Configuración de AnyConnect SSL VPN en C800v con autenticación local

Contenido

Introducción

Este documento describe cómo configurar Cisco IOS XE Headend C8000v para AnyConnect SSL VPN con una base de datos de usuarios local.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco IOS XE
- Cisco Secure Client (CSC)
- Funcionamiento general de SSL
- Public Key Infrastructure (PKI)

Componentes Utilizados

ThLa información de este documento se basa en las siguientes versiones de software y hardware:

- Cisco Catalyst 8000V (C8000V) con versión 17.16.01a
- Cisco Secure Client versión 5.1.8.105
- PC cliente con Cisco Secure Client instalado

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco IOS XE Secure Socket Layer (SSL) VPN es una solución basada en router que ofrece conectividad de acceso remoto SSL VPN integrada con funciones de routing y seguridad líderes del sector en una plataforma inalámbrica, de datos y voz convergentes. Con Cisco IOS XE SSL VPN, los usuarios finales obtienen acceso de forma segura desde casa o desde cualquier ubicación con conexión a Internet, como zonas Wi-Fi. Cisco IOS XE SSL VPN también permite a las empresas ampliar el acceso a la red corporativa a los partners y consultores externos, manteniendo los datos corporativos protegidos durante todo el tiempo.

Esta función se soporta en las plataformas dadas:

Platform	Versión compatible de Cisco IOS XE
Router para servicios basados en la nube de Cisco serie 1000V	Cisco IOS XE Release 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bengaluru 17.4.1
Router de servicios integrados Cisco 4461 Router de servicios integrados Cisco 4451 Router de servicios integrados Cisco 4431	Cisco IOS XE Cupertino 17.7.1a

Configurar

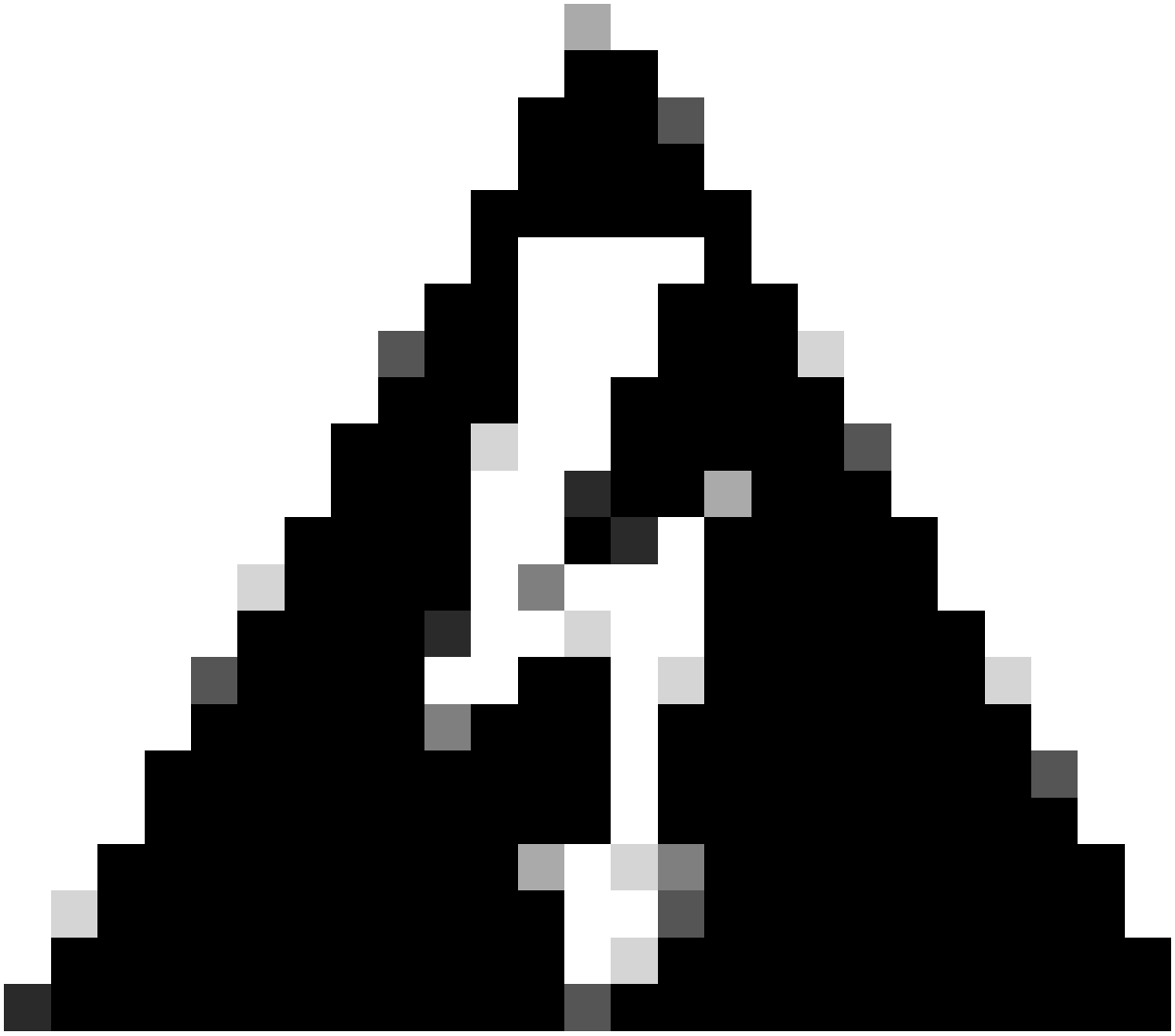
Diagrama de la red

Diagrama de red básico

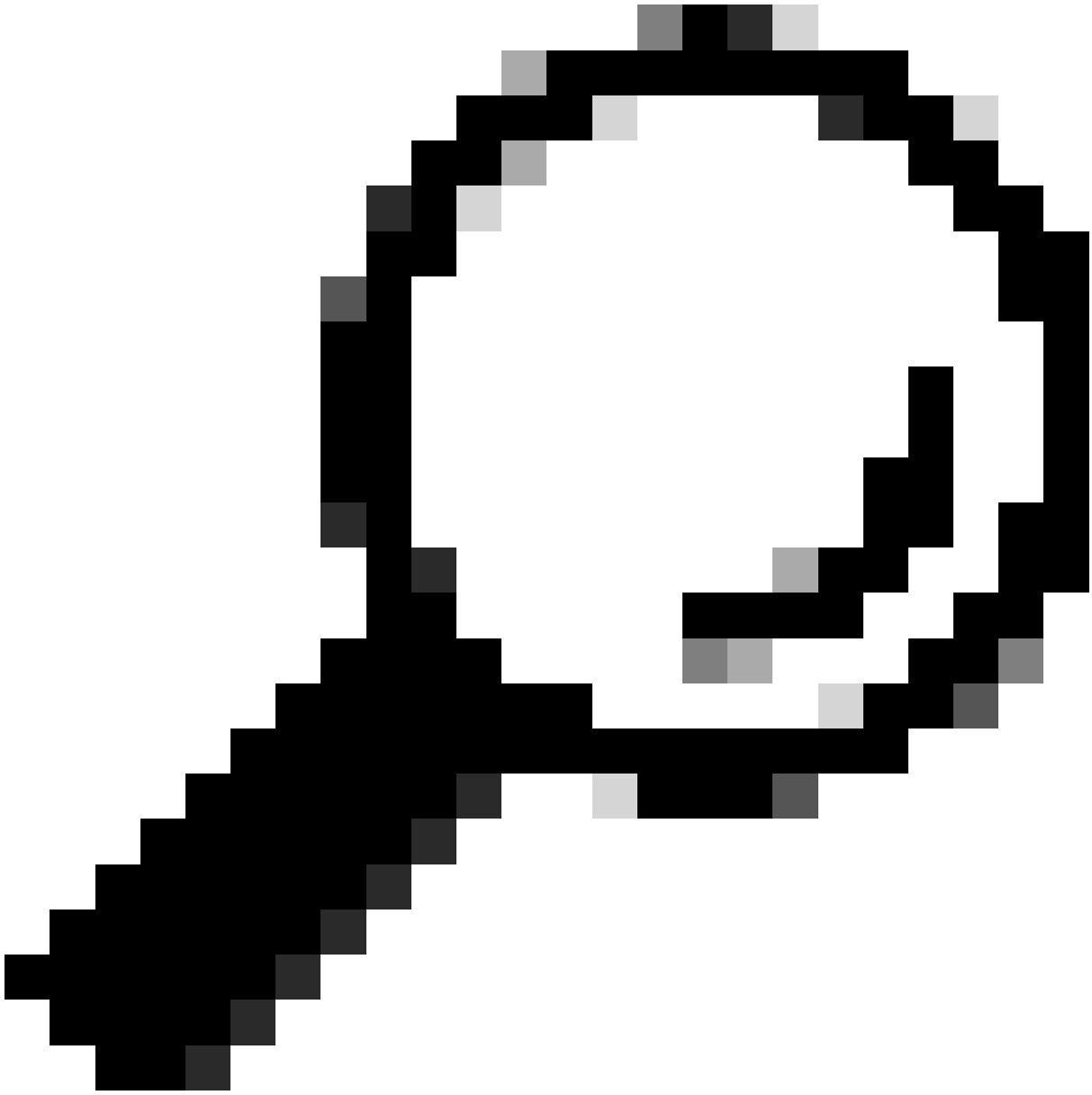
Configuraciones

1. Habilite AAA, configure la autenticación, las listas de autorización y agregue un nombre de usuario a la base de datos local.

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



Advertencia: El comando aaa new-model aplica inmediatamente la autenticación local a todas las líneas e interfaces (excepto la línea de la consola línea con 0). Si se abre una sesión Telnet hacia el router después de habilitar este comando (o si una conexión caduca y debe volver a conectarse), entonces el usuario debe autenticarse con la base de datos local del router. Se recomienda definir un nombre de usuario y una contraseña en el router antes de iniciar la configuración AAA, de modo que no quede bloqueado fuera del router.



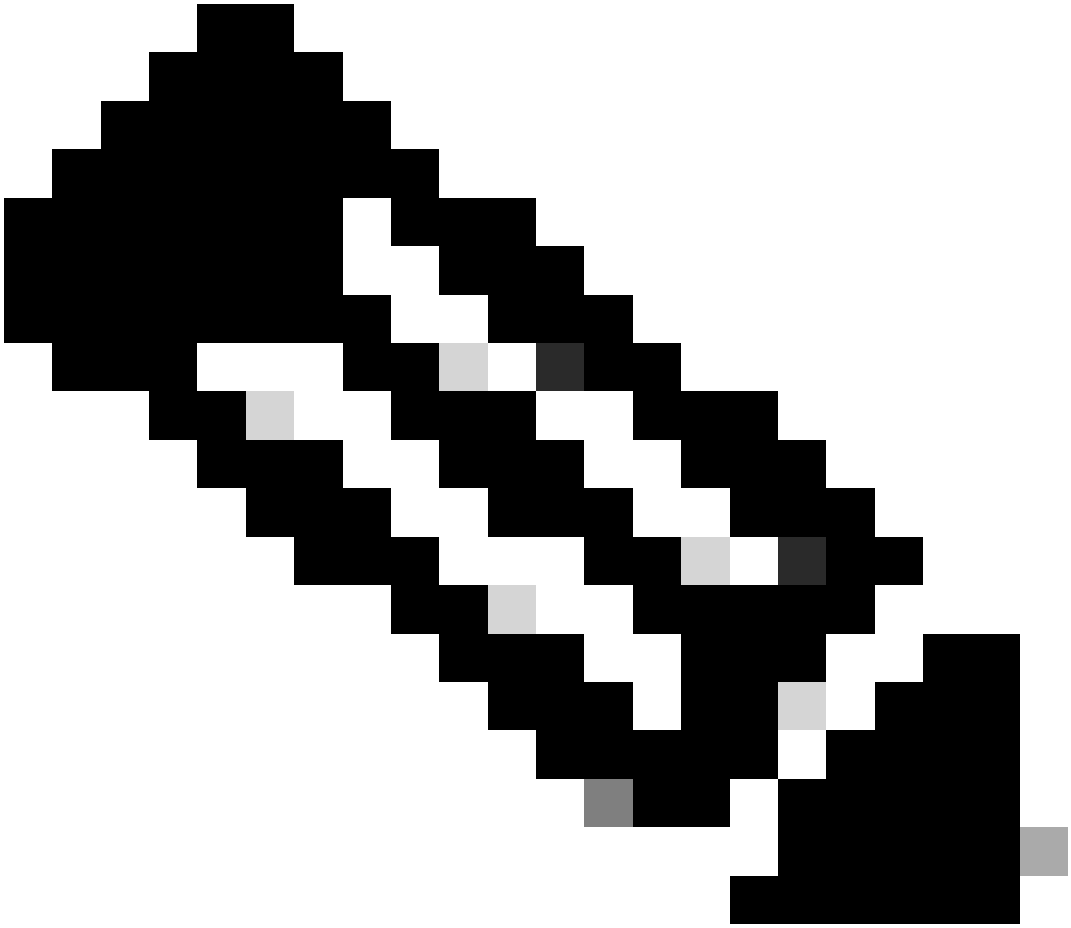
Consejo: Antes de configurar los comandos AAA, guarde la configuración. Puede guardar la configuración nuevamente solo después de haber completado su configuración AAA (y estar satisfecho de que funciona correctamente). Esto le permite recuperarse de bloqueos inesperados, ya que puede revertir cualquier cambio con una recarga del router.

2.Generar par de claves Rivest-Shamir-Adleman (RSA).

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

3. Cree un punto de confianza para instalar el certificado de identidad del router. Puede consultar Cómo Configurar la Inscripción de Certificados para una PKI para obtener más detalles sobre la creación del 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
```



Nota: El nombre común (CN) del nombre del sujeto debe configurarse con la dirección IP o el nombre de dominio completo (FQDN) que utilizan los usuarios para conectarse al gateway seguro (C8000V). Aunque no es obligatorio, si introduce correctamente el CN

---

puede ayudar a reducir el número de errores de certificado que los usuarios encuentran al iniciar sesión.

4. Defina un conjunto local de IP para asignar direcciones a Cisco Secure Client.

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

5. (Opcional) Configure una lista de acceso estándar que se utilizará para el túnel dividido. Esta lista de acceso consta de las redes de destino a las que se puede acceder a través del túnel VPN. De forma predeterminada, todo el tráfico pasa a través del túnel VPN (túnel completo) si el túnel dividido no está 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.Desactivar el servidor HTTP seguro.

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

7. Configure una propuesta SSL.

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

8. Configure una política SSL, llame a la propuesta SSL y al trustpoint PKI.

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

```
ip interface GigabitEthernet1 port 443
```

La política SSL define la propuesta y el punto de confianza que se utilizarán durante la negociación SSL. Sirve como contenedor para todos los parámetros involucrados en la negociación SSL. La selección de la política se realiza haciendo coincidir los parámetros de la sesión con los configurados en la política.

9. (Opcional) Cree un perfil de AnyConnect con la ayuda del editor de perfiles de Cisco Secure Client [Editor de perfiles de Cisco Secure Client] . Se proporciona un fragmento de XML equivalente del perfil como referencia.

<#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. Cargue el perfil XML creado en la memoria flash del router y defina el perfil:

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

11.Desactivar el servidor HTTP seguro.

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

12. Configure la política de autorización de 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
```

La política de autorización SSL es un contenedor de parámetros de autorización que se envían al cliente remoto.La política de autorización se deriva del perfil SSL.

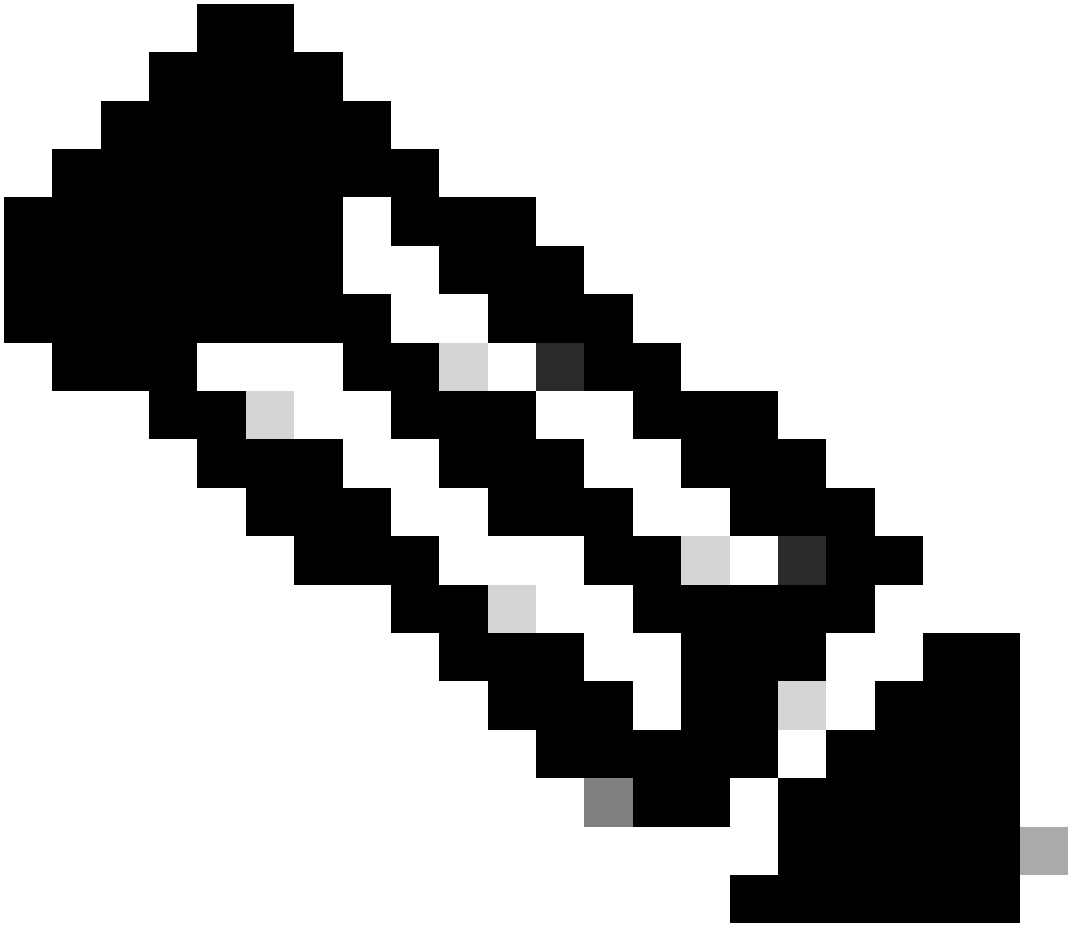
13. Configure una plantilla virtual a partir de la cual se clonan las interfaces de acceso virtual.

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

14. Configure un perfil SSL y defina la autenticación , las listas de cuentas y la plantilla 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
```

La selección de un perfil depende de la política y de los valores de URL.



Nota: La política y la URL deben ser únicas para un perfil SSL VPN, y se debe especificar al menos un método de autorización para activar la sesión.

Se utilizan en el perfil SSL:

- match policy - match statement para seleccionar un perfil SSL ssl_prof para un cliente en el nombre de política SSL ssl_policy.
- match url - sentencias de coincidencia para seleccionar un perfil SSL ssl_prof para un cliente en el directorio URL sslvpn-c8kv.example.com.
- aaa authentication user-pass list - Durante la autenticación se utiliza la lista SSLVPN_AUTHEN.
- aaa authorization group user-pass list - Durante la autorización, la lista de red SSLVPN_AUTHOR se utiliza con la política de autorización ssl_author_policy.
- authentication remote user-pass - Define el modo de autenticación del cliente remoto basado en nombre de usuario/contraseña.
- virtual-template 2 - Define qué plantilla virtual clonar.

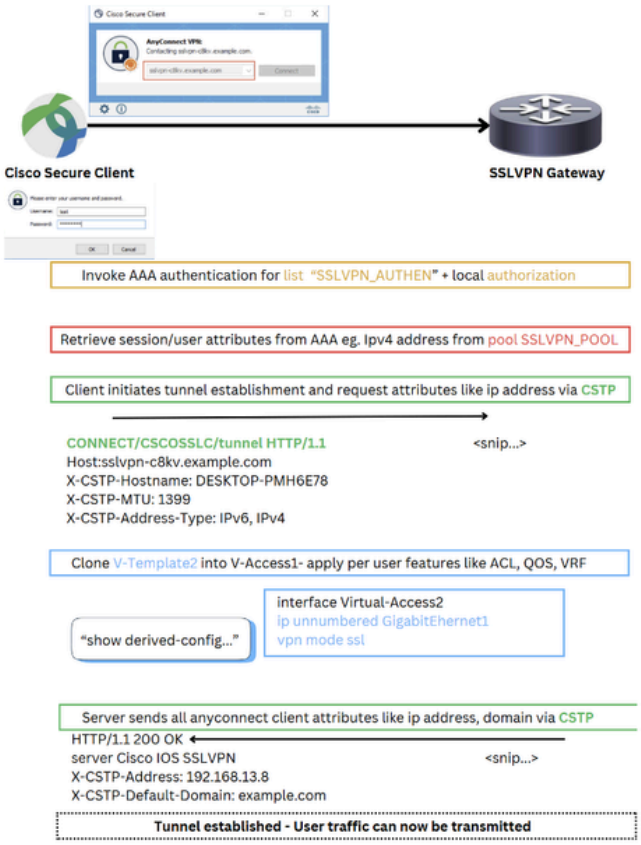
Flujo de conexión

Para comprender los eventos que tienen lugar entre Cisco Secure Client y Secure Gateway durante un establecimiento de conexión SSL VPN, consulte el documento [Comprensión del Flujo de Conexión VPN SSL de AnyConnect]

Flujo de conexión de alto nivel de Cisco Secure Client (AnyConnect) a 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
```

Flujo de conexión de alto nivel 1

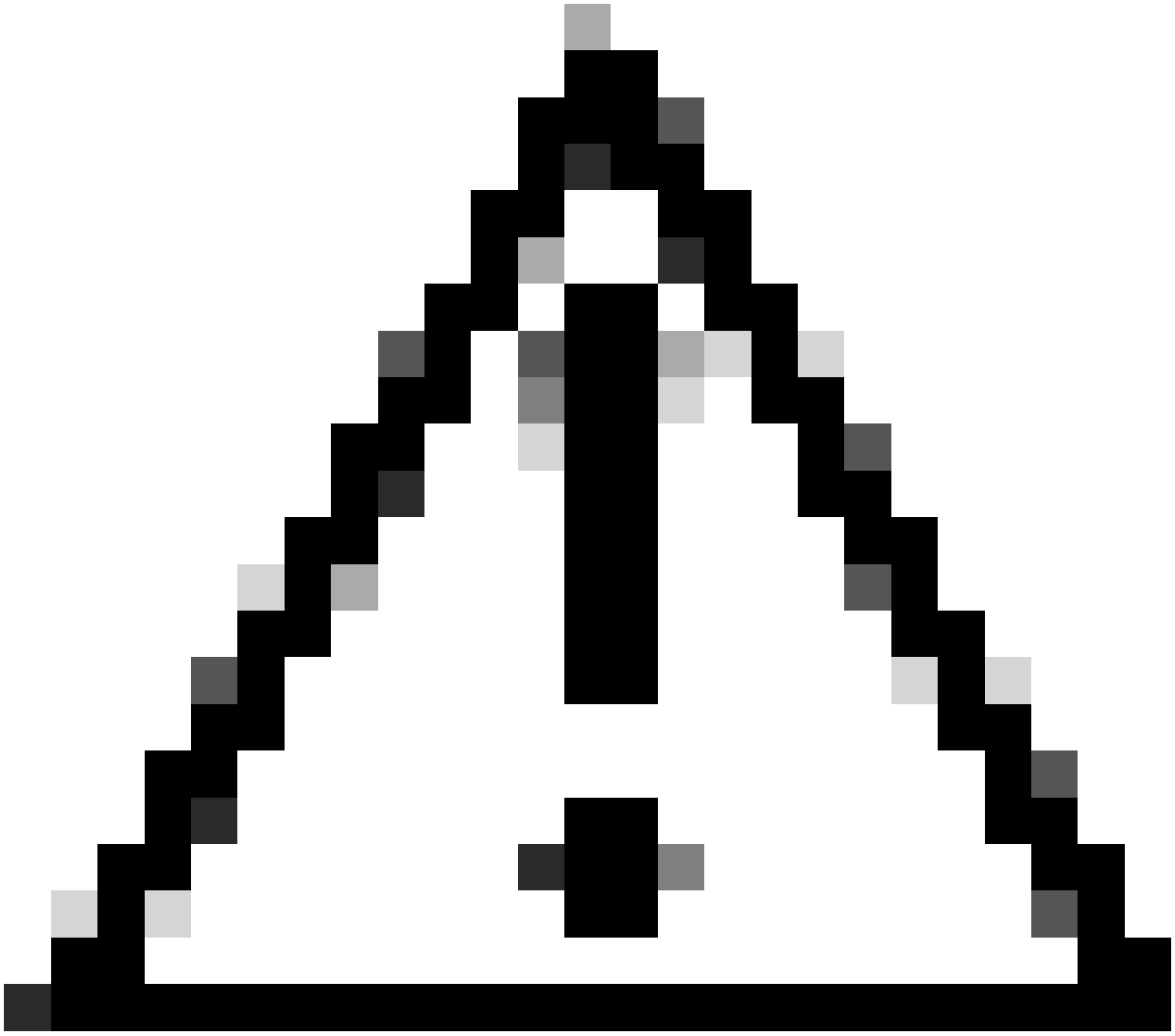



```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443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

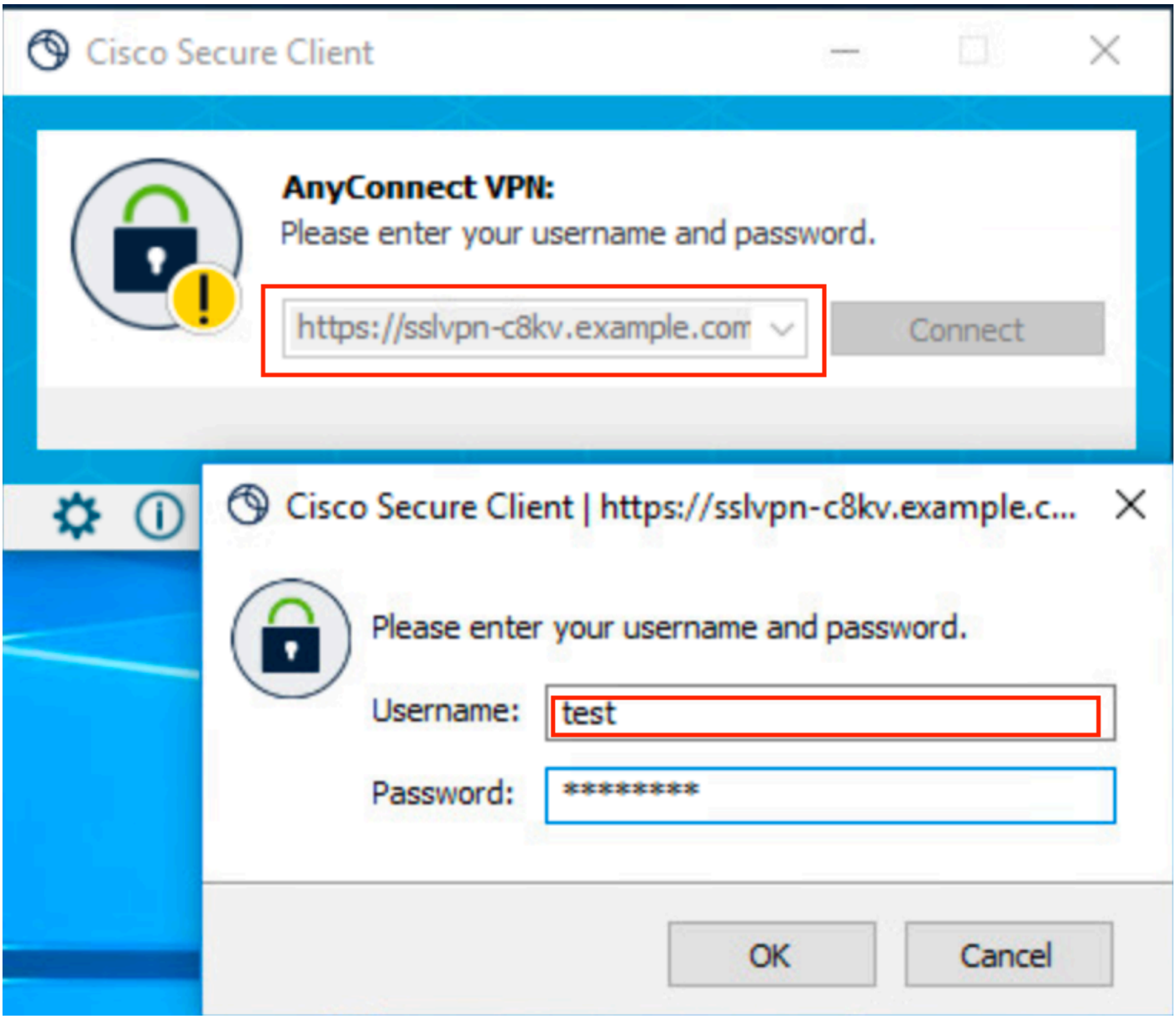
Flujo de conexión de alto nivel 2

Verificación

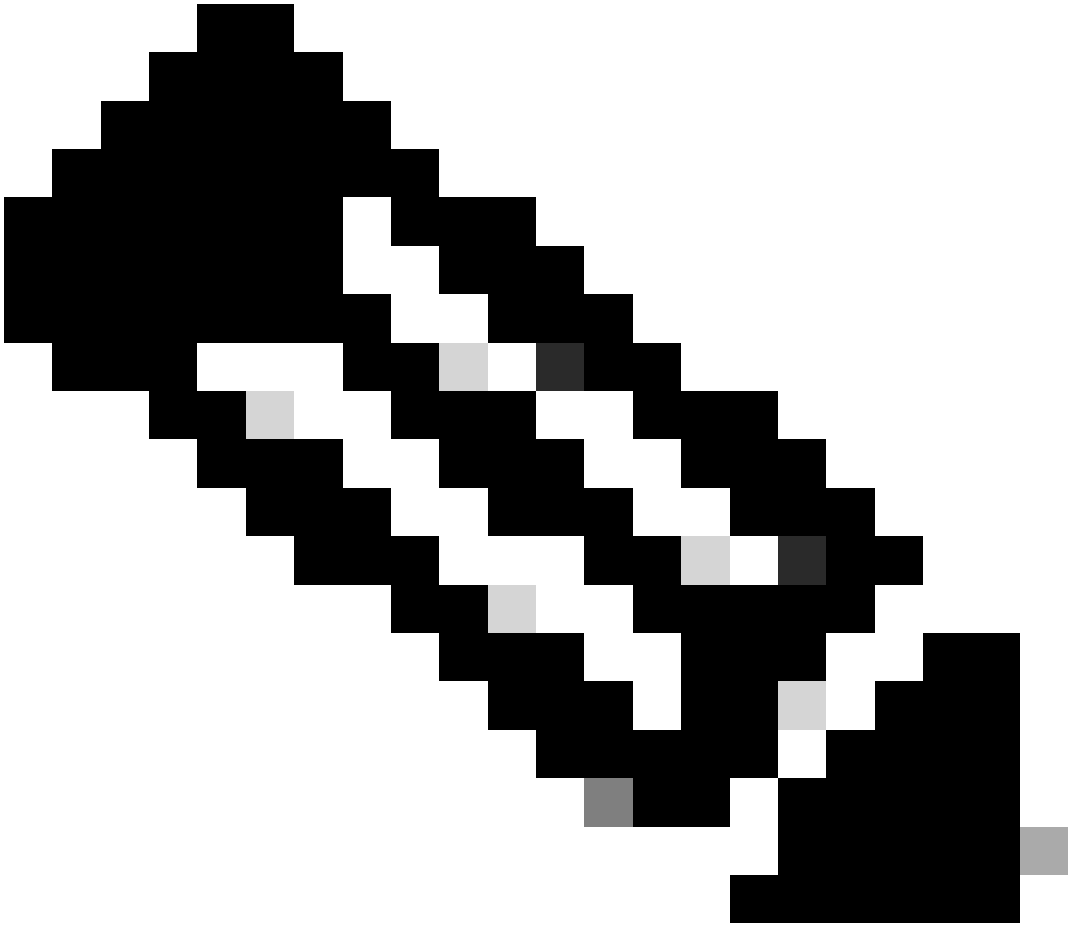
1. Para probar la autenticación, conéctese desde Cisco Secure Client con el nombre de dominio completamente calificado (FQDN) o la dirección IP de C8000v, e ingrese las credenciales.



Precaución: C8000v no admite la descarga de software cliente desde la cabecera. Cisco Secure Client debe estar preinstalado en el PC.



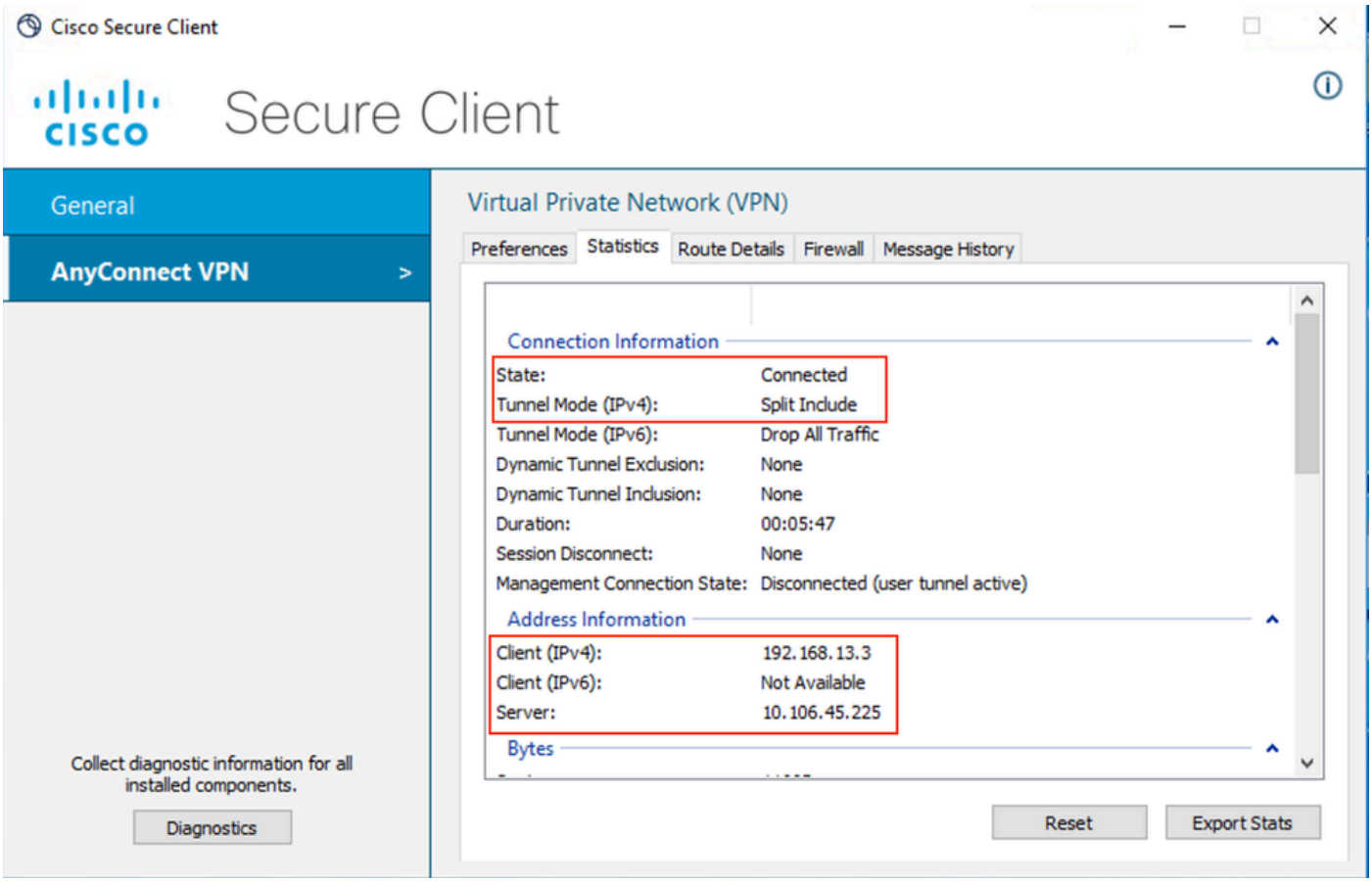
Intento de conexión de Cisco Secure Client



Nota: con una instalación nueva de Cisco Secure Client (sin perfiles XML agregados), el usuario puede introducir manualmente el FQDN del gateway VPN en la barra de direcciones de Cisco Secure Client. Después de un inicio de sesión correcto, Cisco Secure Client intenta descargar el perfil XML de forma predeterminada. Sin embargo, es necesario reiniciar Cisco Secure Client para que el perfil aparezca en la GUI. No basta con cerrar la ventana Cisco Secure Client. Para reiniciar el proceso, haga clic con el botón derecho del ratón en el icono Cisco Secure Client en la bandeja de Windows y seleccione la opción Salir.

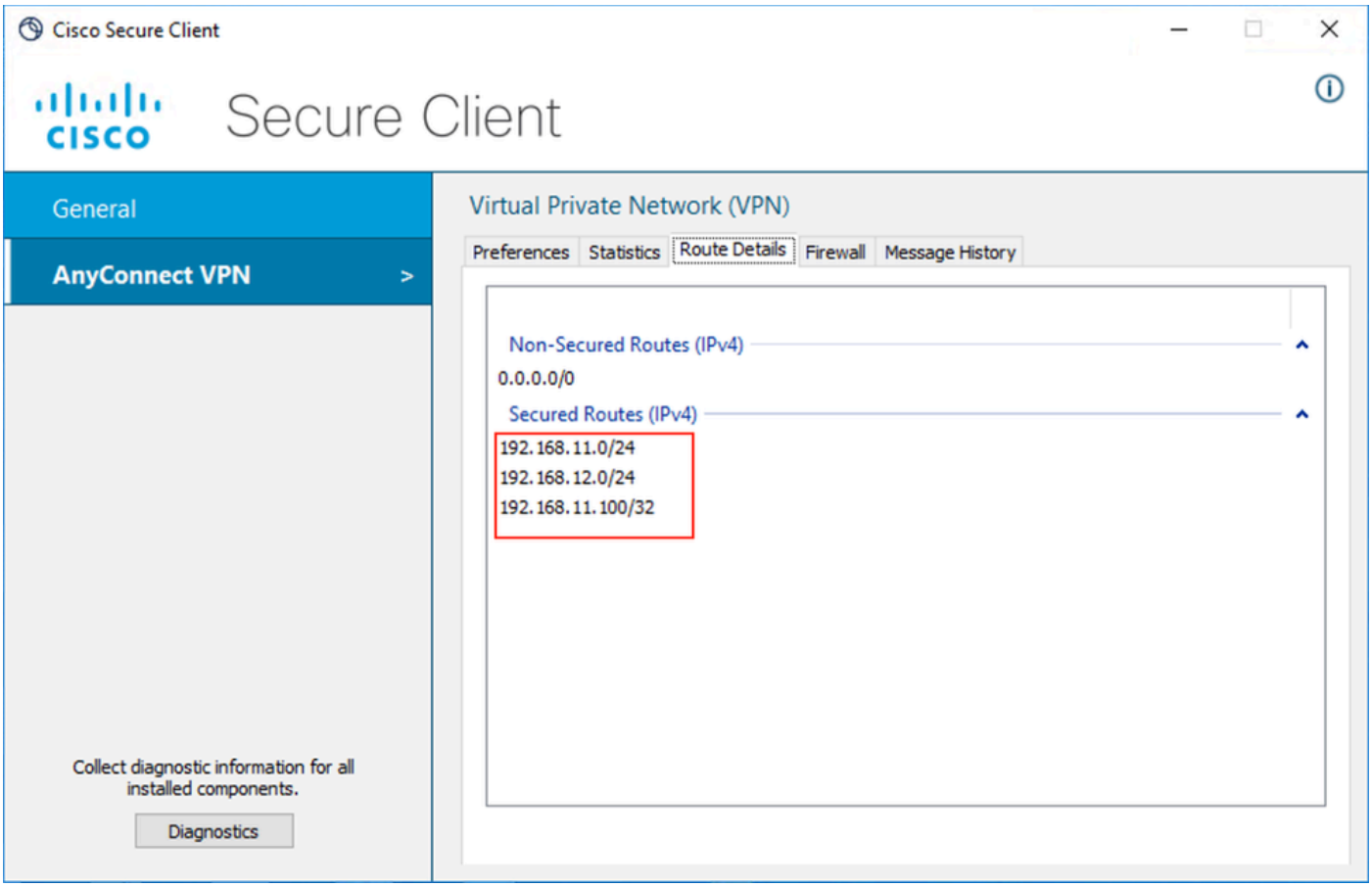
---

2. Una vez establecida la conexión, haga clic en el icono de engranaje en la esquina inferior izquierda y navegue hasta AnyConnect VPN > Statistics. Confirme que la información mostrada corresponde a la información de conexión y dirección.



Estadísticas de Cisco Secure Client (AnyConnect)

3. Acceda a AnyConnectVPN > Detalles de ruta y confirme que la información mostrada corresponde a las rutas seguras y a las rutas no seguras.



Detalles de la ruta de Cisco Secure Client (AnyConnect)

Utilice esta sección para confirmar que su configuración funciona correctamente en C8000v:

1. Para mostrar información de sesión 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 mostrar estadísticas 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. Comprobar la configuración real aplicada para la interfaz de acceso virtual asociada con el 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
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

1. Depuraciones SSL para verificar la negociación entre la cabecera y el 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. Algunos comandos adicionales para verificar la configuración de 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. Herramienta de diagnóstico e informes (DART) para Cisco Secure Client.
Para recopilar el paquete DART, siga los pasos descritos en Ejecutar DART para recopilar datos para solucionar problemas

Depuraciones de ejemplo de una conexión exitosa:

```
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

Información Relacionada

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).