為ISR4k配置AnyConnect SSL VPN（使用本地身份驗證）

目錄

簡介

本文說明如何使用本地使用者資料庫為AnyConnect安全套接字層(SSL)VPN配置整合服務路由器(ISR)4k Cisco IOS® XE頭端的示例配置。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS XE(ISR 4K)
- AnyConnect安全行動化使用者端
- 常規SSL操作
- 公開金鑰基礎架構 (PKI)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISR4451-X/K9路由器，版本17.9.2a
- AnyConnect安全行動化使用者端4.10.04065

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

SSL虛擬私人網路(VPN)功能在Cisco IOS XE軟體中提供支援，讓遠端使用者從網際網路上的任何位置存取企業網路。通過啟用安全套接字層（啟用SSL）的SSL VPN網關提供遠端訪問。SSL

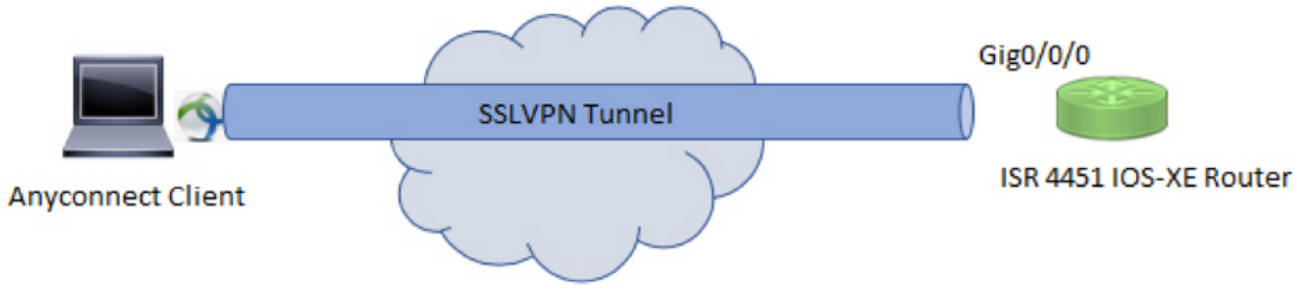
VPN網關允許遠端使用者建立安全的VPN隧道。藉助Cisco IOS XE SSL VPN，終端使用者可以從家裡或任何啟用網際網路的位置（如無線熱點）安全地訪問網路。Cisco IOS XE SSL VPN還使公司能夠向離岸合作夥伴和顧問擴展公司網路訪問，以實現公司資料保護。

以下指定平台支援此功能：

平台	支援的Cisco IOS XE版本
Cisco Cloud Services Router 1000V系列	Cisco IOS XE版本16.9
Cisco Catalyst 8000V	Cisco IOS XE班加羅爾17.4.1
思科4461整合式服務路由器 思科4451整合式服務路由器 思科4431整合式服務路由器	Cisco IOS XE Cupertino 17.7.1a

設定

網路圖表



組態

1.啟用身份驗證、授權和記帳(AAA)，配置身份驗證、授權清單並將使用者名稱新增到本地資料庫。

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

2.建立信任點以安裝身份證書（如果本地身份驗證尚未提供）。有關證書建立的詳細資訊，請參閱PKI的證書註冊。

```
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.配置SSL方案。

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

4.配置SSL策略並呼叫SSL建議和PKI信任點。

```
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是GigabitEthernet0/0/0的IP地址。

5.（可選）配置要用於拆分隧道的標準訪問清單。此訪問清單包括可通過VPN隧道訪問的目標網路。預設情況下，如果沒有配置拆分隧道，則所有流量都會通過VPN隧道（全隧道）。

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

6.建立IPv4地址池。

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

在成功的AnyConnect連線過程中，建立的IP地址池為AnyConnect客戶端分配一個IPv4地址。

7.將AnyConnect頭端映像(webdeploy)上傳到bootflash的**webvpn** 目錄下，並將客戶端配置檔案上傳到路由器的bootflash。

按指定定義AnyConnect映像和客戶端配置檔案：

```
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.配置授權策略。

```
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
```

在授權策略下指定IP池、DNS、拆分隧道清單等。

9.配置從中克隆虛擬訪問介面的虛擬模板。

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

unnumbered命令從配置的介面(GigabitEthernet0/0/0)獲取IP地址，並且在該介面上啟用了IPv4路由。

10.配置SSL配置檔案，並將其下建立的SSL策略與身份驗證和授權引數以及虛擬模板匹配。

```
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
```

在AnyConnect配置檔案編輯器的幫助下建立AnyConnect配置檔案。XML配置檔案的片段可供您參考。完整配置檔案將附加至此文檔。

```
!
!
```

!

驗證

使用本節內容，確認您的組態是否正常運作。

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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1.要從頭端收集的SSL調試：

```
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
```

2.一些用於排除SSL連線問題的其他命令：

```
# 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. AnyConnect客戶端的DART。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。