AnyConnect to IOS Headend Over IPsec with IKEv2 and Certificates 컨피그레이션 예

목차

소개

이 문서에서는 AnyConnect 클라이언트를 실행하는 디바이스에서 FlexVPN 프레임워크를 활용하여 인증서 인증만 있는 Cisco IOS® 라우터에 IPsec으로 보호된 연결을 구현하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FlexVPN
- AnyConnect

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

헤드엔드

Cisco IOS 라우터는 최소 15.2 M&T 릴리스를 실행하는 IKEv2를 실행할 수 있는 모든 라우터가 될 수 있습니다. 그러나 최신 릴리스를 사용해야 합니다(알려진 주의 섹션 참조).

클라이언트

AnyConnect 3.x 릴리스

인증 기관

이 예에서 CA(Certificate Authority)는 15.2(3)T 릴리스를 실행합니다.

EKU(Extended Key Usage)를 지원해야 하기 때문에 최신 릴리스 중 하나를 사용해야 합니다.

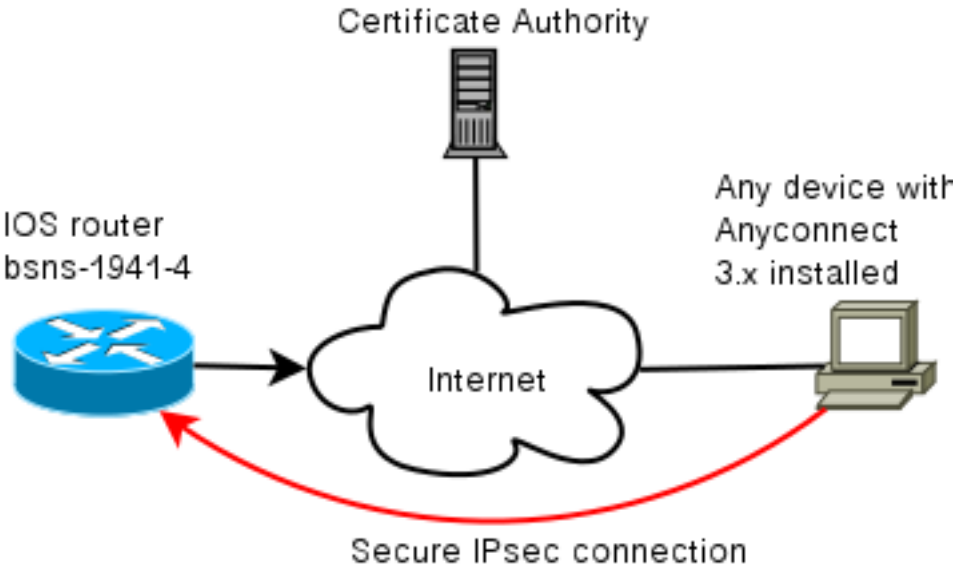
이 구축에서는 IOS 라우터가 CA로 사용됩니다. 그러나 EKU를 사용할 수 있는 모든 표준 기반 CA 애플리케이션도 괜찮습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

구성

네트워크 토폴로지



인증 기관(선택 사항)

IOS 라우터를 사용하도록 선택하면 CA 역할을 수행할 수 있습니다.

IOS CA 컨피그레이션

CA 서버는 클라이언트 및 서버 인증서에 올바른 EKU를 배치해야 합니다. 이 경우 모든 인증서에 대해 server-auth 및 client-auth EKU가 설정되었습니다.

```
bsns-1941-3#show run | s crypto pki
crypto pki server CISCO
database level complete
database archive pem password 7 00071A1507545A545C
issuer-name cn=bsns-1941-3.cisco.com,ou=TAC,o=cisco
grant auto rollover ca-cert
grant auto
auto-rollover
eku server-auth client-auth
```

인증서에 올바른 EKU가 설정되어 있는지 확인하는 방법

bsns-1941-3은 CA 서버이고 bsns-1941-4는 IPsec 헤드엔드입니다. 출력 부분은 간결하게 생략되었습니다.

```
BSNS-1941-4#show crypto pki certificate verbose
Certificate
(...omitted...)

Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: C3D52BE9 1EE97559 C7323995 3C51DC53
Fingerprint SHA1: 76BC7CD4 F298F8D9 A95338DC E5AF7602 9B57BE31
X509v3 extensions:
X509v3 Key Usage: A0000000
Digital Signature
Key Encipherment
X509v3 Subject Key ID: 83647B09 D3300A97 577C3E2C AAE7F47C F2D88ADF
X509v3 Authority Key ID: B3CC331D 7159C3CD 27487322 88AC02ED FAF2AE2E
Authority Info Access:
Extended Key Usage:
Client Auth
Server Auth
Associated Trustpoints: CISCO2
Storage: nvram:bsns-1941-3c#5.cer
Key Label: BSNS-1941-4.cisco.com
Key storage device: private config

CA Certificate
(...omitted...)
```

헤드엔드 컨피그레이션

헤드엔드 컨피그레이션은 다음 두 부분으로 구성됩니다. PKI 부품 및 실제 flex/IKEv2입니다.

PKI 컨피그레이션

bsns-1941-4.cisco.com의 CN이 사용된다는 것을 알 수 있습니다. 이 항목은 적절한 DNS 항목과 일치해야 하며 <Hostname>의 AnyConnect 프로필에 포함되어야 합니다.

```
crypto pki trustpoint CISCO2
enrollment url http://10.48.66.14:80
serial-number
ip-address 10.48.66.15
subject-name cn=bsns-1941-4.cisco.com,ou=TAC,o=cisco
revocation-check none

crypto pki certificate map CMAP 10
subject-name co cisco
```

Crypto/IPsec 컨피그레이션

제안서의 PRF/무결성 설정은 인증서가 지원하는 것과 일치해야 **합니다**. 일반적으로 SHA-1입니다.

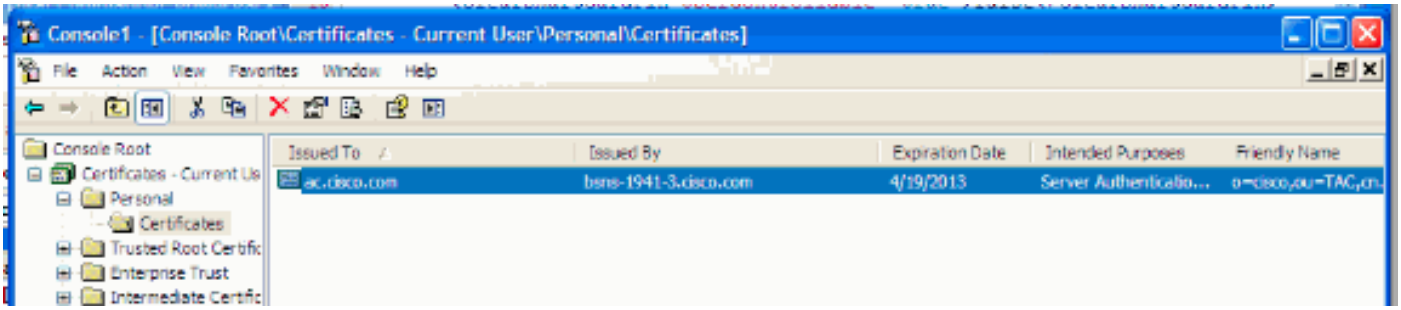
```
crypto ikev2 authorization policy AC
pool AC

crypto ikev2 proposal PRO
encryption 3des aes-cbc-128
integrity sha1
group 5 2

crypto ikev2 policy POL
match fvrf any
proposal PRO

crypto ikev2 profile PRO
match certificate CMAP
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint CISCO2
aaa authorization group cert list default AC
virtual-template 1

no crypto ikev2 http-url cert
crypto ipsec transform-set TRA esp-3des esp-sha-hmac

crypto ipsec profile PRO
set transform-set TRA
set ikev2-profile PRO

interface Virtual-Template1 type tunnel
ip unnumbered GigabitEthernet0/0
tunnel mode ipsec ipv4 tunnel protection ipsec profile PRO
```

클라이언트

IKEv2 및 인증서와의 성공적인 AnyConnect 연결을 위한 클라이언트 컨피그레이션은 두 부분으로 구성됩니다.

인증서 등록

인증서가 올바르게 등록되면 시스템 또는 개인 저장소에 있는지 확인할 수 있습니다. 클라이언트 인증서에는 EKU도 있어야 합니다.



AnyConnect 프로파일

AnyConnect 프로파일은 길고 매우 기본적입니다.

관련 부품은 다음을 정의합니다.

1. 연결하는 호스트
2. 프로토콜 유형
3. 해당 호스트에 연결할 때 사용할 인증

사용 항목:

```
<ServerList>
<HostEntry>
<HostName>bsns-1941-4.cisco.com</HostName>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>
IKE-RSA
</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

AnyConnect의 연결 필드에서 `<HostName>`에 표시된 값인 전체 FQDN을 제공해야 합니다.

연결 확인

간결함에 대해서는 일부 정보가 생략되어 있다.

```
BSNS-1941-4#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA
Tunnel-id Local Remote fvrf/ivrf Status
```

```
2    10.48.66.15/4500    10.55.193.212/65311   none/none    READY
Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:5,
Auth sign: RSA, Auth verify: RSA
Life/Active Time: 86400/180 sec


IPv6 Crypto IKEv2 SA

BSNS-1941-4#show crypto ipsec sa

interface: Virtual-Access1
Crypto map tag: Virtual-Access1-head-0, local addr 10.48.66.15

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/0/0)
current_peer 10.55.193.212 port 65311
PERMIT, flags={origin_is_acl,}
#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
#pkts decaps: 26, #pkts decrypt: 26, #pkts verify: 26

local crypto endpt.: 10.48.66.15, remote crypto endpt.: 10.55.193.212
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x5C171095(1545015445)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8283D0F0(2189676784)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel UDP-Encaps, }
conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000040,
crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4215478/3412)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound esp sas:
spi: 0x5C171095(1545015445)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel UDP-Encaps, }
conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000040,
crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4215482/3412)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

차세대 암호화

위 컨피그레이션은 최소 작업 컨피그레이션을 표시하기 위한 참조 자료로 제공됩니다. 가능하면 NGC(Next Generation Cryptography)를 사용하는 것이 좋습니다.

마이그레이션에 대한 현재 권장 사항은 여기에서 확인할 수 있습니다.
http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

NGC 컨피그레이션을 선택할 때 클라이언트 소프트웨어와 헤드엔드 하드웨어 모두 이를 지원하는지 확인합니다. ISR 2세대 및 ASR 1000 라우터는 NGC에 대한 하드웨어 지원 때문에 헤드엔드로 권장됩니다.

AnyConnect에서는 AnyConnect 3.1 버전부터 NSA의 Suite B 알고리즘 제품군이 지원됩니다.

알려진 주의 사항 및 문제

- IOS 헤드엔드에 이 라인을 구성해야 합니다. **crypto ikev2 http-url cert가 없습니다**. IOS 및 AnyConnect에서 이 설정이 구성되어 있지 않을 때 발생하는 오류는 매우 잘못된 것입니다.
- IKEv2 세션이 포함된 초기 IOS 15.2M&T 소프트웨어가 RSA-SIG 인증에 적합하지 않을 수 있습니다. 이는 Cisco 버그 ID CSCtx31294와 관련될 수 있습니다(등록된 고객만 해당). 최신 152M 또는 15.2T 소프트웨어를 실행해야 합니다.
- 특정 시나리오에서 IOS는 인증할 올바른 신뢰 지점을 선택하지 못할 수 있습니다. Cisco는 이 문제를 인식하고 있으며 15.2(3)T1 및 15.2(4)M1 릴리스부터 수정되었습니다.
- AnyConnect에서 다음과 유사한 메시지를 보고하는 경우:

```
The client certificate's cryptographic service provider(CSP)
does not support the sha512 algorithm
```

그런 다음 IKEv2 제안서의 무결성/PRF 설정이 인증서가 처리할 수 있는 것과 일치하는지 확인해야 합니다. 위의 컨피그레이션 예에서는 SHA-1이 사용됩니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems