Configure AnyConnect SSL VPN for ISR4k with Local Authentication

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

Introduction

This document describes a sample configuration of how to configure an ISR 4k Cisco IOS® XE headend for AnyConnect SSL VPN with a local user database.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco IOS XE (Integrated Service Router (ISR) 4K)
- AnyConnect Secure Mobility Client
- General Secure Sockets Layer (SSL) Operation
- Public Key Infrastructure (PKI)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISR4451-X/K9 Router with version 17.9.2a
- AnyConnect Secure Mobility Client 4.10.04065

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The SSL Virtual Private Network (VPN) feature provides support in the Cisco IOS XE software for remote

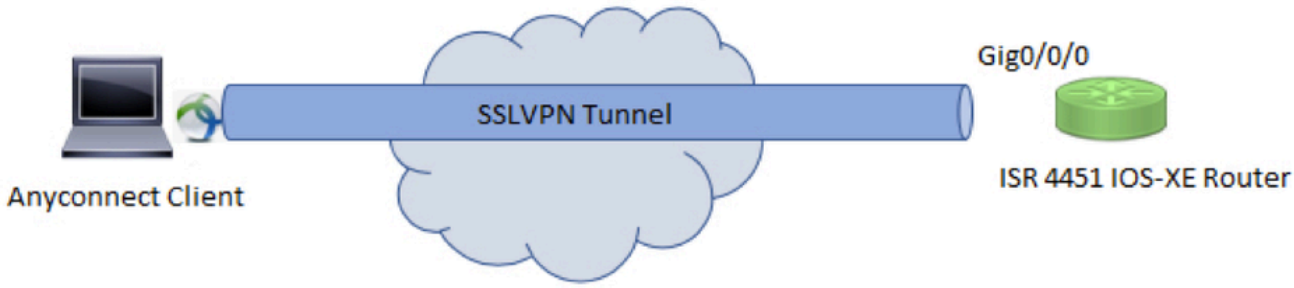
user access to enterprise networks from anywhere on the internet. Remote access is provided through a Secure Socket Layer-enabled (SSL-enabled) SSL VPN gateway. The SSL VPN gateway allows remote users to establish a secure VPN tunnel. With Cisco IOS XE SSL VPN, end users gain access securely from home or any internet-enabled location such as wireless hotspots. Cisco IOS XE SSL VPN also enables companies to extend corporate network access to offshore partners and consultants, for corporate data protection.

This feature is supported on the given platforms:

Platform	Supported Cisco IOS XE Release
Cisco Cloud Services Router 1000V Series	Cisco IOS XE Release 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bengaluru 17.4.1
Cisco 4461 Integrated Services Router Cisco 4451 Integrated Services Router Cisco 4431 Integrated Services Router	Cisco IOS XE Cupertino 17.7.1a

Configure

Network Diagram



Configurations

1. Enable Authentication, Authorization, and Accounting (AAA), configure authentication, authorization lists, and add a username to the local database.

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

```
aaa authorization network default local
!
username test password cisco123
```

2. Create a Trustpoint to install the identity certificate, if not already present for local authentication. You can refer to Certificate Enrollment for a PKI for more details on the certificate creation.

```
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 an SSL proposal.

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

4. Configure an SSL policy and call the SSL proposal and the PKI trustpoint.

```
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 is the IP address of GigabitEthernet0/0/0.

5. (Optional) Configure a standard access list to be used for the split-tunnel. This access list consists of the destination networks that can be accessed through the VPN tunnel. By default, all the traffic passes through the VPN tunnel (Full Tunnel) if the split tunnel is not configured.

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

6. Create an IPv4 address pool.

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

The IP address pool created assigns an IPv4 address to the AnyConnect client during a successful AnyConnect connection.

7. Upload the AnyConnect headend image (webdeploy) under **webvpn** directory of bootflash and upload the client profile to the bootflash of the router.

```
mkdir bootflash:webvpn
```

For Anyconnect package:

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

For Client Profile:

```
copy tftp: bootflash:
```

Define the AnyConnect image and the client profile as specified:

```
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 an authorization policy.

```
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
```

The IP pool, DNS, split-tunnel list, and so on are specified under the authorization policy.

9. Configure a Virtual template from which the virtual-access interfaces are cloned.

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

The unnumbered command gets the IP address from the interface configured (GigabitEthernet0/0/0) and IPv4 routing is enabled on that interface.

10. Configure an SSL profile and match the SSL policy created under it along with the authentication and authorization parameters and the virtual template.

```
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
```

11. Disable HTTP secure server.

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

Create an AnyConnect profile with the help of the AnyConnect Profile Editor. A snippet of the XML profile is given for your reference.

```
!
!
<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>
!
```

Verify

Use this section in order to confirm that your configuration works properly.

1. Check the SSL connection parameters for your anyconnect connection.

<#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. Verify the SSL session status.

<#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. Verify the tunnel statistics for the active connection.

<#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. Check the actual configuration applied for the Virtual-Acces interface associated with client.

<#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
```

Troubleshoot

This section provides the information you can use in order to troubleshoot your configuration.

1. SSL debugs to collect from the 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. A few additional commands to troubleshoot SSL connection issues:

```
# 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 from the AnyConnect client.