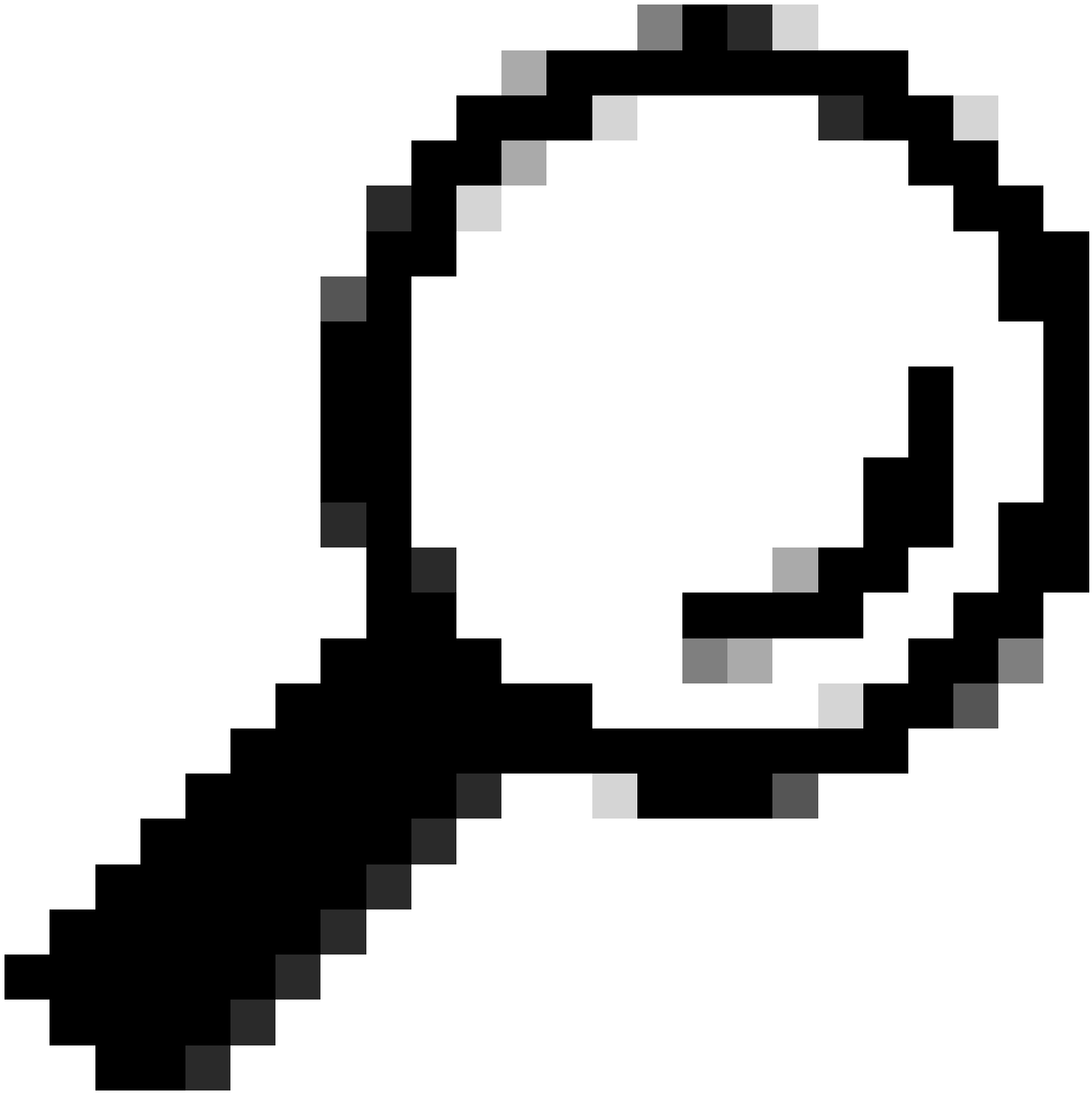
Configurações

1. Ative o AAA, configure a autenticação, as listas de autorização e adicione um nome de usuário ao banco de dados local.

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



aviso: O comando aaa new-model aplica imediatamente a autenticação local a todas as linhas e interfaces (com exceção da linha de console line con 0). Se uma sessão telnet for aberta para o roteador depois que esse comando for ativado (ou se o tempo limite de uma conexão for excedido e for necessário reconectar), o usuário deverá ser autenticado com o banco de dados local do roteador. É recomendável definir um nome de usuário e uma senha no roteador antes de iniciar a configuração AAA, para que você não seja bloqueado no roteador.



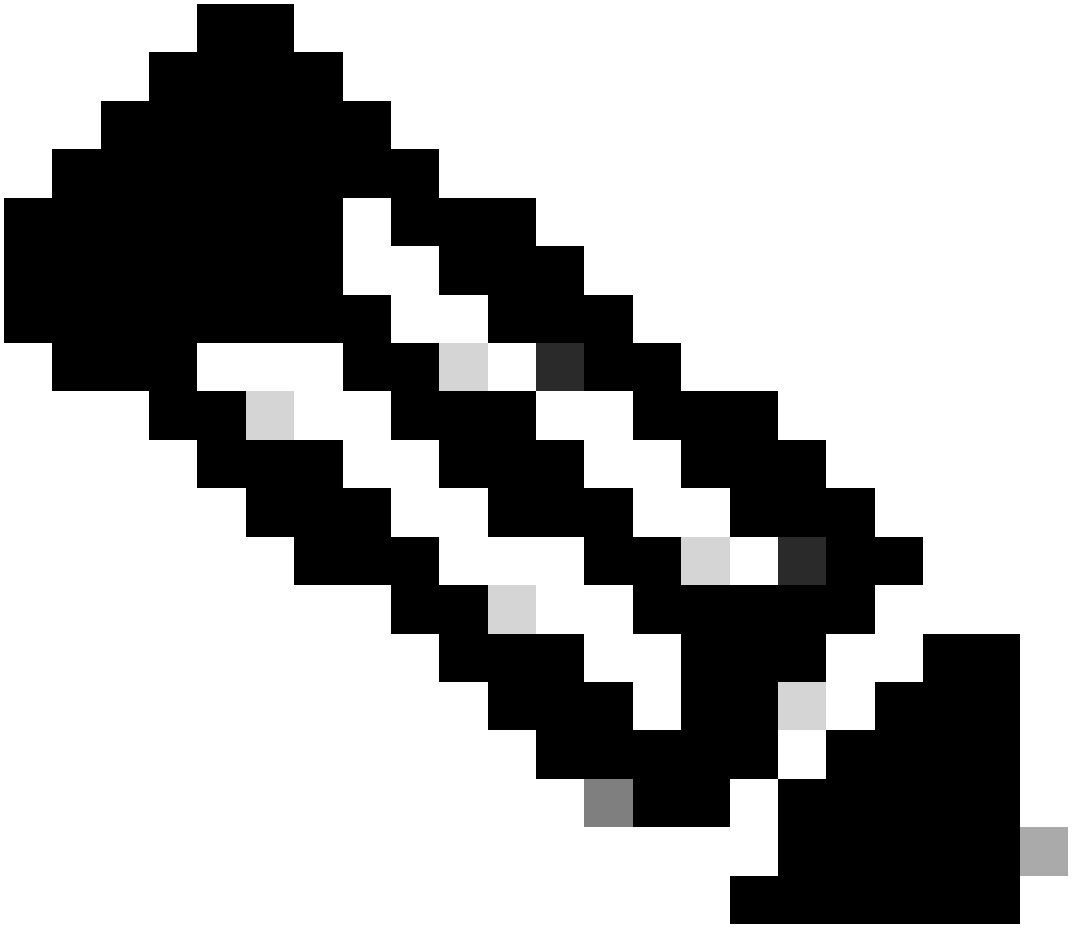
Tip: Antes de configurar os comandos AAA, salve sua configuração. Você pode salvar a configuração novamente somente depois de ter concluído sua configuração AAA (e estiver satisfeito que ela funciona corretamente). Isso permite que você se recupere de bloqueios inesperados, pois pode reverter qualquer alteração com uma recarga do roteador.

2.Gere o par de chaves Rivest-Shamir-Adleman (RSA).

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

3. Crie um ponto confiável para instalar o certificado de identidade do roteador. Você pode consultar Como configurar a inscrição de certificado para uma PKI para obter mais detalhes sobre a criação do certificado.

```
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
```



Note: O Nome comum (CN) no Nome do assunto deve ser configurado com o endereço IP ou o Nome de domínio totalmente qualificado (FQDN) que os usuários usam para se conectar ao Secure Gateway (C8000V). Embora não seja obrigatório, a inserção correta

---

do CN pode ajudar a reduzir o número de erros de certificado encontrados pelos usuários no login.

4. Defina um pool IP local para atribuir endereços ao Cisco Secure Client.

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

5. (Opcional) Configure uma lista de acesso padrão a ser usada para o túnel dividido. Essa lista de acesso consiste nas redes de destino que podem ser acessadas através do túnel VPN. Por padrão, todo o tráfego passa pelo túnel VPN (túnel completo) se o túnel dividido não estiver configurado.

```
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.Desabilite o servidor seguro HTTP.

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

7. Configure uma proposta SSL.

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

8. Configure uma política SSL, chame a proposta SSL e o ponto de confiança PKI.

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

```
ip interface GigabitEthernet1 port 443
```

A política SSL define a proposta e o ponto de confiança a serem usados durante a negociação SSL. Ele serve como um contêiner para todos os parâmetros envolvidos na negociação SSL. A seleção da política é feita pela correspondência dos parâmetros da sessão com aqueles configurados sob a política.

9. (Opcional) Crie um perfil do AnyConnect com a ajuda do Cisco Secure Client Profile Editor Cisco Secure Client Profile Editor . Um trecho de XML equivalente do perfil é fornecido para sua referência.

<#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. Carregue o perfil XML criado na memória flash do roteador e defina o perfil:

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

11.Desabilite o servidor seguro HTTP.

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

12. Configure a Política de Autorização 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
```

A política de autorização SSL é um contêiner de parâmetros de autorização que são enviados para o cliente remoto.A política de autorização é referenciada no perfil SSL.

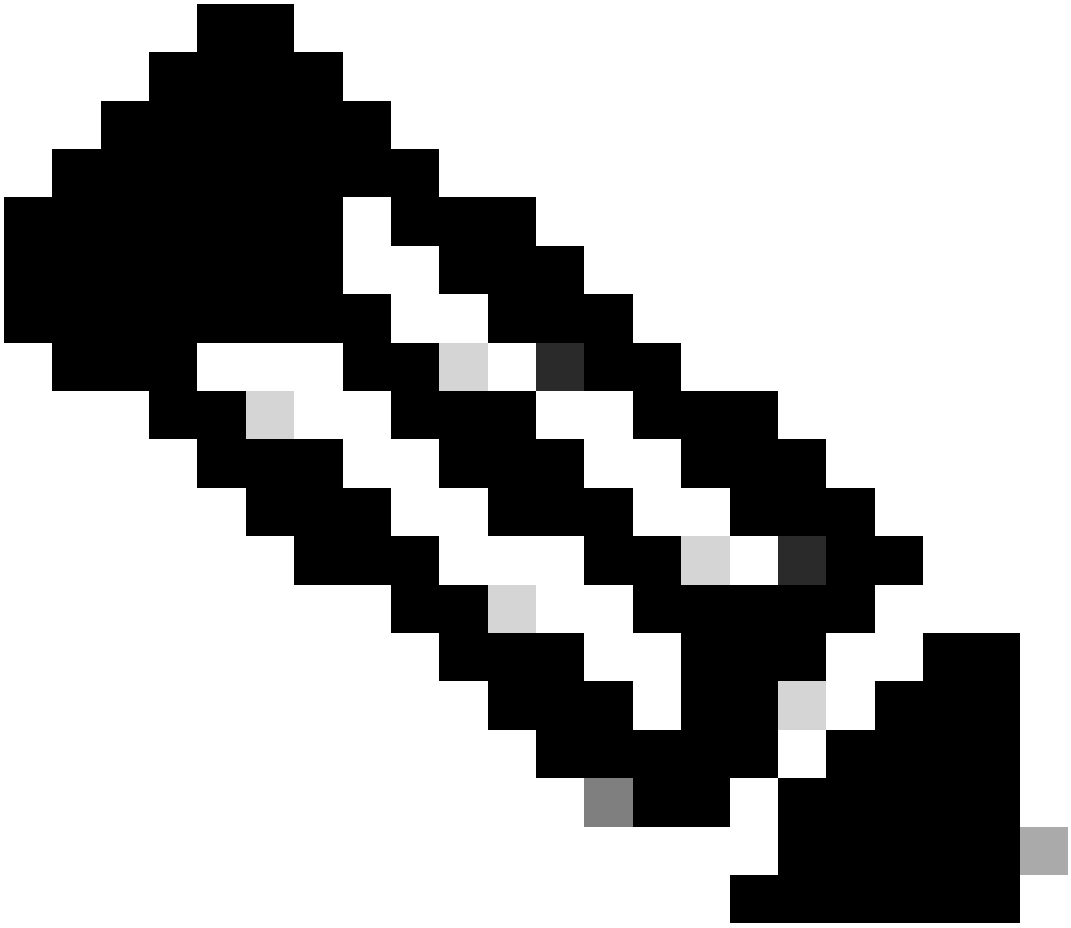
13. Configure um molde Virtual a partir do qual as interfaces de acesso virtual sejam clonadas.

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

14. Configurar um perfil SSL e defina a autenticação , as listas de contabilidade e o modelo virtual.

```
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
```

A seleção de um perfil depende dos valores da política e da URL.



Note: A política e a URL devem ser exclusivas para um perfil de VPN SSL e pelo menos um método de autorização deve ser especificado para ativar a sessão.

Eles são usados no perfil SSL:

- match policy - combine a instrução para selecionar um perfil SSL ssl_prof para um cliente no nome da política SSL ssl_policy.
- match url - corresponda instruções para selecionar um perfil SSL ssl_prof para um cliente no diretório URL sslvpn-c8kv.example.com.
- aaa authentication user-pass list - Durante a autenticação, a lista SSLVPN_AUTHEN é usada.
- aaa authorization group user-pass list - Durante a autorização, a lista de rede SSLVPN_AUTHOR é usada com a política de autorização ssl_author_policy.
- authentication remote user-pass - Define o modo de autenticação do cliente remoto com base em nome de usuário/senha.
- virtual-template 2 - Define o modelo virtual a ser clonado.

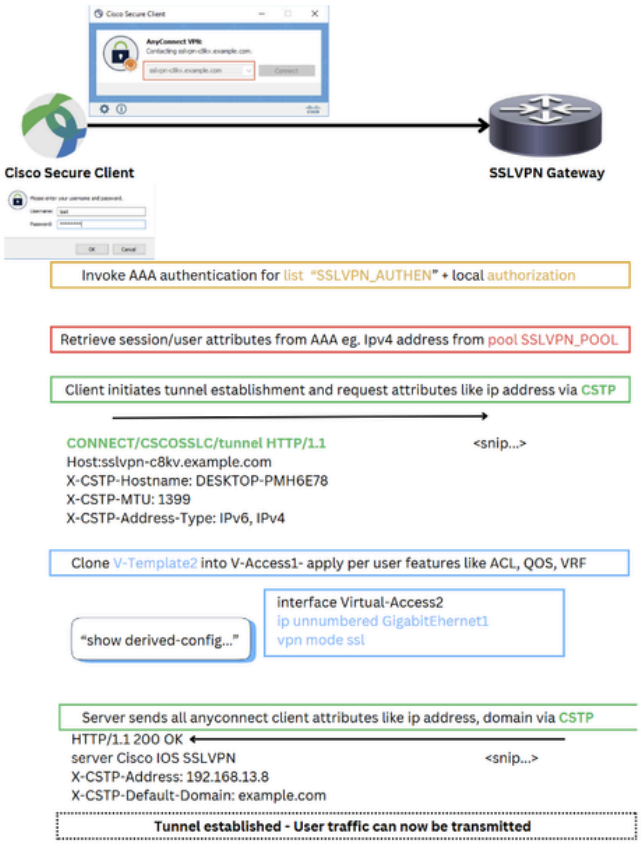
Fluxo de conexão

Para entender os eventos que ocorrem entre o Cisco Secure Client e o Secure Gateway durante o estabelecimento de uma conexão VPN SSL, consulte o documento [Entendendo o fluxo de conexão VPN SSL do AnyConnect]

Cisco Secure Client (AnyConnect) para fluxo de conexão de alto nível do 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
```

Fluxo de conexão de alto nível 1

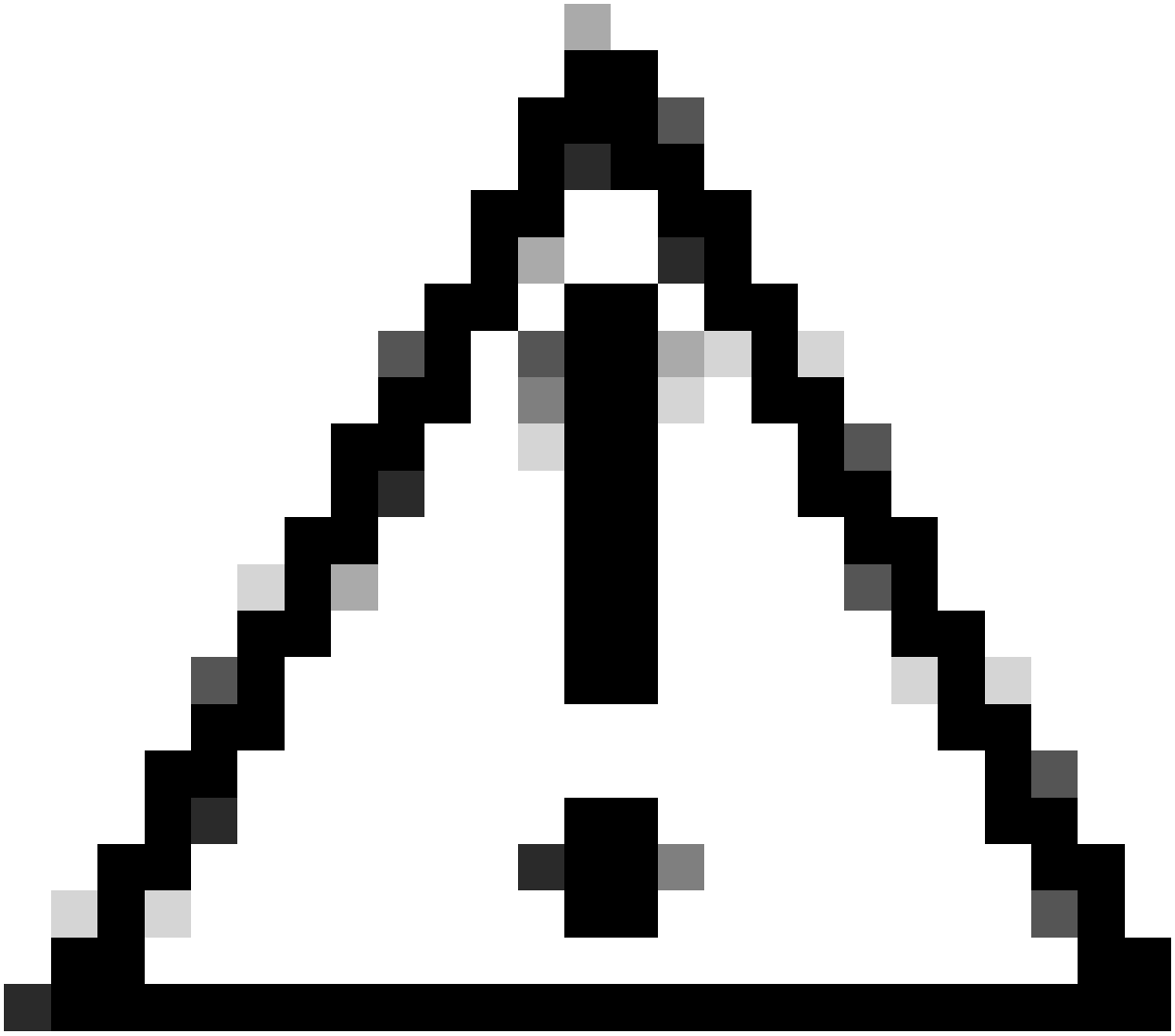



```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443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

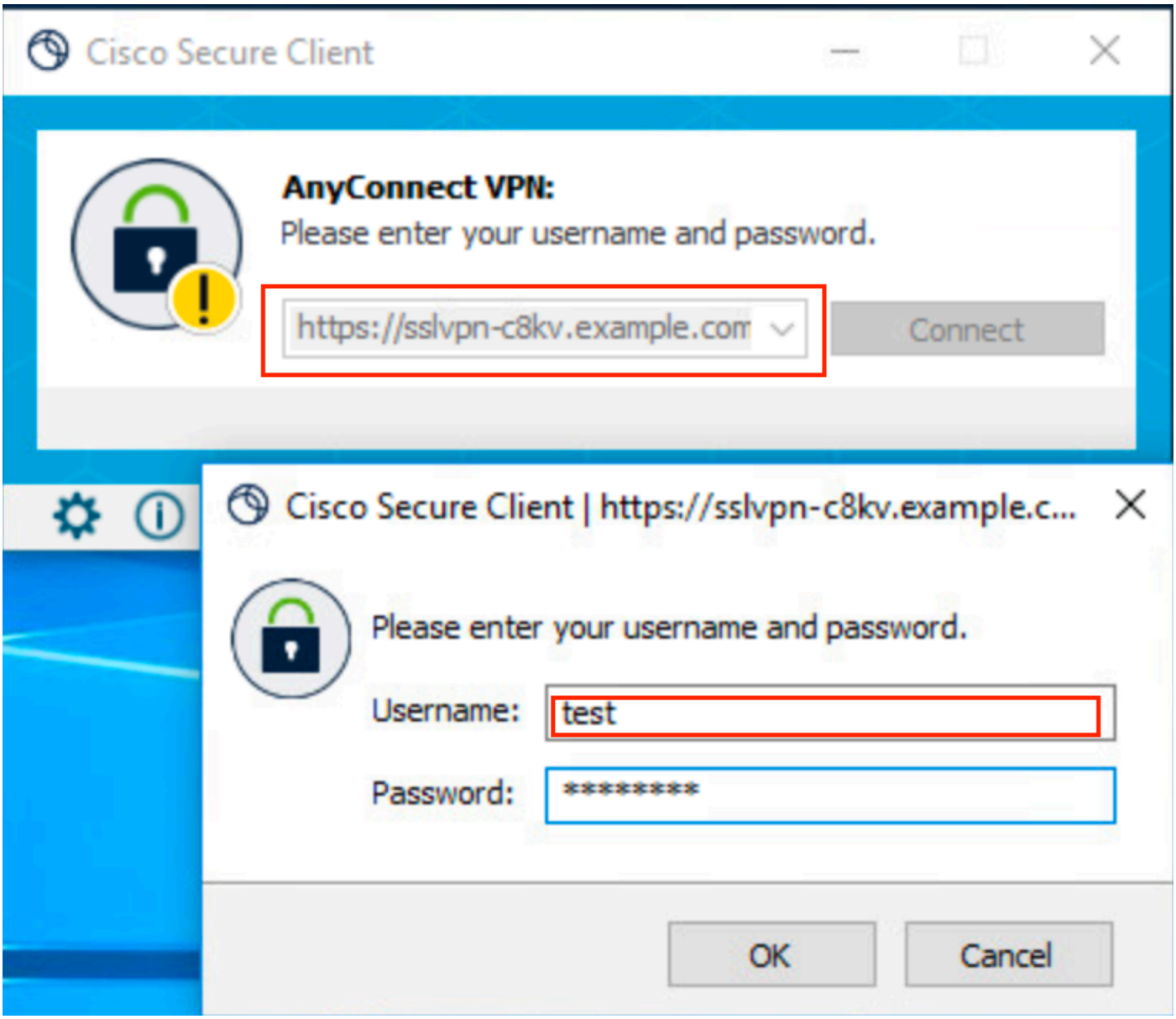
Fluxo de conexão de alto nível 2

Verificar

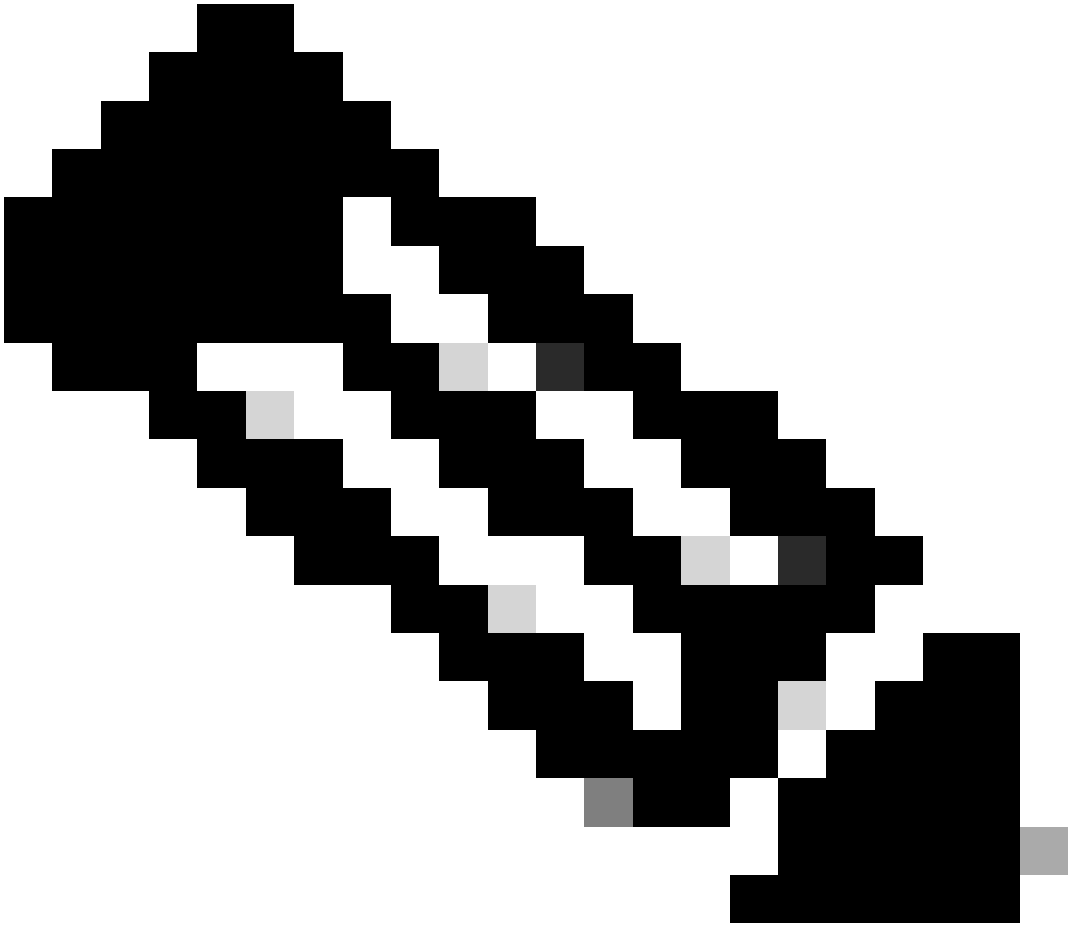
1. Para testar a autenticação, conecte-se do Cisco Secure Client com o Fully Qualified Domain Name (FQDN) ou o endereço IP do C8000v e insira as credenciais.



Caution: O C8000v não suporta download de software cliente do headend. O Cisco Secure Client deve ser pré-instalado no PC.



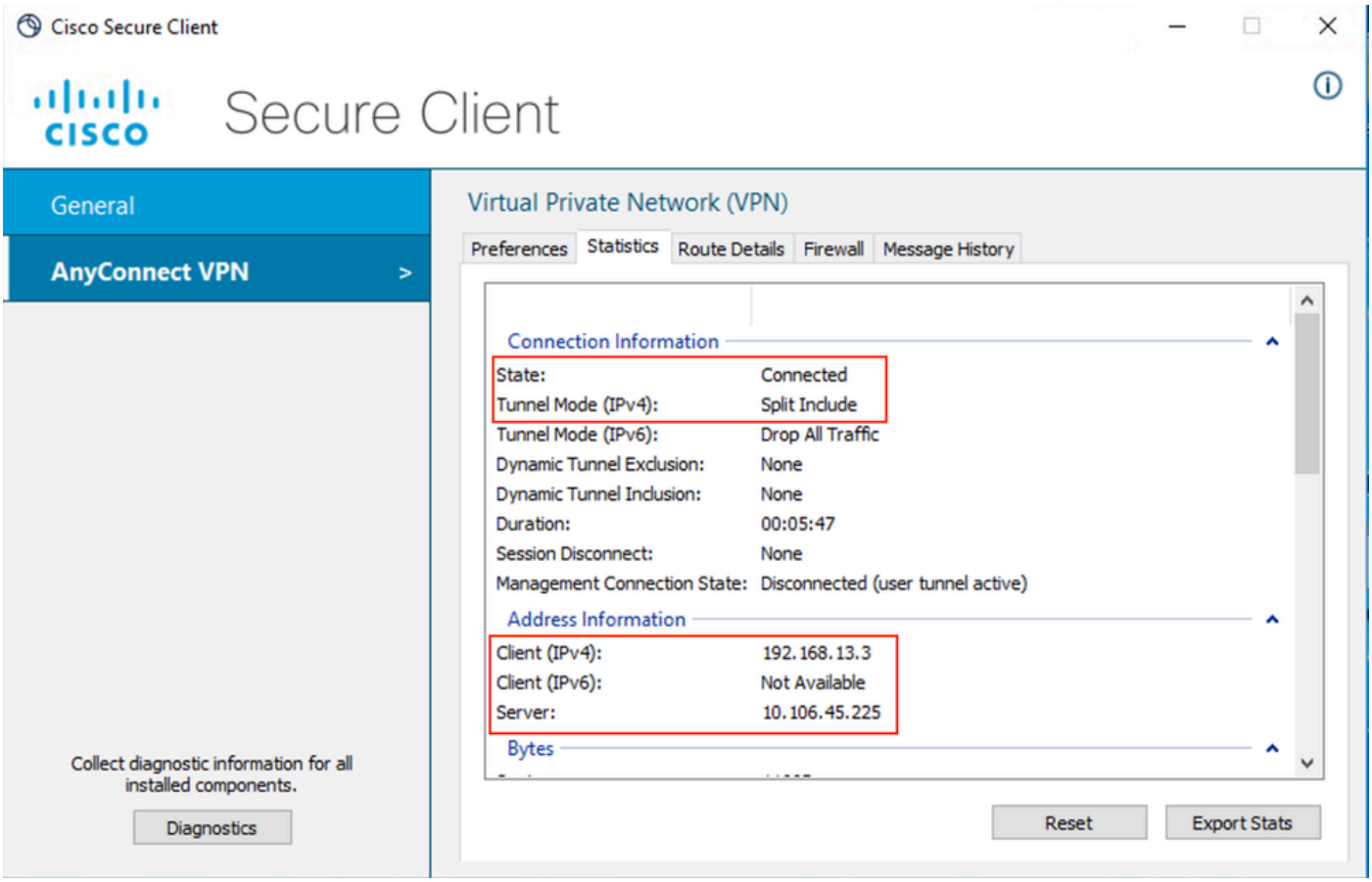
Tentativa de conexão do Cisco Secure Client



Observação: com uma nova instalação do Cisco Secure Client (sem perfis XML adicionados), o usuário pode inserir manualmente o FQDN do gateway VPN na barra de endereços do Cisco Secure Client. Após um login bem-sucedido, o Cisco Secure Client tenta fazer o download do perfil XML por padrão. No entanto, o Cisco Secure Client precisa ser reiniciado para que o perfil seja exibido na GUI. Fechar simplesmente a janela do Cisco Secure Client não é suficiente. Para reiniciar o processo, clique com o botão direito do mouse no ícone do Cisco Secure Client na bandeja do Windows e selecione a opção Sair.

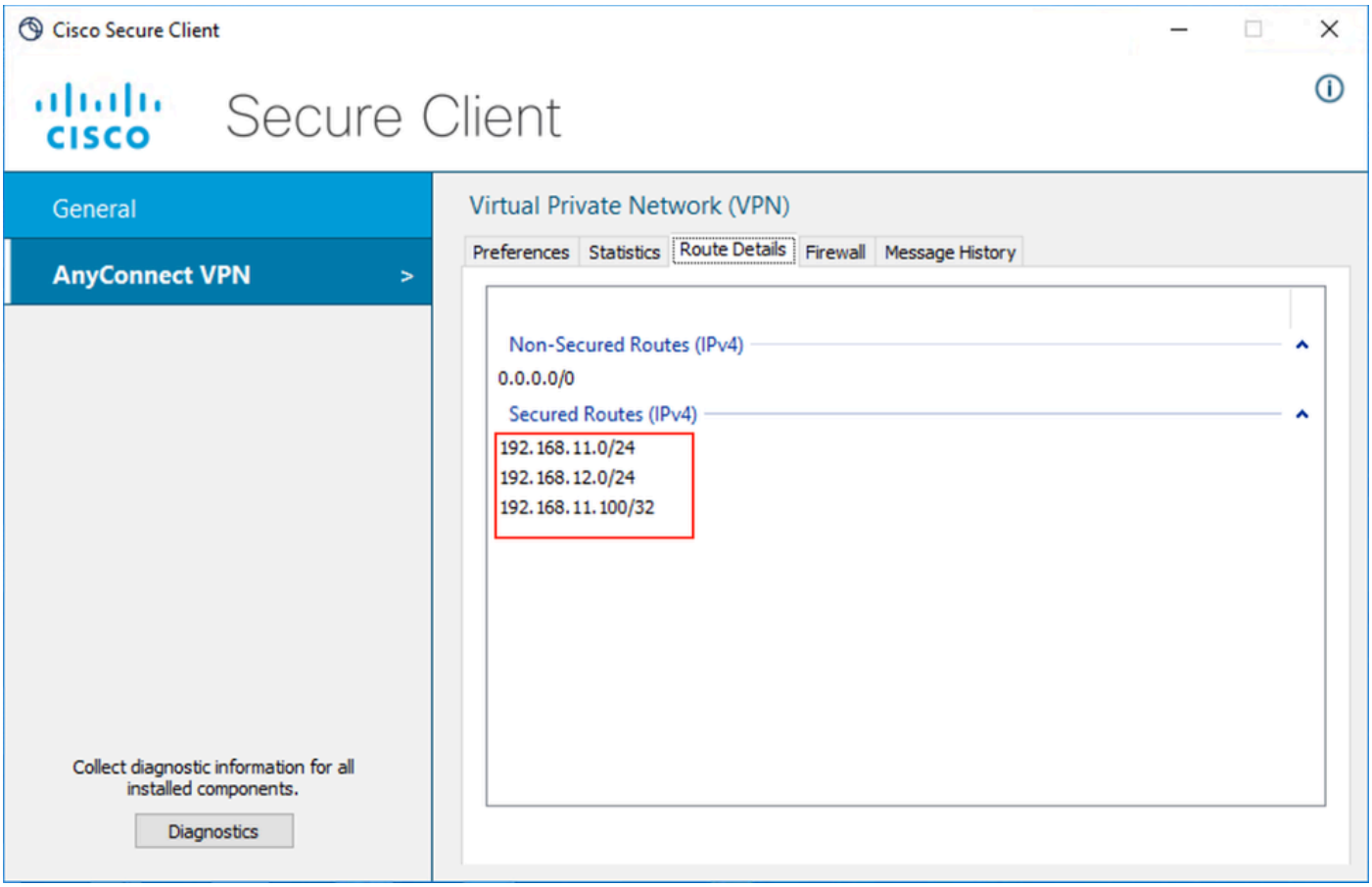
---

2. Depois que a conexão for estabelecida, clique no ícone Gear no canto inferior esquerdo e navegue para AnyConnect VPN > Statistics. Confirme se as informações exibidas correspondem às Informações de conexão e endereço.



Estatísticas do Cisco Secure Client (AnyConnect)

3. Navegue até AnyConnectVPN > Detalhes da rota e confirme se as informações exibidas correspondem às rotas seguras e não seguras.



Detalhes de rota do Cisco Secure Client (AnyConnect)

Use esta seção para confirmar se sua configuração funciona corretamente no C8000v:

1. Para exibir informações da sessão 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. Para exibir estatísticas de vpn ssl - 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. Para verificar a configuração real aplicada para a interface de Acesso Virtual associada ao cliente.

<#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
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

1. Depurações SSL para verificar a negociação entre o headend e o cliente.

<#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. Alguns comandos adicionais para verificar a configuração 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. Ferramenta de Diagnóstico e Relatórios (DART) para o Cisco Secure Client.
Para coletar o pacote DART, execute as etapas descritas em Executar DART para coletar dados para solução de problemas

Exemplo de depurações de uma conexão bem-sucedida:

```
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

Informações Relacionadas

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.