ローカル認証を使用したISR4k用のAnyConnect SSL VPNの設定

内容

概要

このドキュメントでは、ローカルユーザデータベースを使用したAnyConnect Secure Sockets Layer(SSL)VPN用にIntegrated Service Router(ISR)4k Cisco IOS® XEヘッドエンドを設定する方法の設定例について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco IOS XE(ISR 4K)
- AnyConnect セキュア モビリティ クライアント
- 一般的なSSLの動作
- 公開キー インフラストラクチャ（PKI）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISR4451-X/K9ルータ（バージョン17.9.2a）
- AnyConnectセキュアモビリティクライアント4.10.04065

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

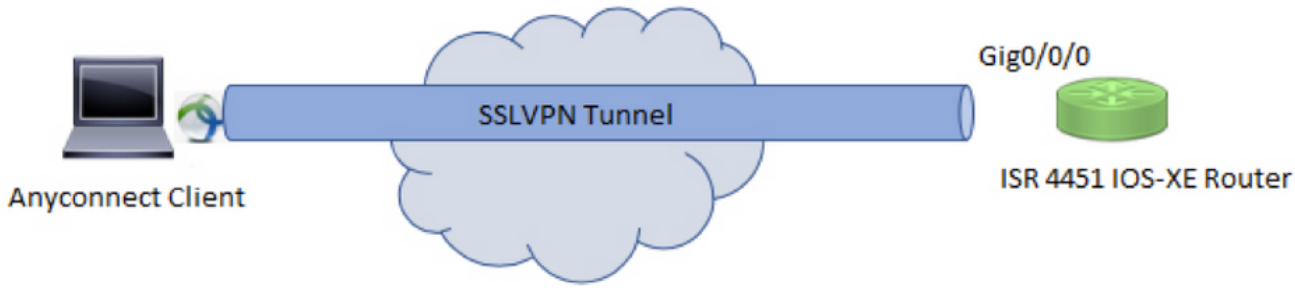
SSLバーチャルプライベートネットワーク(VPN)機能は、Cisco IOS XEソフトウェアでサポートされ、インターネット上のどこからでも企業ネットワークにリモートユーザがアクセスできるようにします。リモートアクセスは、Secure Socket Layer(SSL)対応のSSL VPNゲートウェイを介して提供されます。SSL VPNゲートウェイを使用すると、リモートユーザはセキュアなVPNトンネルを確立できます。Cisco IOS XE SSL VPNを使用すると、エンドユーザは自宅や、無線ホットスポットなどのインターネット対応の場所から安全にアクセスできます。また、Cisco IOS XE SSL VPNを使用すると、企業のデータを保護するために、企業のネットワークアクセスを海外のパートナーやコンサルタントに拡張することもできます。

この機能は、次のプラットフォームでサポートされています。

Platform	サポートされるCisco IOS XEリリース
シスコ クラウド サービス ルータ 1000V シリーズ	Cisco IOS XE Release 16.9
Cisco Catalyst 8000V	Cisco IOS XEバンガロール17.4.1
Cisco 4461 サービス統合型ルータ Cisco 4451 サービス統合型ルータ Cisco 4431 サービス統合型ルータ	Cisco IOS XE Cuppertino 17.7.1a

設定

ネットワーク図



設定

1.認証、許可、アカウンティング(AAA)を有効にし、認証、許可リストを設定し、ローカルデータベースにユーザ名を追加します。

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

2.ローカル認証用のID証明書が存在しない場合は、トラストポイントを作成してインストールします。証明書の作成の詳細については、『PKIの証明書の登録』を参照してください。

```
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. SSLプロポーザルを設定します。

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

4. SSLポリシーを設定し、SSLプロポーザルとPKIトラストポイントを呼び出します。

```
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はGigabitEthernet0/0/0のIPアドレスです。

5.（オプション）スプリットトンネルに使用する標準アクセスリストを設定します。このアクセスリストは、VPNトンネルを介してアクセス可能な宛先ネットワークで構成されます。デフォルトでは、スプリットトンネルが設定されていない場合、すべてのトラフィックはVPNトンネル（フルトンネル）を通過します。

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

6. IPv4アドレスプールを作成します。

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

作成されたIPアドレスプールは、AnyConnect接続が正常に行われるときに、AnyConnectクライアントにIPv4アドレスを割り当てます。

7.ブートフラッシュの**webvpn**ディレクトリの下にAnyConnectヘッドエンドイメージ(webdeploy)をアップロードし、クライアントプロファイルをルータのブートフラッシュにアップロードします。

AnyConnectイメージとクライアントプロファイルを指定どおりに定義します。

```
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.認可ポリシーを設定します。

```
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プール、DNS、スプリットトンネルリストなどは、認可ポリシーで指定されます。

9.バーチャルアクセスインターフェイスのクローニング元のバーチャルテンプレートを設定します。

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

unnumberedコマンドは、設定されたインターフェイス(GigabitEthernet0/0/0)からIPアドレスを取得し、そのインターフェイスでIPv4ルーティングが有効になります。

10. SSLプロファイルを設定し、その下に作成されたSSLポリシーと、認証および許可パラメータ、および仮想テンプレートを照合します。

```
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
```

AnyConnectプロファイルエディタを使用して、AnyConnectプロファイルを作成します。XMLプロファイルのスニペットが参照用に提供されます。この文書には完全なプロファイルが添付されています。

```
!
!
```

!

確認

ここでは、設定が正常に機能しているかどうかを確認します。

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
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

1.ヘッドエンドから収集するSSLデバッグ：

```
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. SSL接続の問題をトラブルシューティングするためのいくつかの追加コマンド：

```
# 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クライアントからのDART。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。