Configuración de AnyConnect SSL VPN para ISR4k con autenticación local

Contenido

Introducción

Este documento describe una configuración de ejemplo de cómo configurar un centro distribuidor Cisco IOS® XE de 4.000 rpm del router de servicios integrados (ISR) para VPN AnyConnect Secure Sockets Layer (SSL) con una base de datos de usuarios local.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco IOS XE (ISR 4K)
- AnyConnect Secure Mobility Client
- Funcionamiento general de SSL
- Public Key Infrastructure (PKI)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router Cisco ISR4451-X/K9 con versión 17.9.2a
- AnyConnect Secure Mobility Client 4.10.04065

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

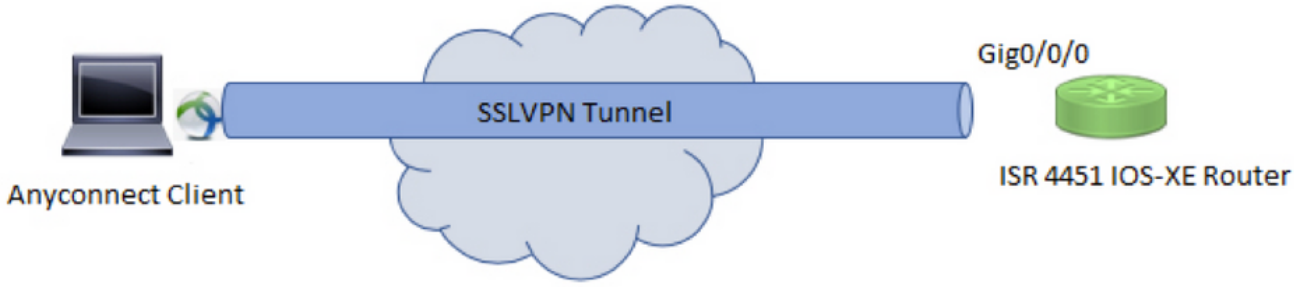
La función SSL Virtual Private Network (VPN) proporciona compatibilidad con el software Cisco IOS XE para el acceso de usuarios remotos a redes empresariales desde cualquier lugar de Internet. El acceso remoto se proporciona a través de un gateway VPN SSL habilitado para Secure Socket Layer (SSL habilitado). El gateway VPN SSL permite a los usuarios remotos establecer un túnel VPN seguro. 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 públicas. Cisco IOS XE SSL VPN también permite a las empresas ampliar el acceso a la red corporativa a los partners y consultores externos para proteger los datos corporativos.

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



Configuraciones

1. Active la autenticación, autorización y contabilidad (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 default local
aaa authorization exec default local
aaa authorization network default local
!
username test password cisco123
```

2. Cree un punto de confianza para instalar el certificado de identidad, si aún no está presente para la autenticación local. Puede consultar Inscripción de Certificados para una PKI para obtener más detalles sobre la creación del 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 una propuesta SSL.

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

4. Configure una política SSL y llame a la propuesta SSL y al trustpoint 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 es la dirección IP de GigabitEthernet0/0/0.

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 192.168.10.0 0.0.0.255
```

6. Cree un conjunto de direcciones IPv4.

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

El conjunto de direcciones IP creado asigna una dirección IPv4 al cliente AnyConnect durante una conexión AnyConnect correcta.

7. Cargue la imagen de cabecera de AnyConnect (webdeploy) en el directorio webvpn de bootflash y cargue el perfil del cliente en la bootflash del router.

```
mkdir bootflash:webvpn
```

Para el paquete Anyconnect:

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

Para el perfil del cliente:

```
copy tftp: bootflash:
```

Defina la imagen de AnyConnect y el perfil del cliente según lo 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 una directiva de autorización.

```
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
```

El conjunto de IP, DNS, la lista de túnel dividido, etc. se especifican en la directiva de autorización.

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

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

El comando no numerado obtiene la dirección IP de la interfaz configurada (GigabitEthernet0/0/0) y el ruteo IPv4 está habilitado en esa interfaz.

10. Configure un perfil SSL y haga coincidir la política SSL creada en él junto con los parámetros de autenticación y autorización y la plantilla 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
```

Cree un perfil de AnyConnect con la ayuda del Editor de perfiles de AnyConnect. Se proporciona un fragmento del perfil XML como referencia.

```
!
!
<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>
!
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

<#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
```

Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

1. Depuraciones SSL para recopilar de la cabecera:

```
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. Algunos comandos adicionales para resolver problemas de conexión 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 del cliente AnyConnect.

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).