인증서 인증과 함께 IKEv2를 사용하여 DMVPN 3단계 구성

목차

소개

이 문서에서는 IKEv2를 사용하여 인증서 인증을 통해 DMVPN(Dynamic Multipoint VPN) 3단계를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음과 같은 주제에 대해 숙지할 것을 권장합니다.

- DMVPN에 대한 기본 지식
- EIGRP에 대한 기본 지식
- PKI(Public Key Infrastructure)에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco IOS® 버전 17.3.8a를 실행하는 Cisco C8000v(VXE)

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.

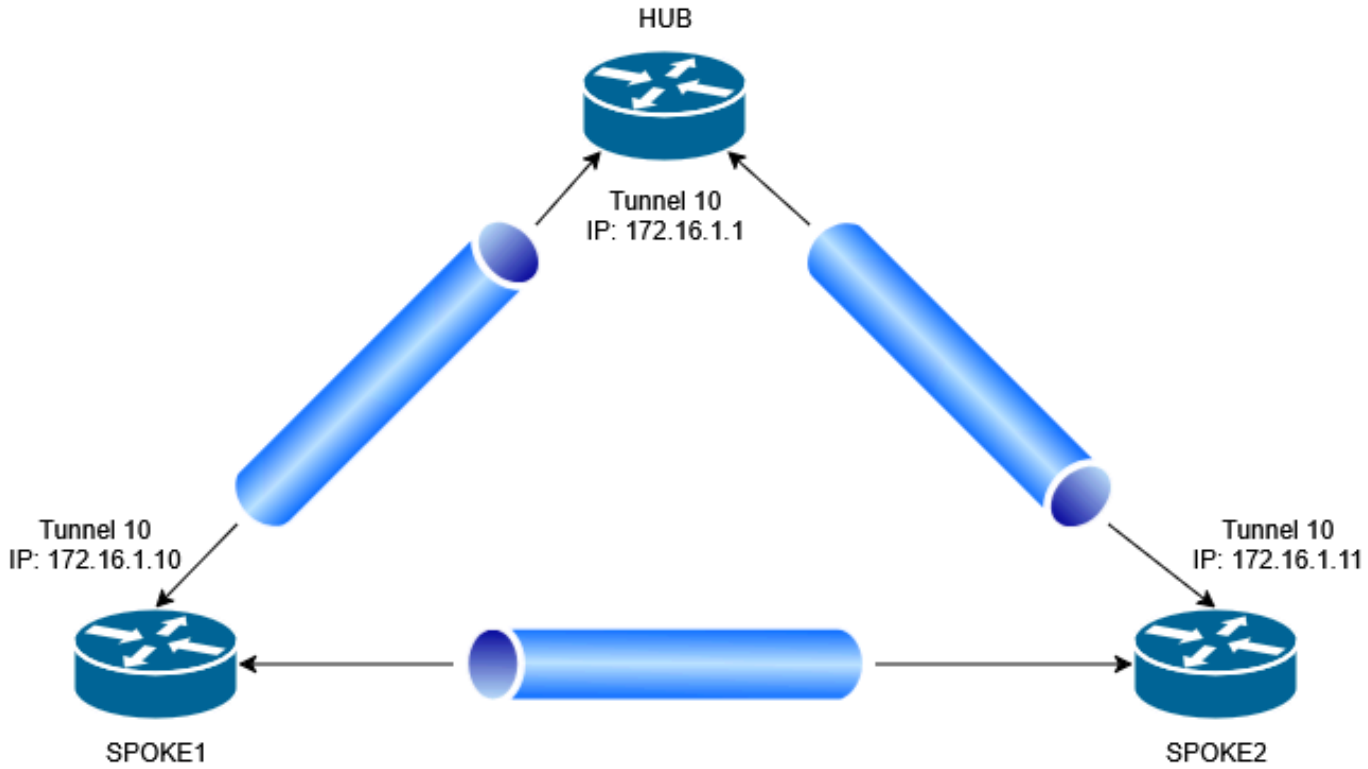
배경 정보

DMVPN(Dynamic Multipoint VPN) Phase 3에서는 직접 스포크 투 스포크(Spoke to Spoke) 연결을 도입하여 대부분의 트래픽 경로에 대해 허브를 우회하여 VPN 네트워크가 더 효율적으로 작동할 수 있게 합니다. 이 설계는 레이턴시를 최소화하고 리소스 사용률을 최적화합니다. NHRP(Next Hop Resolution Protocol)를 사용하면 스포크가 서로 동적으로 식별하고 직접 터널을 생성하여 크고 복잡한 네트워크 토폴로지를 지원할 수 있습니다.
IKEv2(Internet Key Exchange version 2)는 이 환경에서 보안 터널을 설정하기 위한 기본 메커니즘을 제공합니다. 이전 프로토콜에 비해 IKEv2는 고급 보안 조치, 더 빠른 키 재설정 프로세스, 모빌리티 및 다중 연결 모두에 대한 향상된 지원을 제공합니다. DMVPN 3단계와 통합되므로 터널 설정 및 키 관리가 안전하고 효과적으로 처리됩니다.
네트워크 보안을 더욱 강화하기 위해 IKEv2는 디지털 인증서 인증을 지원합니다. 이 접근 방식을 사용하면 디바이스에서 인증서를 사용하여 서로 간의 ID를 확인할 수 있으므로 관리가 단순해지고 공유 비밀과 관련된 위험이 줄어듭니다. 인증서 기반 신뢰는 개별 키를 관리하기가 어려운 대규모 구축에서 특히 유용합니다.
DMVPN Phase 3, IKEv2 및 인증서 인증은 모두 강력한 VPN 프레임워크를 제공합니다. 이 솔루션은 유연한 연결, 강력한 데이터 보호, 간소화된 운영을 보장함으로써 현대 기업의 요구 사항을 해결합니다.

구성

이 섹션에서는 인증서 기반 인증을 사용하여 IKEv2를 사용하는 DMVPN Phase 3을 구성하는 단계별 지침을 제공합니다. 허브 라우터와 스포크 라우터 간에 안전하고 확장 가능한 VPN 연결을 활성화하려면 다음 단계를 완료하십시오.

네트워크 다이어그램



설정

인증서 인프라 준비

모든 디바이스(허브 및 스포크)에 필요한 디지털 인증서가 설치되어 있는지 확인합니다. 보안 IKEv2 인증서 인증을 활성화하려면 이러한 인증서를 신뢰할 수 있는 CA에서 발급하고 각 디바이스에 올바르게 등록해야 합니다.
허브 및 스포크 라우터에 인증서를 등록하는 절차는 다음과 같습니다.

1. crypto pki trustpoint <Trustpoint Name> 명령을 사용하여 필요한 정보로 신뢰 지점을 구성합니다.

<#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. crypto pki authenticate <Trustpoint Name> 명령을 사용하여 신뢰 지점을 인증합니다.

<#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
```

참고: crypto pki authenticate 명령을 실행한 후 디바이스 인증서 서명에 사용되는 CA(Certificate Authority)의 인증서를 붙여넣어야 합니다. 이 단계는 허브와 스포크 라우터 모두에서 인증서 등록을 진행하기 전에 디바이스와 CA 간에 신뢰를 설정하는 데 필수적입니다.

3. crypto pki enroll <Trustpoint Name> 명령을 사용하여 개인 키 및 CSR(Certificate Signing Request)을 생성합니다.

<#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/M4O+ivsqJhpFOPRUxdCGSUVgLQUhzQ
cwnuMtSbfdn5fMKIj7wO6Qa7Gvx2rjrdoyxH9JgXjTEMzMv6HP9/EuN2o+qKzR/+
CNzMUDJobbOlBNbeOWKL4IAQjbvNTOyA5iuUzHZCgMrCFG3oU7v+a2tMiSZihvdu
+m2JSDNXn5cXyewQbQsEaELAOOyosi2t6BQyzM3FRU23dCwnFVwY1VAADC7CrNh3
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]:
```

참고: 이 프로세스 중에 사용되는 개인 키는 라우터가 생성하는 기본 개인 키입니다. 그러나

필요한 경우 사용자 지정 개인 키 사용도 지원됩니다.

4. CSR을 생성한 후 서명할 CA(Certificate Authority)에 보냅니다.

5. 인증서가 서명되면 crypto pki import <Trustpoint Name> certificate 명령을 사용하여 생성된 신뢰 지점과 연결된 서명된 인증서를 가져옵니다.

<#root>

```
Hub(config)#
```

crypto pki import myCertificate certificate

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

6. CA에서 서명한 인증서를 PEM 형식으로 붙여넣습니다.

Crypto IKEv2 및 IPSec 컨피그레이션

Crypto IKEv2 및 IPSec의 컨피그레이션은 스포크와 허브 모두에서 동일할 수 있습니다. 이는 터널이 성공적으로 설정될 수 있도록 모든 디바이스에서 사용되는 제안서 및 암호와 같은 요소가 항상 일치해야 하기 때문입니다. 이러한 일관성은 DMVPN 3단계 환경 내에서 상호 운용성과 보안 통신을 보장합니다.

1. IKEv2 제안서를 구성합니다.

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

2. IKEv2 프로필을 구성합니다.

<#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
```

참고: 여기서 PKI 인증서 인증이 정의되며 인증에 사용되는 신뢰 지점입니다.

3. IPSec 프로필 및 변형 집합을 구성합니다.

```
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
```

터널 컨피그레이션

이 섹션에서는 허브 및 스포크 모두에 대한 터널 컨피그레이션을 다룹니다. 특히 DMVPN 설정의 3단계에 초점을 맞춥니다.

1. 허브 터널 구성

```
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 터널 구성

```
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 터널 구성

```
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
```

다음을 확인합니다.

DMVPN 3단계 네트워크가 올바르게 작동하는지 확인하려면 다음 명령을 사용합니다.

- show dmvpn interface <터널 이름>
- show crypto ikev2 sa
- show crypto ipsec sa peer <peer IP>

show dmvpn interface <Tunnel Name> 명령을 사용하면 허브와 스포크 간의 활성 세션을 볼 수 있습니다. Spoke1의 관점에서 출력에는 이러한 설정된 연결이 반영될 수 있습니다.

<#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 명령은 스포크와 허브 사이에 형성된 IKEv2 터널을 표시하여 1단계 협상이 성공했음을 확인합니다.

```
<#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> 명령을 사용하여 스포크와 허브 간에 설정된 IPSec 터널을 확인하여 DMVPN 네트워크 내에서 안전한 데이터 전송을 보장할 수 있습니다.

<#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:
```

문제 해결

문제 해결을 위해 다음 명령을 사용할 수 있습니다.

- debug dmvpn condition peer [nbma/tunnelIP] - 피어의 NBMA 또는 터널 IP 주소에 해당하는 DMVPN 세션에 대한 조건부 디버깅을 활성화하여 해당 피어와 관련된 문제를 격리합니다.
- debug dmvpn all(모두 디버그)을 사용하면 NHRP, 암호화 IKE, IPsec, 터널 보호 및 암호화 소켓을 비롯한 DMVPN의 모든 측면에 대해 포괄적인 디버깅을 수행할 수 있습니다. 과도한 디버그 정보로 라우터를 압도하지 않으려면 조건부 필터와 함께 이 명령을 사용하는 것이 좋습니다.
- show dmvpn, 터널 인터페이스, NHRP 매핑 및 피어 정보를 비롯한 현재 DMVPN 상태를 표시합니다.
- show crypto ikev2 sa, 1단계 VPN 협상 확인에 유용한 IKEv2 보안 연결의 상태를 표시합니다.
- show crypto ipsec sa, Displays IPsec Security Associations, show phase 2 tunnel status and traffic statistics.

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.