Konfigurieren von AnyConnect SSL VPN für ISR4k mit lokaler Authentifizierung

Inhalt

Einleitung

In diesem Dokument wird eine Beispielkonfiguration für die Konfiguration eines Integrated Service Router (ISR) 4.000 Cisco IOS® XE-Headends für AnyConnect Secure Sockets Layer (SSL) VPN mit einer lokalen Benutzerdatenbank beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco IOS XE (ISR 4000)
- AnyConnect Secure Mobility-Client
- Allgemeiner SSL-Betrieb
- Public Key Infrastructure (PKI)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISR4451-X/K9 Router mit Version 17.9.2a
- AnyConnect Secure Mobility Client 4.10.04065

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

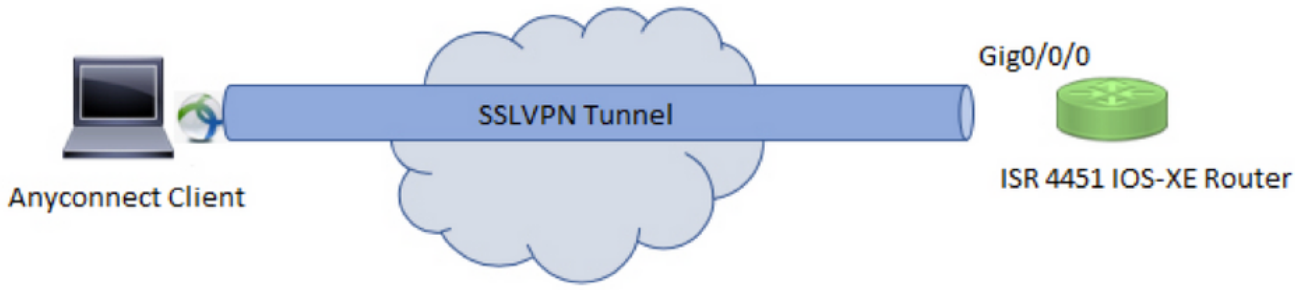
Die SSL Virtual Private Network (VPN)-Funktion bietet in der Cisco IOS XE-Software Unterstützung für den Remote-Benutzerzugriff auf Unternehmensnetzwerke von einem beliebigen Standort im Internet aus. Der Remote-Zugriff erfolgt über ein SSL-fähiges SSL VPN-Gateway mit Secure Socket Layer. Über das SSL VPN-Gateway können Remote-Benutzer einen sicheren VPN-Tunnel einrichten. Mit dem Cisco IOS XE SSL VPN erhalten Endbenutzer sicheren Zugriff von zu Hause oder von einem beliebigen internetfähigen Standort, z. B. einem Wireless-Hotspot. Cisco IOS XE SSL VPN ermöglicht es Unternehmen außerdem, den Zugriff auf das Unternehmensnetzwerk für Offshore-Partner und -Berater zu erweitern, um den Schutz der Unternehmensdaten zu gewährleisten.

Diese Funktion wird auf den folgenden Plattformen unterstützt:

Plattform	Unterstützte Cisco IOS XE-Version
Cisco Cloud Services Router der Serie 1000V	Cisco IOS XE Version 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bengaluru 17.4.1
Cisco Integrated Services Router 4461 Cisco Integrated Services Router 4451 Cisco Integrated Services Router 4431	Cisco IOS XE Cupertino 17.7.1a

Konfigurieren

Netzwerkdiagramm



Konfigurationen

1. Aktivieren Sie Authentication, Authorization und Accounting (AAA), konfigurieren Sie die Authentifizierung, Autorisierungslisten, und fügen Sie der lokalen Datenbank einen Benutzernamen hinzu.

```
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network default local
```

```
!
username test password cisco123
```

2. Erstellen Sie einen Vertrauenspunkt, um das Identitätszertifikat zu installieren, falls es nicht bereits für die lokale Authentifizierung vorhanden ist. Weitere Informationen zur Zertifikatserstellung finden Sie unter Zertifikatregistrierung für eine PKI.

```
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. Konfigurieren Sie ein SSL-Angebot.

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

4. Konfigurieren Sie eine SSL-Richtlinie, und rufen Sie das SSL-Angebot und den PKI-Vertrauenspunkt auf.

```
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 ist die IP-Adresse von GigabitEthernet0/0/0.

5. (Optional) Konfigurieren Sie eine Standard-Zugriffsliste für den Split-Tunnel. Diese Zugriffsliste besteht aus den Zielnetzwerken, auf die über den VPN-Tunnel zugegriffen werden kann. Standardmäßig durchläuft der gesamte Datenverkehr den VPN-Tunnel (vollständiger Tunnel), wenn der Split-Tunnel nicht konfiguriert ist.

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

6. Erstellen Sie einen IPv4-Adresspool.

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

Der erstellte IP-Adresspool weist dem AnyConnect-Client während einer erfolgreichen AnyConnect-Verbindung eine IPv4-Adresse zu.

7. Laden Sie das AnyConnect-Headend-Image (webdeploy) unter **webvpn** des Verzeichnisses "bootflash" hoch und laden Sie das Client-Profil in den Bootflash des Routers hoch.

Definieren Sie das AnyConnect-Abbild und das Clientprofil wie angegeben:

```
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. Autorisierungsrichtlinie konfigurieren

```
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
```

Der IP-Pool, DNS, die Split-Tunnel-Liste usw. werden in der Autorisierungsrichtlinie festgelegt.

9. Konfigurieren Sie eine virtuelle Vorlage, aus der die Schnittstellen für den virtuellen Zugriff geklont werden.

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

Mit dem Befehl ohne Nummer wird die IP-Adresse von der konfigurierten Schnittstelle abgerufen (GigabitEthernet0/0/0), und IPv4-Routing ist auf dieser Schnittstelle aktiviert.

10. Konfigurieren Sie ein SSL-Profil, und ordnen Sie die unter ihm erstellte SSL-Richtlinie sowie die Authentifizierungs- und Autorisierungsparameter und die virtuelle Vorlage zu.

```
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
```

Erstellen Sie mithilfe des AnyConnect Profile Editors ein AnyConnect-Profil. Ein Ausschnitt des XML-Profils wird als Referenz angegeben. Dieses Dokument enthält das vollständige Profil.

```
!
!
```

!

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

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
```

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

1. SSL-Debugging zum Sammeln vom 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. Einige zusätzliche Befehle zur Behebung von SSL-Verbindungsproblemen:

```
# 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 vom AnyConnect-Client.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.