DMVPN Fase 3 configureren met IKEv2 met certificaatverificatie

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Achtergrondinformatie

Configureren

- Netwerkdiagram
- Configuraties
  - Certificaatinfrastructuur voorbereiden
  - Crypto IKEv2- en IPSec-configuratie
  - tunnelconfiguratie

Verifiëren

Problemen oplossen

Inleiding

In dit document wordt informatie beschreven over het configureren van fase 3 van Dynamic Multipoint VPN (DMVPN) met certificaatverificatie met IKEv2.

Voorwaarden

Vereisten

Cisco raadt aan om kennis te hebben van de onderwerpen:

- Kennis van DMVPN.
- Basiskennis van EIGRP.
- Basiskennis van Public Key Infrastructure (PKI).

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversie:

- Cisco C8000v (VXE) met Cisco IOS® versie 17.3.8a.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

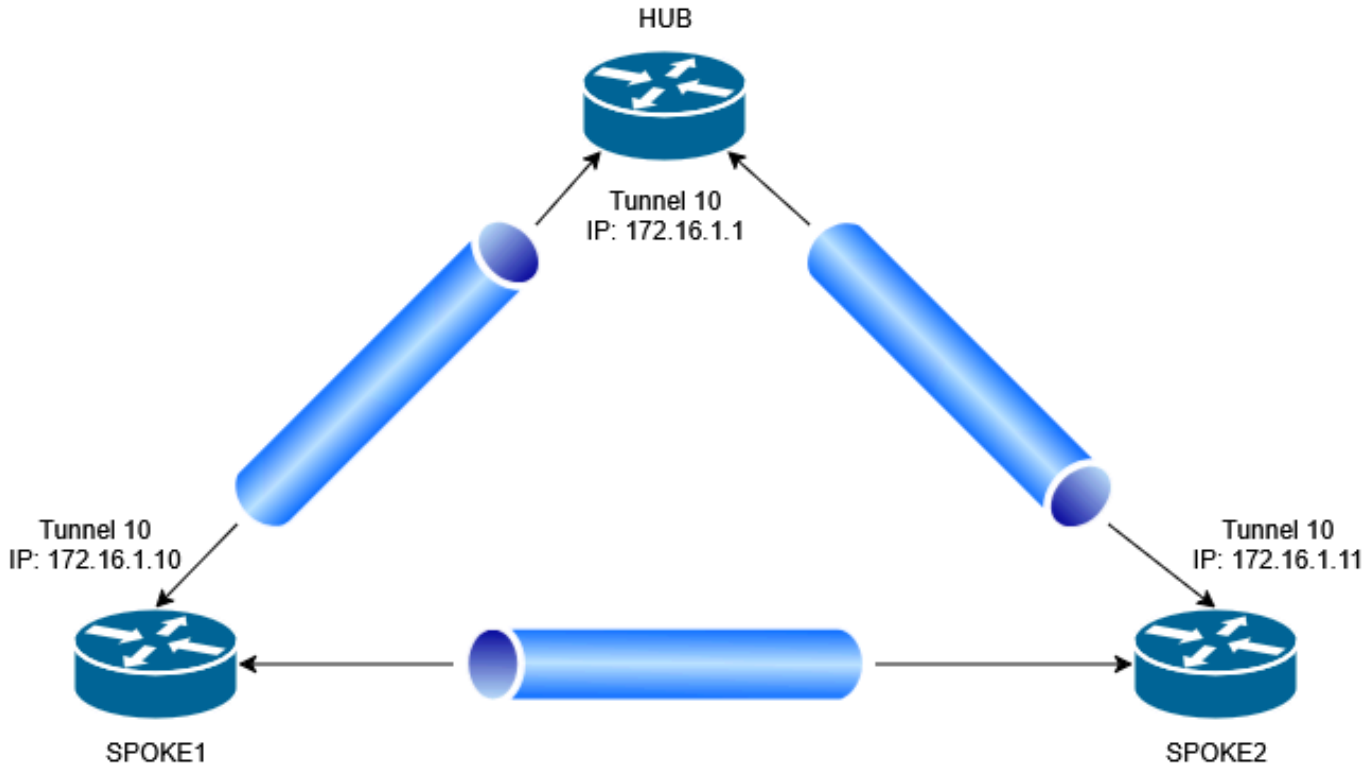
Achtergrondinformatie

Dynamic Multipoint VPN (DMVPN) Fase 3 introduceert directe Spoke to Spoke-connectiviteit, waardoor VPN-netwerken efficiënter kunnen werken door de Hub voor de meeste verkeerspaden te omzeilen. Dit ontwerp minimaliseert de latentie en optimaliseert het gebruik van bronnen. Het gebruik van het Next Hop Resolution Protocol (NHRP) stelt sprekers in staat om elkaar dynamisch te identificeren en directe tunnels te creëren, die grote en complexe netwerktopologieën ondersteunen.
Internet Key Exchange versie 2 (IKEv2) biedt het onderliggende mechanisme voor het opzetten van beveiligde tunnels in deze omgeving. In vergelijking met eerdere protocollen biedt IKEv2 geavanceerde beveiligingsmaatregelen, snellere rekeying-processen en verbeterde ondersteuning voor zowel mobiliteit als meerdere verbindingen. De integratie met DMVPN Fase 3 zorgt ervoor dat tunnelinstallatie en sleutelbeheer veilig en effectief worden afgehandeld.
Om de netwerkbeveiliging verder te versterken, ondersteunt IKEv2 digitale certificaatverificatie. Met deze aanpak kunnen apparaten elkaars identiteit verifiëren met behulp van certificaten, wat het beheer vereenvoudigt en de risico's in verband met gedeelde geheimen vermindert. Vertrouwen op basis van certificaten is vooral nuttig bij uitgebreide implementaties waarbij het beheren van individuele sleutels een uitdaging zou zijn.
Alles bij elkaar bieden DMVPN Fase 3, IKEv2 en certificaatverificatie een robuust VPN-framework. Deze oplossing voldoet aan de eisen van moderne bedrijven door te zorgen voor flexibele connectiviteit, sterke bescherming van gegevens en gestroomlijnde activiteiten.

Configureren

Deze sectie bevat stapsgewijze instructies voor het configureren van DMVPN Fase 3 met IKEv2 met behulp van op certificaten gebaseerde verificatie. Voer deze stappen uit om veilige en schaalbare VPN-connectiviteit tussen Hub- en Spoke-routers mogelijk te maken.

Netwerkdiagram



Configuraties

Certificaatinfrastructuur voorbereiden

Zorg ervoor dat alle apparaten (Hubs en Spokes) de nodige digitale certificaten hebben geïnstalleerd. Deze certificaten moeten worden uitgegeven door een vertrouwde certificeringsinstantie en op de juiste wijze zijn geregistreerd op elk apparaat om een veilige IKEv2-certificaatverificatie mogelijk te maken.
Voer de volgende stappen uit om een certificaat in te schrijven voor Hub- en Spoke-routers:

1. Configureer een trustpoint met de vereiste informatie met behulp van de opdracht crypto pki trustpoint <Trustpoint Name>.

<#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. Authenticeer het trustpoint met de opdracht crypto pki authenticate <Trustpoint Name>.

<#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
```

Opmerking: Nadat u de opdracht crypto pki authenticate hebt uitgegeven, moet u het certificaat van Certificate Authority (CA) plakken dat wordt gebruikt om de apparaatcertificaten te ondertekenen. Deze stap is essentieel om vertrouwen te creëren tussen het apparaat en de CA voordat u doorgaat met certificaatregistratie op zowel Hub- als Spoke-routers.

---

3. Genereer de privésleutel en het certificaatondertekeningsverzoek (CSR) met behulp van de opdracht crypto pki enroll <Trustpoint Name>.

<#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
o44SifYW5HtWq1tU1cLTY4sjNf6XJQxjmHPudbUp164RDfUSo37Zjvjt7S80OoLU
+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]:
```

Opmerking: De privésleutel die tijdens dit proces wordt gebruikt, is de standaardprivésleutel die door de router wordt gegenereerd. Het gebruik van aangepaste privésleutels wordt echter ook ondersteund, indien nodig.

4. Na het genereren van de CSR, stuurt u deze naar de te ondertekenen certificeringsinstantie (CA).

5. Nadat het certificaat is ondertekend, gebruikt u de opdracht crypto pki import <Trustpoint Name> certificaat om het ondertekende certificaat te importeren dat is gekoppeld aan het aangemaakte trustpoint.

<#root>

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


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

6. Plak het door de bevoegde autoriteit ondertekende certificaat in PEM-formaat.

Crypto IKEv2- en IPSec-configuratie

De configuratie voor Crypto IKEv2 en IPSec kan hetzelfde zijn op zowel de spaken als de Hub. Dit komt omdat elementen zoals de voorstellen en de gebruikte cijfers altijd moeten overeenkomen met alle apparaten om ervoor te zorgen dat de tunnel met succes kan worden vastgesteld. Deze consistentie garandeert interoperabiliteit en veilige communicatie binnen de DMVPN fase 3-omgeving.

1. Configureer een IKEv2-voorstel.

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

2. Configureer een IKEv2-profiel.

<#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
```

Opmerking: hier is waar PKI-certificaatverificatie is gedefinieerd en het vertrouwenspunt dat wordt gebruikt voor verificatie.

---

3. Configureer een IPSec-profiel en een transformatieset.

```
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
```

tunnelconfiguratie

Dit gedeelte behandelt de configuratie van tunnels voor zowel de Hub als de Spokes, met speciale aandacht voor fase 3 van de DMVPN-installatie.

1. Hub tunnelconfiguratie.

```
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 tunnelconfiguratie.

```
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-tunnelconfiguratie.

```
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
```

Verifiëren

Om te bevestigen dat het DMVPN Fase 3-netwerk correct functioneert, gebruikt u de volgende opdrachten:

- dmvpn-interface <tunnelnaam> weergeven
- Crypto IKEV2 SA weergeven
- crypto ipsec sa peer <peer IP> weergeven

Met de opdracht show dmvpn interface <Tunnel Name> ziet u de actieve sessies tussen de Hub en de spaken. Vanuit het perspectief van Spoke1 kan de output deze gevestigde verbindingen weerspiegelen.

<#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
```

De show crypto ikev2 sa opdracht toont de IKEv2 tunnels gevormd tussen de spaken en de Hub, bevestiging van succesvolle Fase 1 onderhandelingen.

<#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

Met de opdracht show crypto ipsec sa peer <peer IP> kunt u de IPSec-tunnels tussen de spaken en de Hub verifiëren, waardoor veilig gegevenstransport binnen het DMVPN-netwerk wordt gewaarborgd.

<#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:
```

Problemen oplossen

Voor het oplossen van problemen kunt u de volgende opdrachten gebruiken:

- debug dmvpn condition peer [nbma/tunnelIP], maakt voorwaardelijke debugging mogelijk voor DMVPN-sessies die specifiek zijn voor een NBMA- of tunnel-IP-adres van een peer, waardoor problemen met betrekking tot die peer kunnen worden geïsoleerd.
- debug dmvpn all, maakt uitgebreide debugging mogelijk voor alle aspecten van DMVPN, waaronder NHRP, crypto IKE, IPsec, tunnelbescherming en crypto-sockets. Het wordt aanbevolen om deze opdracht te gebruiken met een voorwaardelijk filter om te voorkomen dat de router wordt overweldigd door overmatige foutopsporingsinformatie.
- toont dmvpn, geeft de huidige DMVPN-status weer, inclusief tunnelinterfaces, NHRP-toewijzingen en peer-informatie.
- toon crypto ikev2 sa, Toont de status van IKEv2 Security Associations, handig voor het verifiëren van Fase 1 VPN-onderhandelingen.
- toont crypto ipsec sa, geeft IPsec Security Associations weer, toont fase 2 tunnelstatus en verkeersstatistieken.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.