为ISR4k配置AnyConnect SSL VPN并进行本地身份验证

目录

[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[背景信息](#)

[配置](#)

- [网络图](#)
- [配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何为具有本地用户数据库的AnyConnect SSL VPN配置ISR 4k Cisco IOS® XE头端的示例配置。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS XE(集成服务路由器(ISR)4K)
- AnyConnect 安全移动客户端
- 通用安全套接字层(SSL)操作
- 公用密钥基础结构 (PKI)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ISR4451-X/K9路由器，版本17.9.2a
- AnyConnect安全移动客户端4.10.04065

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

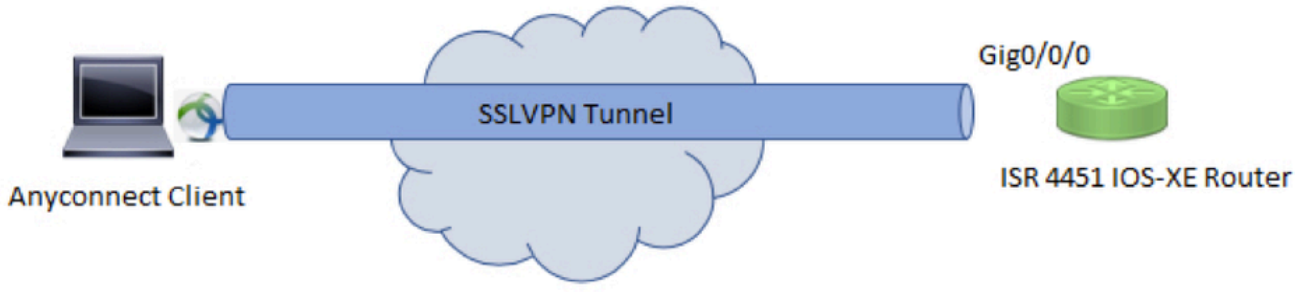
SSL虚拟专用网络(VPN)功能在Cisco IOS XE软件中提供支持，以便远程用户从互联网上的任何位置访问企业网络。通过启用安全套接字层（启用SSL）的SSL VPN网关提供远程访问。SSL VPN网关允许远程用户建立安全的VPN隧道。借助Cisco IOS XE SSL VPN，最终用户可以从家里或任何支持互联网的位置（如无线热点）安全地访问网络。Cisco IOS XE SSL VPN还使公司能够将公司网络访问扩展到离岸合作伙伴和顾问，以实现公司数据保护。

以下特定平台支持此功能：

Platform	支持的Cisco IOS XE版本
思科云服务路由器1000V系列	思科IOS XE版本16.9
Cisco Catalyst 8000V	思科IOS XE班加罗尔17.4.1
Cisco 4461 集成业务路由器 Cisco 4451 集成业务路由器 Cisco 4431 集成业务路由器	思科IOS XE Cupertino 17.7.1a

配置

网络图



配置

1.启用身份验证、授权和记帐(AAA)，配置身份验证、授权列表并将用户名添加到本地数据库。

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

2.创建信任点以安装身份证书（如果本地身份验证中不存在身份证书）。有关证书创建的详细信息，请参阅PKI的证书注册。

```
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提议。

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

4.配置SSL策略并调用SSL建议和PKI信任点。

```
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是GigabitEthernet0/0/0的IP地址。

5.（可选）配置用于拆分隧道的标准访问列表。此访问列表包括可通过VPN隧道访问的目标网络。默认情况下，如果未配置拆分隧道，则所有流量都会通过VPN隧道(Full Tunnel)。

```
ip access-list standard split_tunnel_acl
```

```
 10 permit 192.168.10.0 0.0.0.255
```

6.创建IPv4地址池。

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

在AnyConnect连接成功期间，创建的IP地址池会为AnyConnect客户端分配IPv4地址。

7.在bootflash的webvpn目录下上传AnyConnect头端映像(webdeploy)，并将客户端配置文件上传到路由器的bootflash。

```
mkdir bootflash:webvpn
```

对于Anyconnect软件包：

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

对于客户端配置文件：

```
copy tftp: bootflash:
```

按指定定义AnyConnect映像和客户端配置文件：

```
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.配置授权策略。

```
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
```

IP池、DNS、拆分隧道列表等在授权策略下指定。

9.配置用于克隆虚拟访问接口的虚拟模板。

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

unnumbered命令从配置的接口(GigabitEthernet0/0/0)获取IP地址，并且在该接口上启用了IPv4路由。

10.配置SSL配置文件，并将在其下创建的SSL策略与身份验证和授权参数以及虚拟模板匹配。

```
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
```

1.禁用HTTP安全服务器。

```
no ip http secure-server
```

在AnyConnect配置文件编辑器的帮助下创建AnyConnect配置文件。此处提供了XML配置文件的片段以供参考。

!
!

false

true

false

All

All

false

Native

false

30

false

true

false

false

true

IPv4,IPv6

true

ReconnectAfterResume

false

true

Automatic

SingleLocalLogon

SingleLocalLogon

AllowRemoteUsers

LocalUsersOnly

false

Automatic

```
false
```

```
false
```

```
 20
```

```
 4
```

```
false
```

```
false
```

```
        true

         SSLVPN

         sslvpn.cisco.com

!
```

验证

使用本部分可确认配置能否正常运行。

1.检查anyconnect连接的SSL连接参数。

<#root>

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.验证SSL会话状态。

<#root>

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.检验活动连接的隧道统计信息。

<#root>

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.检查应用于与客户端关联的虚拟访问接口的实际配置。

<#root>

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
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

1.要从头端收集的SSL调试：

```
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
```

2.一些用于排除SSL连接问题的额外命令：

```
# 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.来自AnyConnect客户端的DART。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。