AnyConnect SSL VPN voor ISR4k met lokale verificatie configureren

Inhoud

Inleiding

Dit document beschrijft een voorbeeldconfiguratie van hoe u een geïntegreerde services router (ISR) 4k Cisco IOS® XE head-end voor AnyConnect Secure Sockets Layer (SSL) VPN kunt configureren met een lokale gebruikersdatabase.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco IOS XE (ISR 4K)
- AnyConnect beveiligde mobiliteit-client
- Algemene SSL-werking
- Public Key Infrastructure (PKI)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISR 4451-X/K9 router met versie 17.9.2a
- AnyConnect Secure Mobility-client 4.10.04065

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

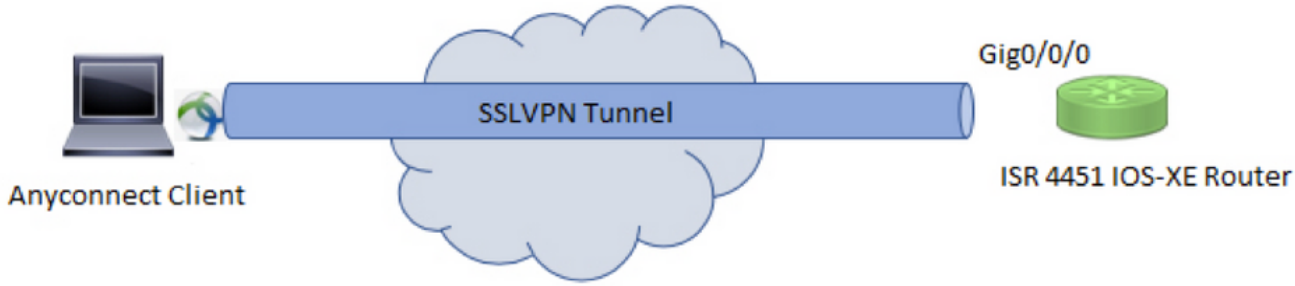
SSL Virtual Private Network (VPN) biedt ondersteuning in de Cisco IOS XE-software voor externe gebruikerstoegang tot ondernemingsnetwerken vanaf elke locatie op het internet. Externe toegang wordt verleend via een Secure Socket Layer-enabled (SSL-enabled) SSL VPN-gateway. De SSL VPN gateway staat externe gebruikers toe een beveiligde VPN-tunnel tot stand te brengen. Met Cisco IOS XE SSL VPN krijgen eindgebruikers veilig toegang vanuit huis of elke voor het internet geschikte locatie zoals draadloze hotspots. Cisco IOS XE SSL VPN stelt bedrijven ook in staat om hun bedrijfsnetwerktoegang uit te breiden naar offshore partners en consultants, voor de bescherming van bedrijfsgegevens.

Deze optie wordt ondersteund op de opgegeven platforms:

Platform	Ondersteunde Cisco IOS XE release
Cisco Cloud-services router 1000V Series	Cisco IOS XE release 16.9
Cisco Catalyst 8000V switch	Cisco IOS XE Bengaluru 17.4.1
Cisco 4461 geïntegreerde services router Cisco 4451 geïntegreerde services router Cisco 4431 geïntegreerde services router	Cisco IOS XE-koppeling 17.7.1a

Configureren

Netwerkdiagram



Configuraties

1. Schakel verificatie, autorisatie en accounting (AAA) in, configureer verificatie, autorisatielijsten en voeg een gebruikersnaam toe aan de lokale database.

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

2. Maak een Trustpoint om het identiteitscertificaat te installeren, als dit nog niet bestaat voor lokale verificatie. U kunt verwijzen naar Certificaatinschrijving voor een PKI voor meer informatie over het maken van het certificaat.

```
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. Configureer een SSL-voorstel.

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

4. Configureer een SSL-beleid en bel het SSL-voorstel en het PKI-trustpoint.

```
crypto ssl policy SSL_Policy
ssl proposal SSL_Proposal
pki trustpoint SSL sign
ip address local y.y.y.y port 443
```

y.y.y.y is het IP-adres van Gigabit Ethernet0/0/0.

5. (Optioneel) Configureer een standaardtoegangslijst die voor de splitstunnel moet worden gebruikt. Deze toegangslijst bestaat uit de doelnetwerken die toegankelijk zijn via de VPN-tunnel. In de standaardinstelling passeert al het verkeer door de VPN-tunnel (volledige tunnel) als de gesplitste tunnel niet is geconfigureerd.

```
ip access-list standard split_tunnel_acl
10 permit 192.168.10.0 0.0.0.255
```

6. Maak een IPv4-adresgroep aan.

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

De IP-adressengroep die is gemaakt, wijst een IPv4-adres toe aan de AnyConnect-client tijdens een succesvolle AnyConnect-verbinding.

7. Upload de AnyConnect head-end afbeelding (webopstellen) onder de **webvpn-**directory van bootflash en upload het clientprofiel naar de bootflash van de router.

Definieer het AnyConnect-beeld en het clientprofiel zoals opgegeven:

```
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. Configureer het autorisatiebeleid.

```
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
```

De IP-pool, DNS, lijst met gesplitste tunnels, enzovoort worden gespecificeerd onder het autorisatiebeleid.

9. Configureer een virtuele sjabloon waaruit de virtuele toegangsinterfaces worden gekloond.

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

De ongenummerde opdracht krijgt het IP-adres van de geconfigureerde interface (Gigabit Ethernet0/0/0) en IPv4-routing is op die interface ingeschakeld.

10. Een SSL-profiel configureren en het SSL-beleid dat onder het profiel is gemaakt, aanpassen, samen met de verificatie- en autorisatieparameters en de virtuele sjabloon.

```
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
```

Maak een AnyConnect-profiel met behulp van de AnyConnect Profile Editor. Een fragment van het XML-profiel wordt gegeven voor uw referentie. Het volledige profiel is als bijlage aan dit document toegevoegd.

```
!
!
```

```
!
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

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
```

Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

1. SSL debugs te verzamelen van de head-end:

```
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. Een paar extra opdrachten om problemen met SSL-verbindingen op te lossen:

```
# 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. Start de AnyConnect-client.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.