Configurazione di DMVPN fase 3 con IKEv2 con autenticazione certificato

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Premesse
- Configurazione
  - Esempio di rete
  - Configurazioni
    - Prepara infrastruttura certificati
    - Configurazione di Crypto IKEv2 e IPSec
    - Configurazione tunnel
- Verifica
- Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare la fase 3 di Dynamic Multipoint VPN (DMVPN) con l'autenticazione dei certificati tramite IKEv2.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di DMVPN.
- Conoscenze base dell'EIGRP.
- Conoscenze base dell'infrastruttura a chiave pubblica (PKI).

Componenti usati

Le informazioni di questo documento si basano sulla seguente versione del software:

- Cisco C800v (VXE) con Cisco IOS® versione 17.3.8a.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

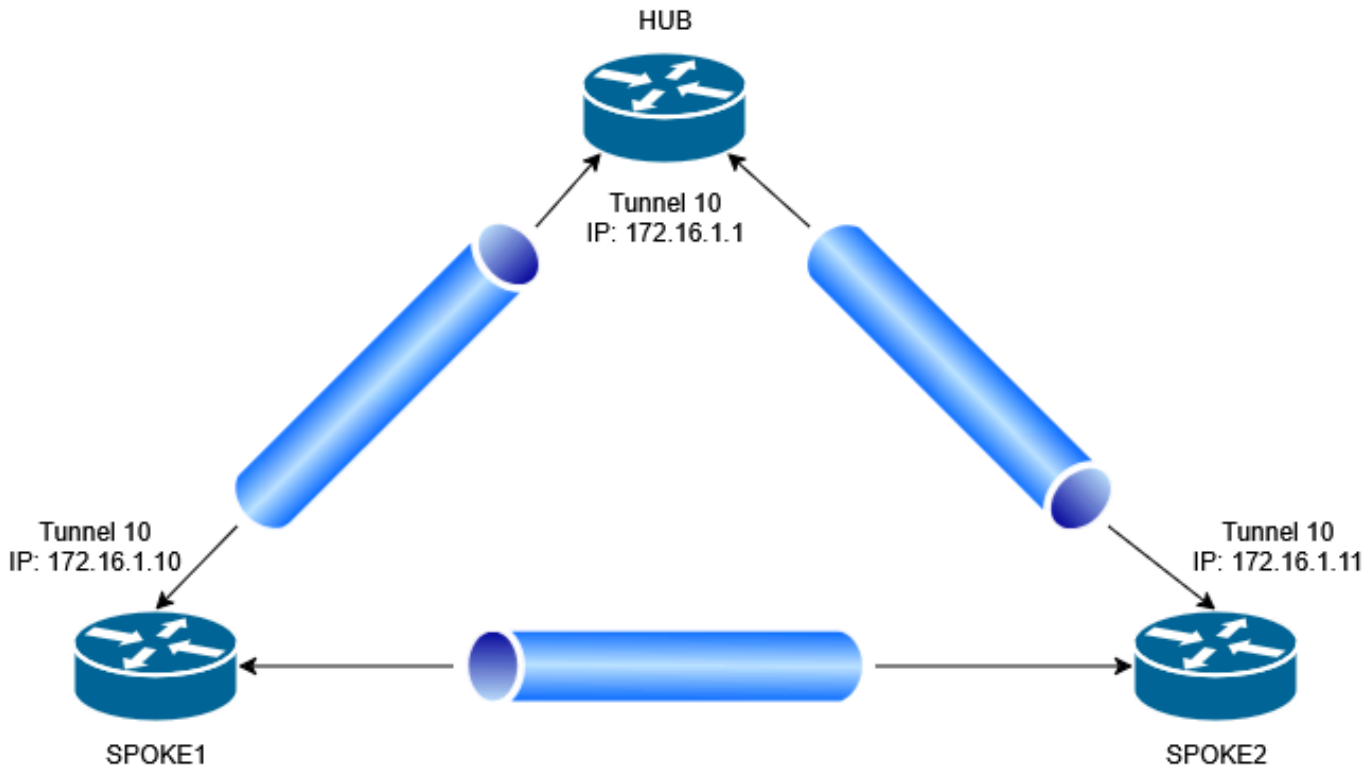
Premesse

La fase 3 della VPN dinamica multipunto (DMVPN) introduce la connettività diretta Spoke to Spoke, che consente alle reti VPN di funzionare in modo più efficiente ignorando l'hub per la maggior parte dei percorsi di traffico. Questa struttura riduce al minimo la latenza e ottimizza l'utilizzo delle risorse. L'utilizzo del protocollo NHRP (Next Hop Resolution Protocol) consente agli spoke di identificarsi in modo dinamico e creare tunnel diretti, supportando topologie di rete complesse e di grandi dimensioni.
IKEv2 (Internet Key Exchange versione 2) rappresenta il meccanismo sottostante per la creazione di tunnel sicuri in questo ambiente. Rispetto ai protocolli precedenti, IKEv2 offre misure di sicurezza avanzate, processi di rigenerazione delle chiavi più rapidi e supporto avanzato per la mobilità e le connessioni multiple. L'integrazione con DMVPN fase 3 garantisce una gestione sicura ed efficace della configurazione del tunnel e della gestione delle chiavi.
Per rafforzare ulteriormente la sicurezza della rete, IKEv2 supporta l'autenticazione digitale dei certificati. Questo approccio consente ai dispositivi di verificare le identità tra loro utilizzando i certificati, semplificando la gestione e riducendo i rischi associati ai segreti condivisi. L'attendibilità basata su certificati è particolarmente vantaggiosa in implementazioni estese in cui la gestione di singole chiavi potrebbe risultare difficoltosa.
Complessivamente, DMVPN Fase 3, IKEv2 e l'autenticazione dei certificati forniscono un solido framework VPN. Questa soluzione soddisfa i requisiti delle aziende moderne garantendo connettività flessibile, protezione dei dati e operazioni semplificate.

Configurazione

In questa sezione vengono fornite istruzioni dettagliate per configurare DMVPN Fase 3 con IKEv2 utilizzando l'autenticazione basata su certificati. Completare questi passaggi per abilitare la connettività VPN sicura e scalabile tra router Hub e Spoke.

Esempio di rete



Configurazioni

Prepara infrastruttura certificati

Verificare che in tutti i dispositivi (hub e spoke) siano installati i certificati digitali necessari. Per abilitare l'autenticazione sicura dei certificati IKEv2, questi certificati devono essere emessi da una CA attendibile e devono essere registrati correttamente in ogni dispositivo.
Per registrare un certificato su router Hub e Spoke, attenersi alla seguente procedura:

1. Configurare un trust point con le informazioni richieste utilizzando il comando crypto pki trustpoint <Nome trust point>.

<#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. Autenticare il trust point utilizzando il comando crypto pki authenticate <nome trust point>.

<#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
```

Nota: dopo aver eseguito il comando crypto pki authentication, è necessario incollare il certificato dall'autorità di certificazione (CA) utilizzato per firmare i certificati del dispositivo. Questo passaggio è essenziale per stabilire un'attendibilità tra il dispositivo e la CA prima di procedere con la registrazione dei certificati su router Hub e Spoke.

---

3. Generare la chiave privata e la richiesta di firma del certificato (CSR) utilizzando il comando crypto pki enroll **<nome trust point>**.

<#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]:
```

Nota: La chiave privata utilizzata durante questo processo è la chiave privata predefinita generata dal router. Tuttavia, se necessario, è supportato anche l'utilizzo di chiavi private personalizzate.

4. Dopo aver generato il CSR, inviarlo all'Autorità di certificazione (CA) per la firma.

5. Dopo aver firmato il certificato, utilizzare il comando crypto pki import <nome trust point> per importare il certificato firmato associato al trust point creato.

<#root>

```
Hub(config)#
```

crypto pki import myCertificate certificate

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

6. Incollare il certificato firmato dalla CA in formato PEM.

Configurazione di Crypto IKEv2 e IPSec

La configurazione di Crypto IKEv2 e IPSec può essere la stessa su entrambi gli spoke e sull'hub. Infatti, per garantire la corretta connessione del tunnel, è necessario che elementi come le proposte e le cifrature utilizzate corrispondano sempre tra tutti i dispositivi. Questa coerenza garantisce interoperabilità e comunicazioni sicure all'interno dell'ambiente DMVPN fase 3.

1. Configurare una proposta IKEv2.

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

2. Configurare un profilo IKEv2.

<#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
```

Nota: In questa sezione vengono definiti l'autenticazione del certificato PKI e il trust point utilizzato per l'autenticazione.

3. Configurare un profilo IPSec e un set di trasformazioni.

```
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
```

Configurazione tunnel

Questa sezione descrive la configurazione dei tunnel per Hub e Spoke, in particolare per la fase 3 della configurazione di DMVPN.

1. Configurazione del tunnel hub.

```
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. Configurazione tunnel Spoke1.

```
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. Configurazione tunnel Spoke2.

```
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
```

Verifica

Per verificare che la rete DMVPN fase 3 funzioni correttamente, utilizzare questi comandi:

- show dmvpn interface <Nome tunnel>
- show crypto ikev2 sa
- show crypto ipsec sa peer <IP peer>

Il comando show dmvpn interface <Tunnel Name> permette di visualizzare le sessioni attive tra l'hub e gli spoke. Dal punto di vista di Spoke1, l'output può riflettere queste connessioni stabilite.

<#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
```

Il comando show crypto ikev2 sa visualizza i tunnel IKEv2 formati tra gli spoke e l'hub, a conferma dell'esito positivo delle negoziazioni della fase 1.

```
<#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
```

Utilizzando il comando show crypto ipsec sa peer <IP peer>, è possibile verificare i tunnel IPSec stabiliti tra gli spoke e l'hub, assicurando il trasporto sicuro dei dati all'interno della rete DMVPN.

<#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:
```

Risoluzione dei problemi

Per la risoluzione dei problemi, è possibile utilizzare i seguenti comandi:

- debug dmvpn condition peer [nbma/tunnelIP], abilita il debug condizionale per le sessioni DMVPN specifiche di un indirizzo IP del tunnel o NBMA da un peer, semplificando l'isolamento dei problemi correlati a tale peer.
- debug dmvpn all, consente il debug completo per tutti gli aspetti di DMVPN, inclusi NHRP, crypto IKE, IPsec, protezione del tunnel e socket di crittografia. Si consiglia di utilizzare questo comando con un filtro condizionale per evitare di sovraccaricare il router con informazioni di debug eccessive.
- show dmvpn, visualizza lo stato corrente di DMVPN, incluse le interfacce tunnel, i mapping NHRP e le informazioni peer.
- show crypto ikev2 sa, visualizza lo stato delle associazioni di sicurezza IKEv2, utile per verificare le negoziazioni VPN della fase 1.
- show crypto ipsec sa, visualizza le associazioni di sicurezza IPsec, mostrando lo stato del tunnel per la fase 2 e le statistiche del traffico.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).