

FlexVPNの設定：ローカルユーザデータベースを使用したAnyConnect IKEv2リモートアクセス

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[設定](#)

[ローカルデータベースを使用したユーザの認証と許可](#)

[AnyConnectダウンローダ機能を無効にします\(オプション\)。](#)

[AnyConnect XMLプロファイルの配信](#)

[コミュニケーションフロー](#)

[IKEv2 および EAP エクスチェンジ](#)

[確認](#)

[トラブルシューティング](#)

はじめに

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てAnyConnect IKEv2/EAP認証を介したアクセス用にCisco IOS®/XEヘッドエンドを設定する方法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。

- IKEv2プロトコル

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 IOS® XE 16.9.2を実行するCisco Cloud Services Router(CSR)
- Windows 10 で動作する AnyConnect クライアント バージョン 4.6.03049

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、クリアな(デフォルト)設定で作業を開始していま

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

AnyConnect-EAP (アグリゲート認証とも呼ばれる) を使用すると、Flex ServerでCisco独自のAnyConnect-EAP方式を使用してAnyConnectクライアントを認証できます。

EAP-Generic Token Card (EAP-GTC)、EAP Message Digest 5 (EAP-MD5) など、標準ベースの Extensible Authentication Protocol (EAP; 拡張可能認証プロトコル) 方式とは異なり、Flex Server は EAP パススルー モードで動作しません。

EAP とクライアント間の通信はすべて Flex Server で終端し、AUTH ペイロードの作成に必要なセッションキーが Flex Server でローカルに計算されます。

Flex Serverは、IKEv2 RFCの要件に従って、証明書を使用してクライアントに対して自身を認証する必要があります。

ローカル ユーザ認証は Flex Server でサポートされており、リモート認証はオプションです。

これは、リモート アクセス ユーザの数が少ない小規模な導入環境、および認証、認可、およびアカウントリング (AAA) 外部サーバにアクセスできない環境で理想的です。

ただし大規模導入環境や、ユーザ別の属性が必要な状況では、認証と認可に外部 AAA サーバを使用することが推奨されます。


AnyConnect-EAPの実装では、リモート認証、許可、アカウントリングにRADIUSを使用できます。

ネットワーク図



設定

ローカルデータベースを使用したユーザの認証と許可

 注：ルータのローカルデータベースに対してユーザを認証するには、EAPを使用する必要があります。ただし、EAPを使用するには、ローカル認証方式がrsa-sigである必要があります。そのため、ルータには適切な証明書がインストールされている必要があります。自己署名証明書にすることはできません。

設定例では、ローカル ユーザ認証、リモート ユーザおよびグループ認可、およびリモート アカウンティングを使用します。

ステップ 1：AAAを有効にし、認証、許可、およびアカウンティング(AAA)リストを設定し、ユーザ名をローカルデータベースに追加します。

```
aaa new-model
!
aaa authentication login a-eap-authen-local local
aaa authorization network a-eap-author-grp local
!
username test password cisco123
```

ステップ 2：ルータ証明書を保持するトラストポイントを設定します。この例では、PKCS12ファイルインポートを使用しています。その他のオプションについては、PKI(Public Key Infrastructure)コンフィギュレーションガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xs-3s/sec-pki-xe-3s-book/sec-cert-enroll-pki.html

```
Router(config)# crypto pki import IKEv2-TP pkcs12 bootflash:IKEv2-TP.p12 password cisco123
```

ステップ 3：AnyConnect VPNクライアントにアドレスを割り当てるIPローカルプールを定義します。

```
ip local pool ACP00L 192.168.10.5 192.168.10.10
```


ステップ 4：IKEv2ローカル認可ポリシーを作成します。

```
crypto ikev2 authorization policy ikev2-auth-policy
 pool ACP00L
 dns 10.0.1.1
```

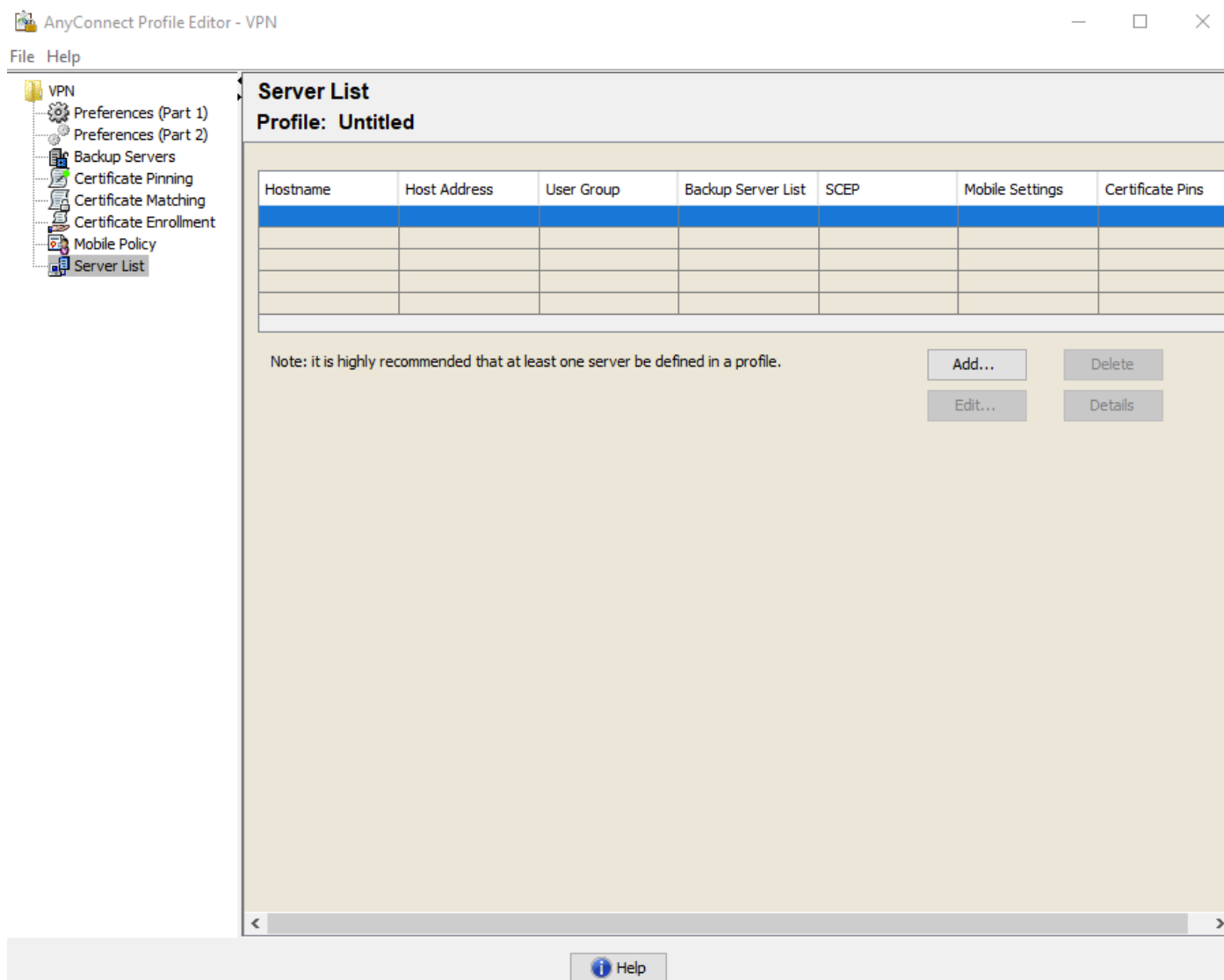
ステップ 5 (オプション) : 目的のIKEv2プロポーザルとポリシーを作成します。設定されていない場合は、スマートデフォルトが使用されます。

```
crypto ikev2 proposal IKEv2-prop1
  encryption aes-cbc-256
  integrity sha256
  group 14
!
crypto ikev2 policy IKEv2-po1
  proposal IKEv2-prop1
```

手順 6 : AnyConnectプロフィールの作成

 注:AnyConnectプロフィールは、クライアントマシンに配信される必要があります。詳細については、次のセクションを参照してください。

図に示すように、AnyConnectプロフィールエディタでクライアントプロフィールを設定します。



The screenshot shows the 'AnyConnect Profile Editor - VPN' window. The left sidebar contains a tree view with the following items: VPN, Preferences (Part 1), Preferences (Part 2), Backup Servers, Certificate Pinning, Certificate Matching, Certificate Enrollment, Mobile Policy, and Server List. The main area is titled 'Server List' and 'Profile: Untitled'. It features a table with the following columns: Hostname, Host Address, User Group, Backup Server List, SCEP, Mobile Settings, and Certificate Pins. Below the table, there is a note: 'Note: it is highly recommended that at least one server be defined in a profile.' and four buttons: 'Add...', 'Delete', 'Edit...', and 'Details'. A 'Help' button is located at the bottom center of the window.

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins

[追加]をクリックして、VPNゲートウェイのエントリを作成します。必ず「IPsec」を「Primary Protocol」として選択してください。「ASAゲートウェイ」オプションのチェックを外します。

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) VPN IOS-XE

FQDN or IP Address User Group

vpn.example.com /

Group URL

vpn.example.com

Connection Information

Primary Protocol IPsec

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address Add

Move Up

Move Down

Delete

OK Cancel


プロファイルを保存します。[ファイル] -> [名前を付けて保存]。このプロファイルに相当するXML :


```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema"
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
    <AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
    <ShowPreConnectMessage>false</ShowPreConnectMessage>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreMac>All</CertificateStoreMac>
    <CertificateStoreOverride>false</CertificateStoreOverride>
    <ProxySettings>Native</ProxySettings>
    <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
    <AuthenticationTimeout>12</AuthenticationTimeout>
    <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">false</LocalLanAccess>
    <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
```

```

<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
  <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSA SecurIDIntegration UserControllable="false">Automatic</RSA SecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVpNEstablishment>LocalUsersOnly</WindowsVpNEstablishment>
<AutomaticVpnPolicy>false</AutomaticVpnPolicy>
<PPPEXclusion UserControllable="false">Disable
  <PPPEXclusionServerIP UserControllable="false"></PPPEXclusionServerIP>
</PPPEXclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
  <HostEntry>
    <HostName>VPN IOS-XE</HostName>
    <HostAddress>vpn.example.com</HostAddress>
    <PrimaryProtocol>IPsec
      <StandardAuthenticationOnly>true
        <AuthMethodDuringIKENegotiation>EAP-AnyConnect</AuthMethodDuringIKENegotiation>
      </StandardAuthenticationOnly>
    </PrimaryProtocol>
  </HostEntry>
</ServerList>
</AnyConnectProfile>


```

 注: AnyConnectでは、キーIDタイプのデフォルトのIKE IDとして"*\$AnyConnectClient\$"を使用します。ただし、AnyConnectプロファイルでこのIDを手動で変更して、導入のニーズに合わせることができます。

 注:XMLプロファイルをルータにアップロードするには、Cisco IOS® XE 16.9.1バージョン以降が必要です。古いバージョンのCisco IOS® XEソフトウェアを使用している場合は、クライアントでプロファイルダウンロード機能を無効にする必要があります。詳細については、「AnyConnectダウンロード機能の無効化」の項を参照してください。


作成したXMLプロファイルをルータのフラッシュメモリにアップロードし、プロファイルを定義します。


```
crypto vpn anyconnect profile acvpn bootflash:/acvpn.xml
```

 注:AnyConnect XMLプロファイルに使用されるファイル名はacvpn.xmlです。

手順 7 : クライアント認証のAnyConnect-EAP方式のIKEv2プロファイルを作成します。


```
crypto ikev2 profile AnyConnect-EAP
match identity remote key-id *$AnyConnectClient$*
authentication local rsa-sig
authentication remote anyconnect-eap aggregate
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 100
anyconnect profile acvpn
```

 注 : ローカル認証方式よりも前のリモート認証方式の設定は、CLIで受け入れられます。ただし、リモート認証方式がeapの場合、拡張要求Cisco Bug ID CSCvb29701の修正が適用されていないバージョンでは有効になりません。これらのバージョンでは、リモート認証方式としてeap設定を行う場合は、最初にローカル認証方式がrsa-sigとして設定されていることを確認してください。この問題は、その他のリモート認証方式では発生していません。

 注 : Cisco Bug ID CSCvb24236の影響を受けるコードのバージョンでは、ローカル認証の前にリモート認証が設定されると、そのデバイスではリモート認証方式を設定できなくなります。このコードに対するフィックスが適用されているバージョンにアップグレードしてください。

ステップ 8 : ルータでHTTP-URLベースの証明書検索とHTTPサーバを無効にします。

```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

 注 : ご使用のルータハードウェアがNGE暗号化アルゴリズムをサポートしているかどうかを確認するには、[このドキュメント](#)を参照してください (前の例ではNGEアルゴリズムを使用しています)。サポートしていない場合、ハードウェアへのIPSec SAのインストールはネゴシエーションの最後の段階で失敗します。

ステップ 9 : データの保護に使用する暗号化アルゴリズムとハッシュアルゴリズムを定義する

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
mode tunnel
```

ステップ 10 : IPSecプロファイルを作成します。

```
crypto ipsec profile AnyConnect-EAP
 set transform-set TS
 set ikev2-profile AnyConnect-EAP
```

ステップ 11何らかのダミーIPアドレスを使用してループバックインターフェイスを設定します。バーチャルアクセスインターフェイスは、そこからIPアドレスを借ります。

```
interface loopback100
 ip address 10.0.0.1 255.255.255.255
```

ステップ 12仮想テンプレートの設定 (テンプレートをIKEv2プロファイルに関連付ける)

```
interface Virtual-Template100 type tunnel
 ip unnumbered Loopback100
 ip mtu 1400
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile AnyConnect-EAP
```

手順13 (オプション) 。デフォルトでは、クライアントからのすべてのトラフィックはトンネル経由で送信されます。スプリットトンネルを設定すると、選択したトラフィックだけがトンネルを通過できるようになります。

```
ip access-list standard split_tunnel
 permit 10.0.0.0 0.255.255.255
!
crypto ikev2 authorization policy ikev2-auth-policy
 route set access-list split_tunnel
```

ステップ 14 (オプション) : すべてのトラフィックがトンネルを通過する必要がある場合は、リモートクライアントにインターネット接続を許可するようにNATを設定します。

```
ip access-list extended NAT
 permit ip 192.168.10.0 0.0.0.255 any
!
ip nat inside source list NAT interface GigabitEthernet1 overload
!
interface GigabitEthernet1
 ip nat outside
```



```
!  
interface Virtual-Template 100  
 ip nat inside
```

AnyConnectダウンロード機能を無効にします (オプション)。

この手順が必要なのは、16.9.1よりも古いバージョンのCisco IOS® XEソフトウェアを使用している場合だけです。Cisco IOS® XE 16.9.1より前は、XMLプロファイルをルータにアップロードする機能は使用できませんでした。デフォルトでは、AnyConnectクライアントは、ログインが成功した後にXMLプロファイルのダウンロードを試行します。プロファイルが使用できない場合、接続は失敗します。回避策として、クライアント自体でAnyConnectプロファイルのダウンロード機能を無効にすることができます。これを行うには、次のファイルを変更できます。

For Windows:

```
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\AnyConnectLocalPolicy.xml
```

For MAC OS:

```
/opt/cisco/anyconnect/AnyConnectLocalPolicy.xml
```

「BypassDownloader」オプションは、次のように「true」に設定されます。

```
<?xml version="1.0" encoding="UTF-8"?>  
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap/encoding/ http://www.w3.org/2001/XMLSchema-instance">  
<BypassDownloader>true</BypassDownloader>  
<EnableCRLCheck>false</EnableCRLCheck>  
<ExcludeFirefoxNSSCertStore>false</ExcludeFirefoxNSSCertStore>  
<ExcludeMacNativeCertStore>false</ExcludeMacNativeCertStore>  
<ExcludePemFileCertStore>false</ExcludePemFileCertStore>  
<ExcludeWinNativeCertStore>false</ExcludeWinNativeCertStore>  
<FipsMode>false</FipsMode>  
<RestrictPreferenceCaching>false</RestrictPreferenceCaching>  
<RestrictTunnelProtocols>false</RestrictTunnelProtocols>  
<RestrictWebLaunch>false</RestrictWebLaunch>  
<StrictCertificateTrust>false</StrictCertificateTrust>  
<UpdatePolicy>  
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>  
<AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>  
<AllowServiceProfileUpdatesFromAnyServer>true</AllowServiceProfileUpdatesFromAnyServer>  
<AllowSoftwareUpdatesFromAnyServer>true</AllowSoftwareUpdatesFromAnyServer>  
<AllowVPNProfileUpdatesFromAnyServer>true</AllowVPNProfileUpdatesFromAnyServer></UpdatePolicy>  
</AnyConnectLocalPolicy>
```

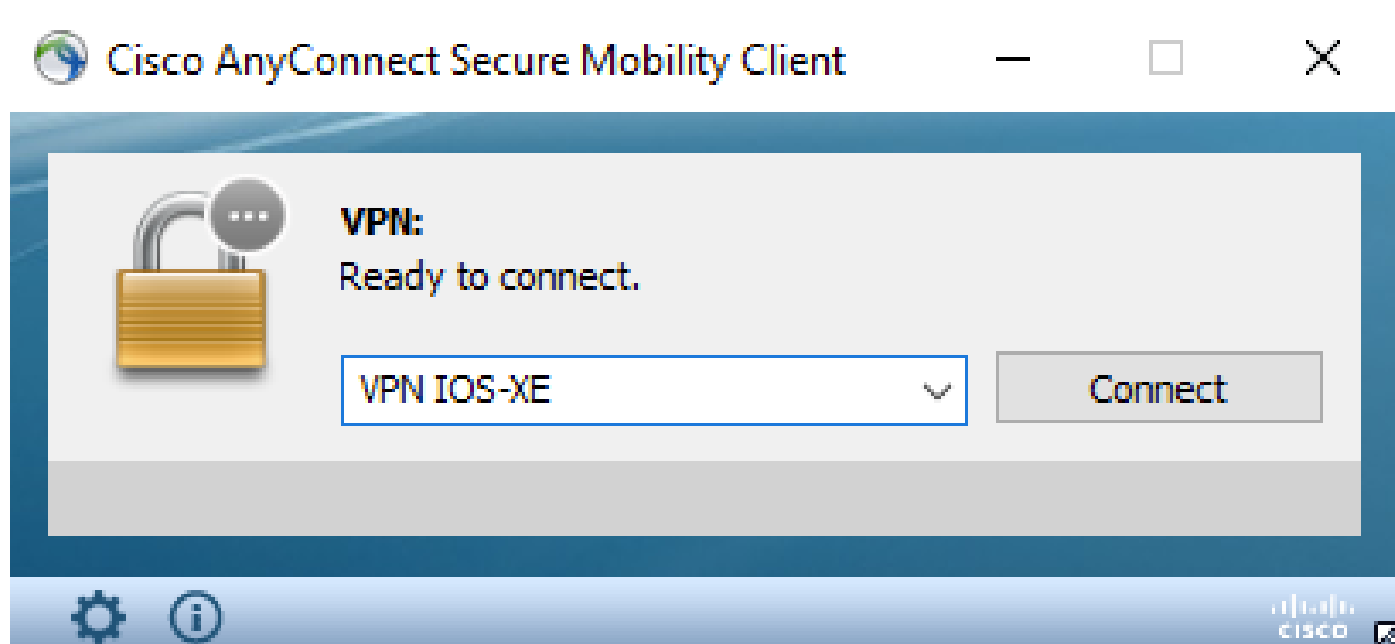
変更後、AnyConnectクライアントを再起動する必要があります。

AnyConnect XMLプロファイルの配信

AnyConnectの新規インストール (XMLプロファイルが追加されていない状態) では、ユーザは AnyConnectクライアントのアドレスバーにVPNゲートウェイのFQDNを手動で入力できます。これにより、ゲートウェイへのSSL接続が確立されます。デフォルトでは、AnyConnectクライアントはIKEv2/IPsecプロトコルを使用してVPNトンネルを確立しようとしません。このため、XMLプロファイルがクライアントにインストールされ、Cisco IOS® XE VPNゲートウェイとのIKEv2/IPsecトンネルを確立する必要があります。

プロファイルは、AnyConnectアドレスバーのドロップダウンリストから選択されたときに使用されます。

表示される名前は、AnyConnectプロファイルエディタの「表示名」で指定された名前と同じです。



XMLプロファイルは、次のディレクトリに手動で配置できます。

For Windows:

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

For MAC OS:

/opt/cisco/anyconnect/profile

プロファイルがGUIに表示されるようにするには、AnyConnectクライアントを再起動する必要があります。AnyConnectウィンドウを閉じるだけでは不十分です。プロセスは、WindowsトレイのAnyConnectアイコンを右クリックし、「Quit」オプションを選択して再起動できます。

Open AnyConnect



Show Connection Notices

VPN

Connect

About

Quit



ENG

11:16 AM

PLP

12/14/2018



コミュニケーションフロー

IKEv2 および EAP エクスチェンジ

IKE_SA_INIT: HDR, SAi1, KEi, Ni,
V(Fragmentation), V(AnyConnect-EAP),
V(Cisco-Copyright)

IKEv2-INTERNAL (1): Received custom vendor id : CISCO(COPYRIGHT)
IKEv2-INTERNAL (1): Received custom vendor id : CISCO-ANYCONNECT-EAP

IKE_SA_INIT: HDR, SAr1, KEr, Nr,
V(Fragmentation), V(AnyConnect-EAP), V(Cisco-
Copyright), V(Cisco-GRE-MODE)

IKEv2-INTERNAL (1): Sending custom vendor id : CISCO(COPYRIGHT)
IKEv2-INTERNAL (1): Sending custom vendor id : CISCO-GRE-MODE
IKEv2-INTERNAL (1): Sending custom vendor id : CISCO-ANYCONNECT-EAP

IKE_AUTH: HDR, SK (IDi, CERTREQ,
CP(CFG_REQUEST(INTERNAL_IP4_ADDRESS,
INTERNAL_IP4_NETMASK, ...)), SAi2, TSi, TSr)

Searching policy based on peer's identity "\$AnyConnectClient\$" of type 'key ID'

IKE_AUTH: HDR, SK (IDr, CERT, AUTH,
EAP(request{ACDT0{<config-auth
type="hello">}}))

-Sending AnyConnect EAP 'hello' request

IKE_AUTH: HDR, SK (EAP(RES{ACDT0{
<config-auth type="init">}}))

IKEv2: (SESSION ID = 38, SA ID = 1): Processing AnyConnect EAP response

IKE_AUTH: HDR, SK (IDr, CERT, AUTH,
EAP(request{ACDT0{<config-auth type="auth-
request">}}))

IKEv2: (SESSION ID = 38, SA ID = 1): Sending AnyConnect EAP 'auth-request'

IKE_AUTH: HDR, SK (EAP(RES{ACDT0{
<config-auth type="auth-reply">}}))

IKEv2: (SESSION ID = 30, SA ID = 1): Processing AnyConnect EAP response

IKE_AUTH: HDR, SK (IDr, CERT, AUTH,
EAP(request{ACDT0{<config-auth
type="complete">}}))

IKEv2: (SESSION ID = 30, SA ID = 1): Sending AnyConnect EAP 'VERIFY' request

Router# show crypto ikev2 sa detailed

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/ivrf	Status
1	192.0.2.1/4500			

192.0.2.100/50899

none/none READY

Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: RSA, Auth verify: A

Life/Active Time: 86400/758 sec

CE id: 1004, Session-id: 4

Status Description: Negotiation done

Local spi: 413112E83D493428 Remote spi: 696FA78292A21EA5

Local id: 192.0.2.1

Remote id: *\$AnyConnectClient\$*

Remote EAP id: test

<----- username

Local req msg id: 0 Remote req msg id: 31

Local next msg id: 0 Remote next msg id: 31

Local req queued: 0 Remote req queued: 31

Local window: 5 Remote window: 1

DPD configured for 0 seconds, retry 0

Fragmentation not configured.

Dynamic Route Update: disabled

Extended Authentication not configured.

NAT-T is detected outside

Cisco Trust Security SGT is disabled

Assigned host addr: 192.168.10.8. <---- Assigned IP

Initiator of SA : No

! Check the crypto session information

Router# show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

X - IKE Extended Authentication, F - IKE Fragmentation

R - IKE Auto Reconnect, U - IKE Dynamic Route Update

S - SIP VPN

Interface: Virtual-Access1. <----- Virtual interface associated with the client

Profile: AnyConnect-EAP
Uptime: 00:14:54
Session status: UP-ACTIVE

Peer: 192.0.2.100

port 50899 fvrf: (none) ivrf: (none).

<----- Public IP of the remote client

Phase1_id: *\$AnyConnectClient\$*
Desc: (none)
Session ID: 8
IKEv2 SA: local 192.0.2.1/4500 remote 192.0.2.100/50899 Active
Capabilities:N connid:1 lifetime:23:45:06
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.10.8
Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 89

drop 0 life (KB/Sec) 4607990/2705.

<----- Packets received from the client

Outbound: #pkts enc'ed 2

drop 0 life (KB/Sec) 4607999/2705.

<----- Packets sent to the client

! Check the actual configuration applied for the Virtual-Access interface associated with client

Router# show derived-config interface virtual-access 1.

Building configuration...

Derived configuration : 258 bytes

```
!  
interface Virtual-Access1  
 ip unnumbered Loopback100  
 ip mtu 1400  
 ip nat inside  
 tunnel source 192.0.2.1  
 tunnel mode ipsec ipv4  
 tunnel destination 192.0.2.100  
 tunnel protection ipsec profile AnyConnect-EAP  
 no tunnel protection ipsec initiate  
end
```

トラブルシューティング

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される IKEv2 デバッグ :

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
```

2. ローカル属性とリモート属性の割り当てを表示するための AAA デバッグ :

```
debug aaa authorization
debug aaa authentication
```

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。