

FlexVPN 구성: 로컬 사용자 데이터베이스를 사용하는 AnyConnect IKEv2 원격 액세스

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[구성](#)

[로컬 데이터베이스를 사용하는 사용자의 인증 및 권한 부여](#)

[AnyConnect 다운로드 기능을 비활성화합니다\(선택 사항\).](#)

[AnyConnect XML 프로파일 제공](#)

[통신 흐름](#)

[IKEv2 및 EAP 교환](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 로컬 사용자 데이터베이스를 사용하여 AnyConnect IKEv2/EAP 인증을 통해 액세스 하기 위해 Cisco IOS®/XE 헤드엔드를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IKEv2 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® XE 16.9.2를 실행하는 Cisco Cloud Services Router
- Windows 10에서 실행되는 AnyConnect 클라이언트 버전 4.6.03049

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

종합 인증이라고도 하는 AnyConnect-EAP는 Flex Server가 Cisco 전용 AnyConnect-EAP 방법을 통해 AnyConnect 클라이언트를 인증하도록 허용합니다.

EAP-GTC(EAP-Generic Token Card), EAP-MD5(EAP-Message Digest 5) 등의 표준 기반 EAP(Extensible Authentication Protocol) 방법과 달리 Flex Server는 EAP 통과 모드에서 작동하지 않습니다.

클라이언트와의 모든 EAP 통신은 Flex Server에서 종료되며 AUTH 페이로드를 구성하는 데 사용되는 필수 세션 키는 Flex Server에서 로컬로 계산됩니다.

Flex Server는 IKEv2 RFC에 필요한 인증서로 클라이언트에 대해 스스로를 인증해야 합니다.

이제 Flex Server에서 로컬 사용자 인증이 지원되며 원격 인증은 선택 사항입니다.

이 기능은 원격 액세스 사용자 수가 적고 외부 AAA(Authentication, Authorization, and Accounting) 서버에 액세스할 수 없는 환경에서 소규모 구축에 적합합니다.

그러나 대규모 구축의 경우 및 사용자별 특성이 필요한 시나리오의 경우 인증 및 권한 부여를 위해 외부 AAA 서버를 사용하는 것이 좋습니다.


AnyConnect-EAP 구현에서는 원격 인증, 권한 부여 및 어카운팅에 Radius를 사용할 수 있습니다.


네트워크 다이어그램



구성

로컬 데이터베이스를 사용하는 사용자의 인증 및 권한 부여

 참고: 라우터의 로컬 데이터베이스에 대해 사용자를 인증하려면 EAP를 사용해야 합니다. 그러나 EAP를 사용하려면 로컬 인증 방법이 rsa-sig여야 하므로 라우터에 적절한 인증서가 설치

 되어 있어야 하며 자체 서명 인증서가 될 수 없습니다.

로컬 사용자 인증, 원격 사용자 및 그룹 권한 부여 및 원격 어카운팅을 사용하는 샘플 컨피그레이션입니다.

1단계. AAA를 활성화하고 인증, 권한 부여 및 계정 관리 목록을 구성하고 로컬 데이터베이스에 사용자 이름을 추가합니다.

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

2단계. 라우터 인증서를 보유할 신뢰 지점을 구성합니다. 이 예에서는 PKCS12 파일 가져오기가 사용됩니다. 기타 옵션은 PKI(Public Key Infrastructure) 컨피그레이션 가이드를 참조하십시오.

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
```

3단계. AnyConnect VPN 클라이언트에 주소를 할당하기 위해 IP 로컬 풀을 정의합니다.

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

4단계. IKEv2 로컬 권한 부여 정책을 생성합니다.

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

5단계(선택 사항) 원하는 IKEv2 제안서 및 정책을 생성합니다. 구성되지 않은 경우 스마트 기본값이 사용됩니다.


```
crypto ikev2 proposal IKEv2-prop1
```

```

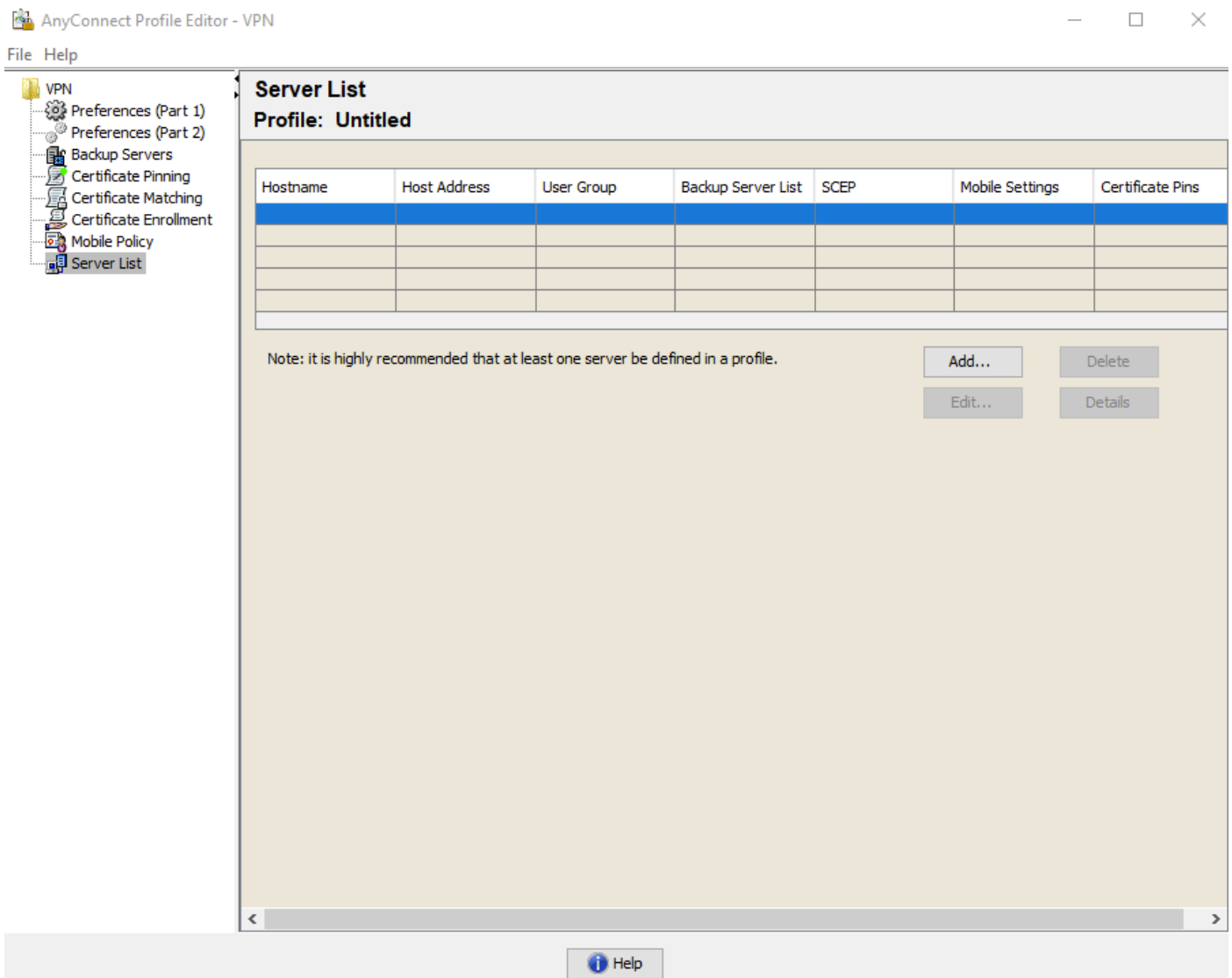
encryption aes-cbc-256
integrity sha256
group 14
!
crypto ikev2 policy IKEv2-pol
proposal IKEv2-prop1

```

6단계. AnyConnect 프로파일 생성

 참고: AnyConnect 프로파일은 클라이언트 머신에 전달되어야 합니다. 자세한 내용은 다음 섹션을 참조하십시오.

이미지에 표시된 대로 AnyConnect 프로파일 편집기로 클라이언트 프로파일을 구성합니다.



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'. At the bottom center, there is a 'Help' button.

VPN 게이트웨이에 대한 항목을 생성하려면 "Add(추가)"를 클릭합니다. "IPsec"을 "Primary Protocol(기본 프로토콜)"로 선택해야 합니다. "ASA 게이트웨이" 옵션의 선택을 취소합니다.

Server **Load Balancing Servers** SCEP Mobile Certificate Pinning

Primary Server

Display Name (required)

FQDN or IP Address /

User Group

Group URL

Connection Information

Primary Protocol

ASA gateway

Auth Method During IKE Negotiation

IKE Identity (IOS gateway only)

Backup Servers

| Host Address | |
|--------------|---|
| | <input type="button" value="Add"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Delete"/> |


프로파일을 저장합니다. 역할 -> 다른 이름으로 저장. 프로필의 XML에 해당하는 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>
  </ClientInitialization>
</AnyConnectProfile>
```

```

<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<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>


```

 참고: AnyConnect는 '\$AnyConnectClient\$'를 key-id 유형의 기본 IKE ID로 사용합니다. 그러나 AnyConnect 프로파일에서 배포 요구 사항에 맞게 이 ID를 수동으로 변경할 수 있습니다.

 참고: XML 프로필을 라우터에 업로드하려면 Cisco IOS® XE 16.9.1 버전 이상이 필요합니다. 이전 버전의 Cisco IOS® XE 소프트웨어를 사용하는 경우 클라이언트에서 프로파일 다운로드 기능을 비활성화해야 합니다. 자세한 내용은 "AnyConnect 다운로더 기능 비활성화" 섹션을 참조하십시오.

생성된 XML 프로파일을 라우터의 플래시 메모리에 업로드하고 프로파일을 정의합니다.


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


 참고: AnyConnect XML 프로파일에 사용되는 파일 이름은 acvpn.xml입니다.

7단계. 클라이언트 인증의 AnyConnect-EAP 방법을 위한 IKEv2 프로파일을 생성합니다.

```
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
```

 참고: 로컬 인증 방법 이전의 원격 인증 방법 컨피그레이션은 CLI에서 수락되지만, 원격 인증 방법이 eap인 경우, 개선 요청 Cisco 버그 ID [CSCvb29701](#)에 대한 수정 사항이 없는 버전에 대해서는 적용되지 않습니다. 이러한 버전의 경우 eap 컨피그레이션이 원격 인증 방법인 경우 먼저 로컬 인증 방법이 rsa-sig로 구성되었는지 확인합니다. 이 문제는 원격 인증 방법의 다른 형태에서는 보이지 않습니다.

 참고: Cisco 버그 ID [CSCvb24236](#)의 영향을 받는 코드 버전에서 로컬 인증 전에 원격 인증이 구성되면 해당 디바이스에서 원격 인증 방법을 더 이상 구성할 수 없습니다. 이 코드에 대한 수정 사항이 있는 버전으로 업그레이드하십시오.

8단계. 라우터에서 HTTP-URL 기반 인증서 조회 및 HTTP 서버를 비활성화합니다.

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

 참고: [이 문서](#)를 참조하여 라우터 하드웨어가 NGE 암호화 알고리즘을 지원하는지(이전 예시에 NGE 알고리즘이 있음) 확인합니다. 그렇지 않으면 하드웨어에 IPSec SA를 설치하지 못할 경우 마지막 협상 단계에서 실패합니다.

9단계. 데이터 보호에 사용되는 암호화 및 해시 알고리즘 정의

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

10단계. IPSec 프로필을 생성합니다.

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

11단계. 일부 더미 IP 주소로 루프백 인터페이스를 구성합니다. Virtual-Access 인터페이스는 IP 주소를 차용합니다.

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

12단계. 가상 템플릿 구성(IKEv2 프로파일에서 템플릿 연결)

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

단계 13(선택 사항). 기본적으로 클라이언트에서 오는 모든 트래픽은 터널을 통해 전송됩니다. 선택한 트래픽만 터널을 통과하도록 허용하는 스플릿 터널을 구성할 수 있습니다.

```
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
```

14단계(선택 사항) 모든 트래픽이 터널을 통과해야 하는 경우 원격 클라이언트에 대한 인터넷 연결을 허용하도록 NAT를 구성합니다.

```
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 다운로드 기능을 비활성화합니다(선택 사항).

이 단계는 16.9.1 이전 Cisco IOS® XE 소프트웨어 버전을 사용하는 경우에만 필요합니다. Cisco IOS® XE 16.9.1 이전에는 라우터에 XML 프로파일을 업로드하는 기능을 사용할 수 없었습니다.

AnyConnect 클라이언트는 기본적으로 로그인에 성공한 후 XML 프로파일 다운로드를 시도합니다. 프로파일을 사용할 수 없는 경우 연결이 실패합니다. 이를 해결하려면 클라이언트 자체에서 AnyConnect 프로파일 다운로드 기능을 비활성화할 수 있습니다. 이 작업을 수행하려면 다음 파일을 수정할 수 있습니다.

For Windows:

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

For MAC OS:

/opt/cisco/anyconnect/AnyConnectLocalPolicy.xml

"BypassDownloader" 옵션은 "true"로 설정됩니다. 예를 들면 다음과 같습니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy xmlns="http://schemas.xmlsoap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema"
<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>
```

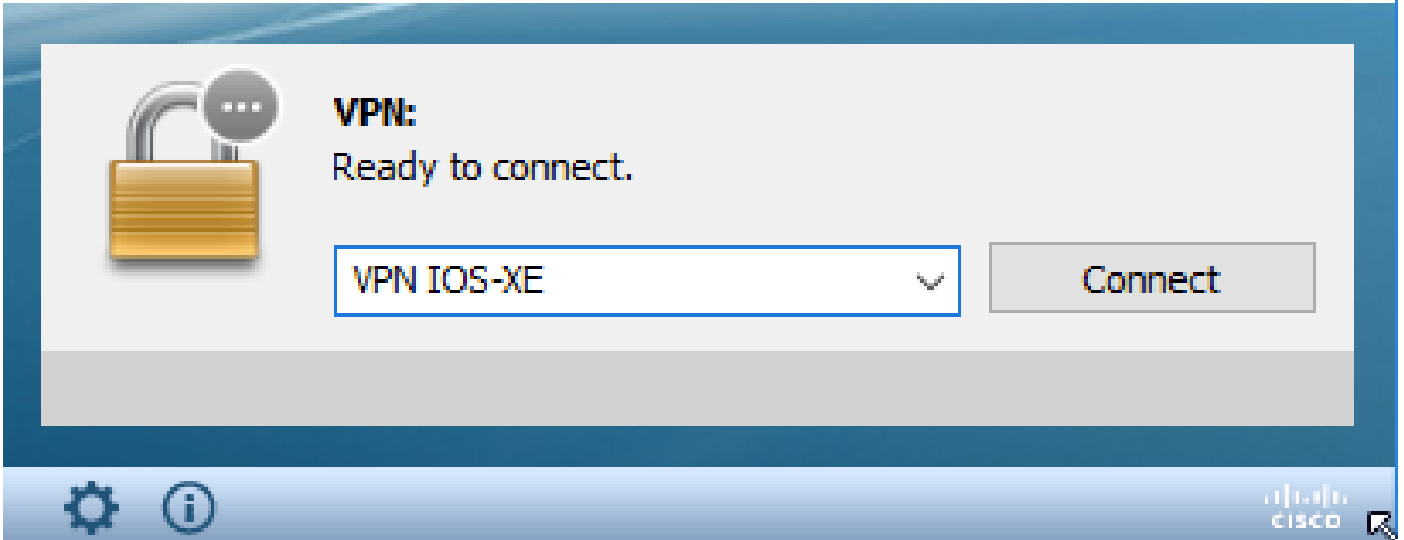
수정 후 AnyConnect 클라이언트를 다시 시작해야 합니다.

AnyConnect XML 프로파일 제공

AnyConnect를 새로 설치하면(XML 프로파일이 추가되지 않음) AnyConnect 클라이언트의 주소 표시줄에 VPN 게이트웨이의 FQDN을 수동으로 입력할 수 있습니다. 그러면 게이트웨이에 대한 SSL 연결이 생성됩니다. AnyConnect 클라이언트는 기본적으로 IKEv2/IPsec 프로토콜로 VPN 터널을 설정하려고 시도하지 않습니다. Cisco IOS® XE VPN 게이트웨이를 사용하여 IKEv2/IPsec 터널을 설정하려면 클라이언트에 XML 프로파일이 설치되어 있어야 하기 때문입니다.

프로파일은 AnyConnect 주소 표시줄의 드롭다운 목록에서 선택할 때 사용됩니다.

표시되는 이름은 AnyConnect 프로파일 편집기의 "Display Name"에 지정된 이름과 같습니다.



XML 프로파일을 이 디렉토리에 수동으로 넣을 수 있습니다.

For Windows:

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

For MAC OS:

/opt/cisco/anyconnect/profile

GUI에서 프로파일을 표시하려면 AnyConnect 클라이언트를 다시 시작해야 합니다. AnyConnect 창을 닫기에는 충분하지 않습니다. Windows 트레이에서 AnyConnect 아이콘을 마우스 오른쪽 버튼으로 클릭하고 "Quit(종료)" 옵션을 선택하여 프로세스를 다시 시작할 수 있습니다.

Open AnyConnect



Show Connection Notices

VPN

Connect

About

Quit



ENG

11:16 AM

PLP

12/14/2018



통신 흐름

IKEv2 및 EAP 교환

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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

1. 헤드엔드에서 수집할 IKEv2 디버깅:

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

2. AAA는 로컬 및/또는 원격 특성의 할당을 보기 위해 디버깅합니다.

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

3. AnyConnect 클라이언트의 DART

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.