# Configurar o AnyConnect SSL VPN para ISR4k com autenticação local

## Contents



## Introdução

Este documento descreve um exemplo de configuração de como configurar um headend do Integrated Service Router (ISR) 4k Cisco IOS® XE para o AnyConnect Secure Sockets Layer (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 (ISR 4K)
- AnyConnect Secure Mobility Client
- Operação geral de SSL
- Public Key Infrastructure (PKI)

### Componentes Utilizados

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

- Roteador Cisco ISR4451-X/K9 com versão 17.9.2a
- AnyConnect Secure Mobility Client 4.10.04065

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

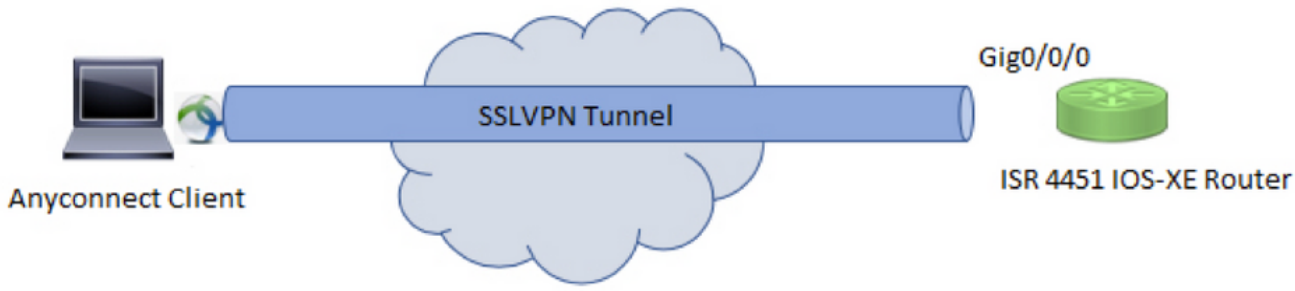
O recurso VPN (Virtual Private Network) SSL fornece suporte no software Cisco IOS XE para acesso de usuário remoto a redes corporativas de qualquer lugar na Internet. O acesso remoto é fornecido através de um gateway VPN SSL habilitado para SSL com Secure Socket Layer (habilitado para SSL). O gateway VPN SSL permite que usuários remotos estabeleçam um túnel VPN seguro. Com o Cisco IOS XE SSL VPN, os usuários finais obtêm acesso seguro de casa ou de qualquer local habilitado para a 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, para proteção de dados corporativos.

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<br>Roteador de serviços integrados Cisco 4451<br>Roteador de serviços integrados Cisco 4431 | Cisco IOS XE Cupertino 17.7.1a |

# Configurar

## Diagrama de Rede



## Configurações

1. Ative a Autenticação, Autorização e Tarifação (AAA - Authentication, Authorization, and Accounting), configure a autenticação, as listas de autorização e adicione um nome de usuário ao banco de dados local.

```
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network default local
!
username test password cisco123
```

2. Crie um Ponto Confiável para instalar o certificado de identidade, se ainda não estiver presente para autenticação local. Você pode consultar Inscrição de certificado para uma PKI para obter mais detalhes sobre a criação do certificado.

```
crypto pki trustpoint SSL
 enrollment mode ra
 enrollment url http://x.x.x.x:80/certsrv/mscep/mscep.dll
 subject-name cn=sslvpn.cisco.com
 revocation-check crl
 rsakeypair SSL-Keys
```

3. Configure uma proposta SSL.

```
crypto ssl proposal SSL_Proposal
 protection rsa-3des-ede-sha1 rsa-aes128-sha1
```

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

```
crypto ssl policy SSL_Policy
 ssl proposal SSL_Proposal
 pki trustpoint SSL sign
 ip address local y.y.y.y port 443
 no shut
```

y.y.y.y é o endereço IP de GigabitEthernet0/0/0.

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 192.168.10.0 0.0.0.255
```

6. Crie um pool de endereços IPv4.

```
ip local pool SSLVPN_POOL 192.168.20.1 192.168.20.10
```

O pool de endereços IP criado atribui um endereço IPv4 ao cliente AnyConnect durante uma conexão bem-sucedida do AnyConnect.

7. Carregue a imagem do headend do AnyConnect (webdeploy) no diretório webvpn do bootflash e carregue o perfil do cliente no bootflash do roteador.

```
mkdir bootflash:webvpn
```

Para o pacote do Anyconnect:

```
copy tftp: bootflash:webvpn:
```

Para o perfil do cliente:

```
copy tftp: bootflash:
```

Defina a imagem do AnyConnect e o perfil do cliente conforme especificado:

```
crypto vpn anyconnect bootflash:/webvpn/anyconnect-win-4.10.04065-webdeploy-k9.pkg sequence 1
!
crypto vpn anyconnect profile sslvpn_client_profile bootflash:/sslvpn_client_profile.xml
```

8. Configure uma política de autorização.

```
crypto ssl authorization policy SSL_Author_Policy
 rekey time 1110
 client profile sslvpn_client_profile
 mtu 1000
 keepalive 500
 dpd-interval client 1000
 netmask 255.255.255.0
 pool SSLVPN_POOL
 dns 8.8.8.8
 banner This is SSL VPN tunnel.
 route set access-list split_tunnel_acl
```

O pool IP, DNS, lista de túneis divididos etc. são especificados na política de autorização.

9. Configure um Modelo virtual a partir do qual as interfaces de acesso virtual sejam clonadas.

```
interface Virtual-Template1 type vpn
 ip unnumbered GigabitEthernet0/0/0
 ip mtu 1400
 ip tcp adjust-mss 1300
```

O comando não numerado obtém o endereço IP da interface configurada (GigabitEthernet0/0/0) e o roteamento IPv4 está ativado nessa interface.

10. Configure um perfil SSL e corresponda à política SSL criada sob ele, juntamente com os parâmetros de autenticação e autorização e o modelo virtual.

```
crypto ssl profile SSL_Profile
 match policy SSL_Policy
 aaa authentication user-pass list default
 aaa authorization group user-pass list default SSL_Author_Policy
 authentication remote user-pass
 virtual-template 1
```

Crie um perfil do AnyConnect com a ajuda do AnyConnect Profile Editor. Um trecho do perfil XML é fornecido para sua referência.

```
!
!
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>false</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<DisableCaptivePortalDetection UserControllable="false">false</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="true">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>SSLVPN</HostName>
<HostAddress>sslvpn.cisco.com</HostAddress>
</HostEntry>
</ServerList>
!
```

# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

<#root>

**1. Check the ssl connection parameters for your anyconnect connection**

**sslvpn# show crypto ssl session user test**

```
Interface         : Virtual-Access1
Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 4.10.04065

Username      : test                  Num Connection : 1
Public IP     : 10.106.52.195
Profile       : SSL_Profile
Policy        : SSL_Policy
Last-Used     : 00:03:58              Created : *05:11:06.166 UTC Wed Feb 22 2023
Tunnel IP     : 192.168.20.10         Netmask : 255.255.255.0
Rx IP Packets : 174                   Tx IP Packets : 142
```

**2. Verify the SSL session status**

**sslvpn# show crypto ssl session**

```
SSL profile name: SSL_Profile
Client_Login_Name  Client_IP_Address    No_of_Connections   Created     Last_Used
test               10.106.52.195            1              00:03:32    00:03:32
```

**3. Verify the tunnel statistics for the active connection**

**sslvpn# show crypto ssl stats tunnel**

```
SSLVPN Profile name : SSL_Profile
Tunnel Statistics:
Active connections       : 1
Peak connections         : 1             Peak time : 5d12h
Connect succeed          : 10            Connect failed : 0
Reconnect succeed        : 38            Reconnect failed : 0
IP Addr Alloc Failed     : 0             VA creation failed : 0
DPD timeout              : 0
Client
in CSTP frames           : 129           in CSTP control : 129
in CSTP data             : 0             in CSTP bytes : 1516
out CSTP frames          : 122           out CSTP control : 122
```

```
out CSTP data            : 0             out CSTP bytes : 1057
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
```

**4. Check the actual configuration applied for the Virtual-Acces interface associated with client**

```
sslvpn# show derived-config interface virtual-access 1


Building configuration...

Derived configuration : 171 bytes
!
interface Virtual-Access1
description ***Internally created by SSLVPN context profile1***
ip unnumbered GigabitEthernet0/0/0
ip mtu 1400
ip tcp adjust-mss 1300
```

# Troubleshooting

Esta seção fornece as informações que você pode usar para solucionar problemas da sua configuração.

1. Depurações SSL para coletar do headend:

```
debug crypto ssl condition client username <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 solucionar problemas de conexão 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. DART do cliente AnyConnect.

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.