Configuration du VPN SSL AnyConnect pour ISR4k avec authentification locale

Table des matières

Introduction

Ce document décrit un exemple de configuration d'une tête de réseau Cisco IOS® XE 4k ISR (Integrated Service Router) pour VPN AnyConnect Secure Sockets Layer (SSL) avec une base de données d'utilisateurs locaux.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco IOS XE (ISR 4K)
- Client de mobilité sécurisée AnyConnect
- Fonctionnement général de SSL
- Infrastructures à clé publique (PKI)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco ISR4451-X/K9 avec version 17.9.2a
- Client AnyConnect Secure Mobility 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. Si votre réseau

est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

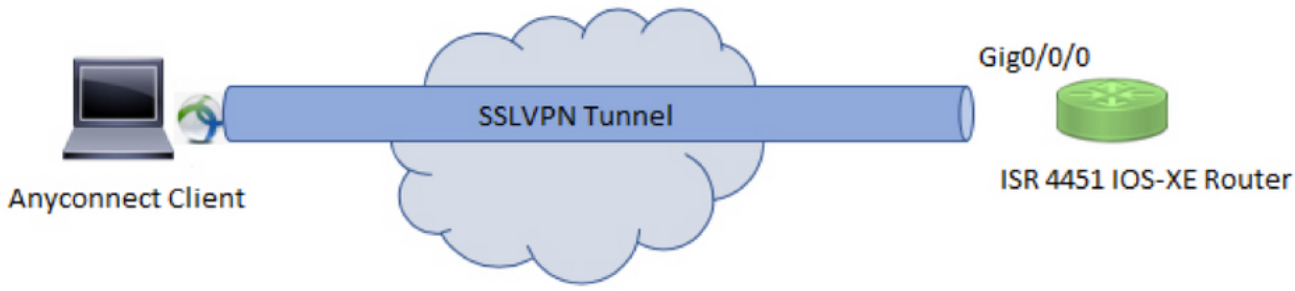
La fonction VPN (Virtual Private Network) SSL prend en charge le logiciel Cisco IOS XE pour permettre aux utilisateurs d'accéder à distance aux réseaux d'entreprise depuis n'importe quel endroit sur Internet. L'accès à distance est fourni via une passerelle VPN SSL (SSL activé) compatible Secure Socket Layer. La passerelle VPN SSL permet aux utilisateurs distants d'établir un tunnel VPN sécurisé. Grâce au VPN SSL Cisco IOS XE, les utilisateurs finaux peuvent accéder en toute sécurité depuis leur domicile ou n'importe quel site Internet, tel que les points d'accès sans fil. Le VPN SSL de Cisco IOS XE permet également aux entreprises d'étendre l'accès au réseau d'entreprise à des partenaires et consultants offshore, pour la protection des données d'entreprise.

Cette fonctionnalité est prise en charge sur les plates-formes indiquées :

Plateforme	Version prise en charge de Cisco IOS XE
Routeur de services cloud Cisco, série 1000V	Cisco IOS XE version 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bangalore 17.4.1
Routeur à services intégrés Cisco 4461 Routeur à services intégrés Cisco 4451 Routeur à services intégrés Cisco 4431	Cisco IOS XE Cupertino 17.7.1a

Configurer

Diagramme du réseau



Configurations

1. Activez AAA (Authentication, Authorization, and Accounting), configurez l'authentification, les listes d'autorisation et ajoutez un nom d'utilisateur à la base de données locale.

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

2. Créez un point de confiance pour installer le certificat d'identité, s'il n'est pas déjà présent pour l'authentification locale. Vous pouvez vous référer à Inscription de certificat pour une PKI pour plus de détails sur la création de certificat.

```
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. Configurez une proposition SSL.

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

4. Configurez une stratégie SSL et appelez la proposition SSL et le point de confiance PKI.

```
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 est l'adresse IP de GigabitEthernet0/0/0.

5. (Facultatif) Configurez une liste d'accès standard à utiliser pour le split-tunnel. Cette liste d'accès comprend les réseaux de destination accessibles via le tunnel VPN. Par défaut, tout le trafic passe par le tunnel VPN (Full Tunnel) si le tunnel partagé n'est pas configuré.

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

6. Créez un pool d’adresses IPv4.

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

Le pool d'adresses IP créé attribue une adresse IPv4 au client AnyConnect lors d'une connexion AnyConnect réussie.

7. Téléchargez l'image de tête de réseau AnyConnect (webdeploy) sous le répertoire webvpn de bootflash et téléchargez le profil client vers le bootflash du routeur.

```
mkdir bootflash:webvpn
```

Package Anyconnect :

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

Pour le profil client :

```
copy tftp: bootflash:
```

Définissez l’image AnyConnect et le profil client comme indiqué :

```
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. Configurez une stratégie d’autorisation.

```
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
```

Le pool d'adresses IP, le DNS, la liste de tunnels partagés, etc. sont spécifiés dans la stratégie d'autorisation.

9. Configurez un modèle virtuel à partir duquel les interfaces d'accès virtuel sont clonées.

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

La commande unnumbered obtient l'adresse IP de l'interface configurée (GigabitEthernet0/0/0) et le routage IPv4 est activé sur cette interface.

10. Configurez un profil SSL et faites correspondre la stratégie SSL créée sous celui-ci avec les paramètres d'authentification et d'autorisation et le modèle virtuel.

```
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
```

Créez un profil AnyConnect à l'aide de l'Éditeur de profil AnyConnect. Un extrait du profil XML est fourni à titre de référence.

```
!
!
<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>
!
```

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

<#root>

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
```

Dépannage

Cette section fournit les informations que vous pouvez utiliser afin de dépanner votre configuration.

1. Débogages SSL à collecter depuis la tête de réseau :

```
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. Quelques commandes supplémentaires pour résoudre les problèmes de connexion SSL :

```
# 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 du client AnyConnect.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.