証明書認証を備えたIKEv2を使用したDMVPNフェーズ3の設定

内容

はじめに

このドキュメントでは、IKEv2を使用した証明書認証でDynamic Multipoint VPN(DMVPN)フェーズ3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。

- DMVPN に関する基礎知識.
- EIGRP に関する基礎知識.
- 公開キーインフラストラクチャ(PKI)に関する基礎知識。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Cisco IOS® バージョン17.3.8aを実行するCisco C8000v(VXE)。

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。

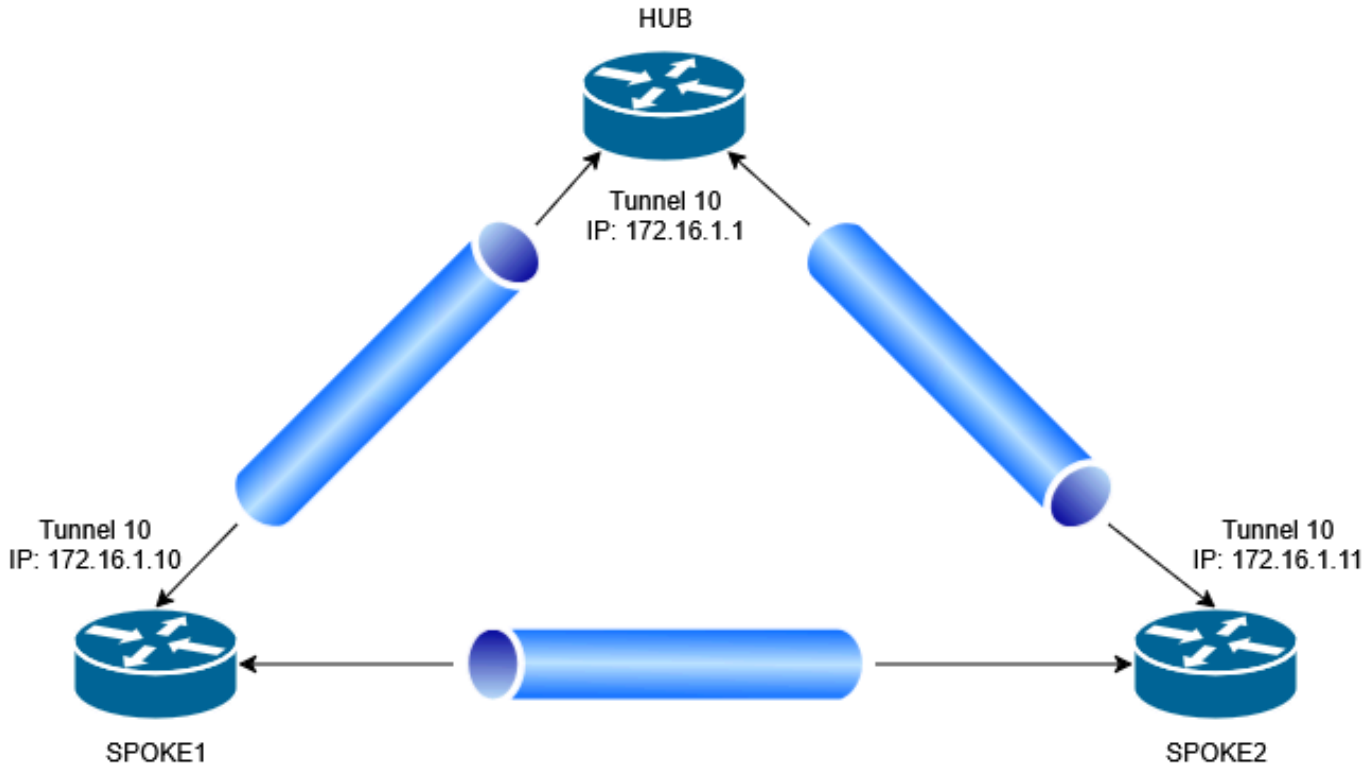
背景説明

Dynamic Multipoint VPN(DMVPN)フェーズ3では、スポーク間の直接接続が導入され、ほとんどのトラフィックパスでハブをバイパスすることにより、VPNネットワークをより効率的に運用できます。この設計では、遅延が最小限に抑えられ、リソース使用率が最適化されます。Next Hop Resolution Protocol(NHRP)を使用すると、スポークは互いを動的に識別し、直接トンネルを作成して、大規模で複雑なネットワークトポロジをサポートできます。
インターネットキーエクスチェンジバージョン2(IKEv2)は、この環境で安全なトンネルを確立するための基盤となるメカニズムを提供します。以前のプロトコルと比較すると、IKEv2は高度なセキュリティ対策を提供し、キーの再生成プロセスを高速化し、モビリティと複数接続の両方のサポートを強化します。DMVPNフェーズ3との統合により、トンネルのセットアップとキー管理が安全かつ効果的に処理されます。
ネットワークセキュリティをさらに強化するために、IKEv2はデジタル証明書認証をサポートしています。このアプローチにより、デバイスは証明書を使用して相互間のIDを検証できます。これにより、管理が簡素化され、共有秘密に関連するリスクが軽減されます。証明書ベースの信頼は、個々のキーの管理が困難な大規模な展開で特に役立ちます。
DMVPNフェーズ3、IKEv2、および証明書認証は、すべて堅牢なVPNフレームワークを提供します。このソリューションは、柔軟な接続、強力なデータ保護、および運用の合理化を実現することで、現代の企業の要件に対応します。

設定

このセクションでは、証明書ベースの認証を使用してIKEv2でDMVPNフェーズ3を設定する手順について説明します。次の手順を実行して、ハブルータとスポークルータ間のセキュアでスケーラブルなVPN接続を有効にします。

ネットワーク図



コンフィギュレーション

証明書インフラストラクチャの準備

すべてのデバイス（ハブとスポーク）に必要なデジタル証明書がインストールされていることを確認します。これらの証明書は、信頼できるCAによって発行され、各デバイスに適切に登録されて、セキュアなIKEv2証明書認証を有効にする必要があります。
ハブルータとスポークルータで証明書を登録するには、次の手順を実行します。

1. コマンドcrypto pki trustpoint <Trustpoint Name>を使用して、必要な情報でトラストポイントを設定します。

<#root>

```
Hub(config)#
```

```
crypto pki trustpoint myCertificate
```

```
Hub(ca-trustpoint)# enrollment terminal
Hub(ca-trustpoint)# ip-address 10.10.1.2
Hub(ca-trustpoint)# subject-name cn=Hub, o=cisco
Hub(ca-trustpoint)# revocation-check none
```

2. コマンドcrypto pki authenticate <Trustpoint Name>を使用して、トラストポイントを認証します。

<#root>

```
Hub(config)#
```

crypto pki authenticate myCertificate

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

注：crypto pki authenticateコマンドを発行した後で、デバイス証明書の署名に使用する認証局(CA)からの証明書を貼り付ける必要があります。この手順は、ハブルータとスポークルータの両方で証明書登録に進む前に、デバイスとCAの間で信頼を確立するために不可欠です。

---

3. コマンドcrypto pki enroll <Trustpoint Name>を使用して、秘密キーと証明書署名要求(CSR)を生成します。

<#root>

```
Hub(config)#
```

crypto pki enroll myCertificate

```
% Start certificate enrollment ..

% The subject name in the certificate will include: cn=Hub, o=cisco
% The subject name in the certificate will include: Hub
% Include the router serial number in the subject name? [yes/no]: n
% The IP address in the certificate is 10.10.1.2

Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

MIICsDCCAZgCAQAwSjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAMTA0hVQjEqMBAG
CSqGSIb3DQEJAhYDSFVCMBYGCSqGSIb3DQEJCBMJMTAuMTAuMS4yMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAo/M40+ivsqJhpF0PRUxdCGSUVgLQUhzQ
cwnuMtSbfdn5fMKIj7wO6Qa7Gvx2rjrdoyxH9JgXjTEMzMv6HP9/EuN2o+qKzR/+
CNzMUDJobb0lBNbe0WKL4IAQjbvNTOyA5iuUzHZCgMrCFG3oU7v+a2tMiSZihvdu
+m2JSDNXn5cXyewQbQsEaELAO0yosi2t6BQyzM3FRU23dCwnFVwY1VAADC7CrNh3
o44SifYW5HtWq1tU1cLTY4sjNf6XJQxjmHPudbUp164RDfUSo37Zjvjt7S8OOoLU
+XUBrE3aRDlwJ+Ug2DO31ZWzfc+rBZ1BsKWlYFBlLk3mL9RA1nf3eQIDAQABoCEw
HwYJKoZIhvcNAQkOMRIwEDAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQAD
ggEBAEKUQURWZ+YeCx9T7kuzIaDwJ53vMqq6rITDJcNF9FJ4IgJ7PsxFOcWXm7MM
O3Oi1yq1K/4X7Mb5Iz6CjtdyXVqakgcEPY7W9NoO3Xo8Nxb4pFfe19EO2Xuj8fxm
GTqi7UAw8ZslzJ2jrS7bXasVMb5jjr39cqQkrXfNIAwF1Sw6IA3oKfTelq8/iCJu
TEjFOD8Si2PWziuxJVS4Adjg5GxbJpd/tDKrKUuvqD2z4HD3M4OoGVvoBWQOtjhB
4gx1q2D2O9KOnMCvVZrOfp/PFd6+cYc57E73ZPVSGQpHIiiWCYtuRKdKArN6vRcP
iiugceU2F3Ll4CI7wXMYqCxQOGU=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
```

注：このプロセスで使用される秘密キーは、ルータによって生成されるデフォルトの秘密キーです。ただし、必要に応じて、カスタム秘密鍵の使用もサポートされています。

4. CSRの生成後、署名する認証局(CA)に送信します。

5. 証明書が署名されたら、コマンドcrypto pki import <Trustpoint Name> certificateを使用して、作成されたトラストポイントに関連付けられている署名付き証明書をインポートします。

<#root>

```
Hub(config)#
crypto pki import myCertificate certificate

% You must authenticate the Certificate Authority before
you can import the router's certificate.
```

6. CAによって署名された証明書をPEM形式で貼り付けます。

暗号化IKEv2およびIPSecの設定

Crypto IKEv2とIPSecの設定は、スポークとハブの両方で同じにすることができます。これは、トンネルが正常に確立されるように、すべてのデバイスでプロポーザルや使用される暗号などの要素が常に一致する必要があるためです。この一貫性により、DMVPNフェーズ3環境内での相互運用性とセキュアな通信が保証されます。

1. IKEv2プロポーザルを設定します。

```
crypto ikev2 proposal ikev2
encryption aes-cbc-256
integrity sha256
group 14
```

2. IKEv2プロファイルを設定します。

<#root>

```
crypto ikev2 profile ikev2Profile
match identity remote address 0.0.0.0
identity local address 10.10.1.2
authentication remote rsa-sig

authentication local rsa-sig
```

```
pki trustpoint
myCertificate
```

注：ここで、PKI証明書認証が定義され、認証に使用されるトラストポイントが定義されます。

3. IPSecプロファイルとトランスフォームセットを設定します。

```
crypto ipsec transform-set ipsec esp-aes 256 esp-sha256-hmac
mode tunnel
crypto ipsec profile ipsec
set transform-set ipsec
set ikev2-profile ikev2Profile
```

トンネルの設定

このセクションでは、ハブとスポークの両方のトンネルの設定について、特にDMVPNセットアップのフェーズ3に焦点を当てて説明します。

1. ハブトンネル設定。

```
interface Tunnel10
ip address 172.16.1.1 255.255.255.0
no ip redirects
no ip split-horizon eigrp 10
ip nhrp authentication cisco123
ip nhrp network-id 10
ip nhrp redirect
tunnel source GigabitEthernet1
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

2. Spoke1トンネル設定。

```
interface Tunnel10
ip address 172.16.1.10 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp map 172.16.1.1 10.10.1.2
ip nhrp map multicast 10.10.1.2
ip nhrp network-id 10
ip nhrp nhs 172.16.1.1
tunnel source GigabitEthernet2
```

```
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

3. Spoke2トンネル設定。

```
interface Tunnel10
ip address 172.16.1.11 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp map 172.16.1.1 10.10.1.2
ip nhrp map multicast 10.10.1.2
ip nhrp network-id 10
ip nhrp nhs 172.16.1.1
tunnel source GigabitEthernet3
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

確認

DMVPNフェーズ3ネットワークが正常に機能していることを確認するには、次のコマンドを使用します。

- show dmvpn interface <トンネル名>
- show crypto ikev2 sa
- show crypto ipsec sa peer <ピアIP>

show dmvpn interface <Tunnel Name>コマンドを使用すると、ハブとスポークの間のアクティブなセッションを確認できます。Spoke1の観点からは、出力はこれらの確立された接続を反映できます。

<#root>

SPOKE1#

show dmvpn interface tunnel10

```
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
T1 - Route Installed, T2 - Nexthop-override, B - BGP
C - CTS Capable, I2 - Temporary
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel10, IPv4 NHRP Details
```

```
Type:Spoke, NHRP Peers:2,

# Ent Peer NBMA Addr Peer Tunnel Add
State
 UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
   1  10.10.1.2           172.16.1.1
UP
      1w6d     S
   1  10.10.3.2          172.16.1.11
UP
  00:00:04     D
```

show crypto ikev2 saコマンドでは、スポークとハブの間に形成されたIKEv2トンネルを表示して、フェーズ1ネゴシエーションの成功を確認します。

```
<#root>
SPOKE1#
show crypto ikev2 sa

IPv4 Crypto IKEv2 SA
Tunnel-id Local            Remote             fvrf/ivrf
Status

1       10.10.2.2/500      10.10.3.2/500      none/none
READY

     Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify:
RSA

     Life/Active Time: 86400/184 sec
Tunnel-id Local            Remote             fvrf/ivrf
Status

2      10.10.2.2/500       10.10.1.2/500      none/none
READY

     Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify:
RSA
```

```
     Life/Active Time: 86400/37495 sec

IPv6 Crypto IKEv2 SA
```

show crypto ipsec sa peer <peer IP>コマンドを使用すると、スポークとハブの間に確立されたIPSecトンネルを確認でき、DMVPNネットワーク内でのセキュアなデータ転送を確保できます。

<#root>

```
SPOKE1#show

crypto ipsec sa peer 10.10.3.2



interface: Tunnel10
Crypto map tag: Tunnel10-head-0, local addr 10.10.2.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.10.2.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.10.3.2/255.255.255.255/47/0)
current_peer 10.10.3.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.10.2.2, remote crypto endpt.: 10.10.3.2
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet2
current outbound spi: 0xF341E02E(4081180718)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8ED55E26(2396347942)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2701, flow_id: CSR:701, sibling_flags FFFFFFFF80000048, crypto map: Tunnel10-head-0
sa timing: remaining key lifetime (k/sec): (4607999/3188)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF341E02E(4081180718)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2702, flow_id: CSR:702, sibling_flags FFFFFFFF80000048, crypto map: Tunnel10-head-0
sa timing: remaining key lifetime (k/sec): (4607999/3188)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:

outbound pcp sas:
```

トラブルシュート

トラブルシューティングには、次のコマンドを使用できます。

- debug dmvpn condition peer [nbma/tunnelIP]:NBMAに固有のDMVPNセッション、またはピアからのトンネルIPアドレスに関する条件付きデバッグを有効にします。これにより、ピアに関連する問題を切り分けることができます。
- debug dmvpn all all:NHRP、暗号化IKE、IPsec、トンネル保護、暗号化ソケットなど、DMVPNのすべての側面で包括的なデバッグを有効にします。過剰なデバッグ情報によってルータが過負荷状態にならないように、このコマンドは条件付きフィルタとともに使用することをお勧めします。
- show dmvpn：トンネルインターフェイス、NHRPマッピング、ピア情報を含む現在のDMVPNステータスを表示します。
- show crypto ikev2 sa:IKEv2セキュリティアソシエーションのステータスを表示します。フェーズ1 VPNネゴシエーションの確認に役立ちます。
- show crypto ipsec sa：フェーズ2のトンネルステータスとトラフィック統計情報を示すIPSecセキュリティアソシエーションを表示します。

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。