目次

概要

このドキュメントでは、FlexVPN フレームワークを使用した証明書認証のみがある Cisco IOS® ルータに、AnyConnect クライアントを実行するデバイスから IPSec で保護された接続を実現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。

- FlexVPN
- AnyConnect

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くものです。

ヘッドエンド

Cisco IOS ルータは、少なくとも 15.2 M&T リリースを実行している IKEv2 を実行できるルータであれば問題ありません。 ただし、可能であれば新しいリリース (「既知の警告」の項を参照) を使用する必要があります。

クライアント

AnyConnect 3.x リリース

認証局

この例では、認証局 (CA) は 15.2(3)T リリースを実行しています。

拡張キー使用法 (EKU) をサポートする必要があるため、より新しいリリースを使用することが重要です。

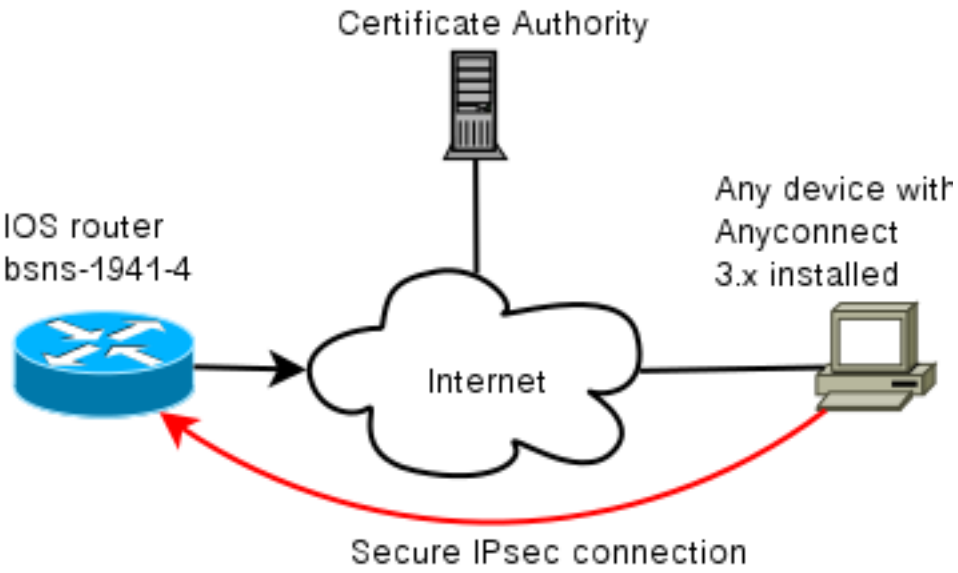
この導入では、IOS ルータは CA として使用されます。 ただし、EKU を使用できる標準規格に基づく CA アプリケーションであれば問題ありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

ネットワーク トポロジ



認証局 (任意)

使用することを選択した場合、IOS ルータは CA として機能できます。

IOS CA の設定

CA サーバはクライアントおよびサーバの証明書に正しい EKU を使用する必要があることを忘れないでください。 この場合、サーバ認証およびクライアント認証 EKU がすべての証明書用に設定されています。

```
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
```

証明書に設定された EKU が正しいかどうかを確認する方法

bsns-1941-3 は CA サーバ、bsns-1941-4 は IPSec ヘッドエンドであることに注意してください。 出力の一部は、簡略化のために省略されています。

```
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...)
```

ヘッドエンド設定

ヘッドエンド設定は、次の 2 つの部分で構成されています。 PKI 部品と実際の flex/IKEv2。

PKI の設定

bsns-1941-4.cisco.com の CN が使用されています。 これは適切な DNS エントリと一致し、AnyConnect のプロファイルの <Hostname> の下に含める必要があります。

```
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 の設定

プロポーザルの PRF/integrity の設定が証明書でサポートされる設定と一致する**必要がある**ことに注意してください。 通常、これは SHA-1 です。

```
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
```

クライアント

IKEv2 および証明書を使用して正常に AnyConnect に接続するクライアントの設定は、次の 2 つの部分から構成されます。

証明書の登録

証明書が正常に登録されると、マシンまたは個人ストアにあることを確認できます。 クライアント証明書にも、EKU が必要なことを忘れないでください。

AnyConnect プロファイル

AnyConnect プロファイルは、非常に長く基本的なプロファイルです。

関連する部分は、次を定義することです。

1. 接続先のホスト
2. プロトコルのタイプ
3. そのホストに接続する場合に使用する認証

使用される情報：

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

AnyConnect の接続フィールドで完全な FQDN を入力する必要があります。これは、<HostName> に表示される値です。

接続の確認

一部の情報は簡略化のために省略されています。

```
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)
```

次世代暗号化

上の構成は、最小の動作設定を示すための参照として提供されています。 可能な場合は次世代暗号化（NGC）を使用することをお勧めします。

移行に関する最新の推奨事項は、次の場所にあります。
http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

NGC 設定を選択する場合、クライアント ソフトウェアとヘッドエンド ハードウェアの両方がこれをサポートすることを確認してください。 ハードウェアが NGC をサポートするため、ISR 世代 2 と ASR 1000 ルータがヘッドエンドとして推奨されます。

AnyConnect 3.1 バージョンの時点では、AnyConnect 側で NSA の Suite B アルゴリズム スイートがサポートされます。

既知の注意事項と問題

- IOS ヘッドエンドで次の行を必ず設定してください。 **no crypto ikev2 http-url cert**。 これが設定されていない場合に、IOS および AnyConnect によって生成されるエラーは誤解を招くものになります。
- IKEv2 セッションを使用した初期の IOS 15.2M&T ソフトウェアは、RSA-SIG 認証で起動しない場合があります。 これは、Cisco Bug ID CSCtx31294（登録ユーザ専用）に関連する可能性があります。 最新の 15.2M または 15.2T ソフトウェアが実行されていることを確認します。
- 特定のシナリオでは IOS が認証する正しいトラストポイントを選択できないことがあります。 シスコはこの問題を認識しており、この問題は 15.2(3)T1 および 15.2(4)M1 リリースで解決されています。
- AnyConnect で次のようなメッセージが報告される場合：`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)
```

IKEv2 プロポーザルの integrity/PRF の設定が、証明書が処理できる設定と一致していることを確認する必要があります。 上記の設定例では、SHA-1 が使用されています。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems