Configuration de DMVPN phase 3 à l'aide d'IKEv2 avec authentification par certificat

Table des matières

Introduction

Ce document décrit les informations sur la façon de configurer le VPN multipoint dynamique (DMVPN) phase 3 avec l'authentification de certificat à l'aide d'IKEv2.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Connaissances de base de DMVPN.
- Connaissances de base du protocole EIGRP.
- Connaissance de base de l'infrastructure à clé publique (ICP).

Composants utilisés

L'information contenue dans le présent document est fondée sur cette version logicielle:

- Cisco C8000v (VXE) exécutant Cisco IOS® Version 17.3.8a.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

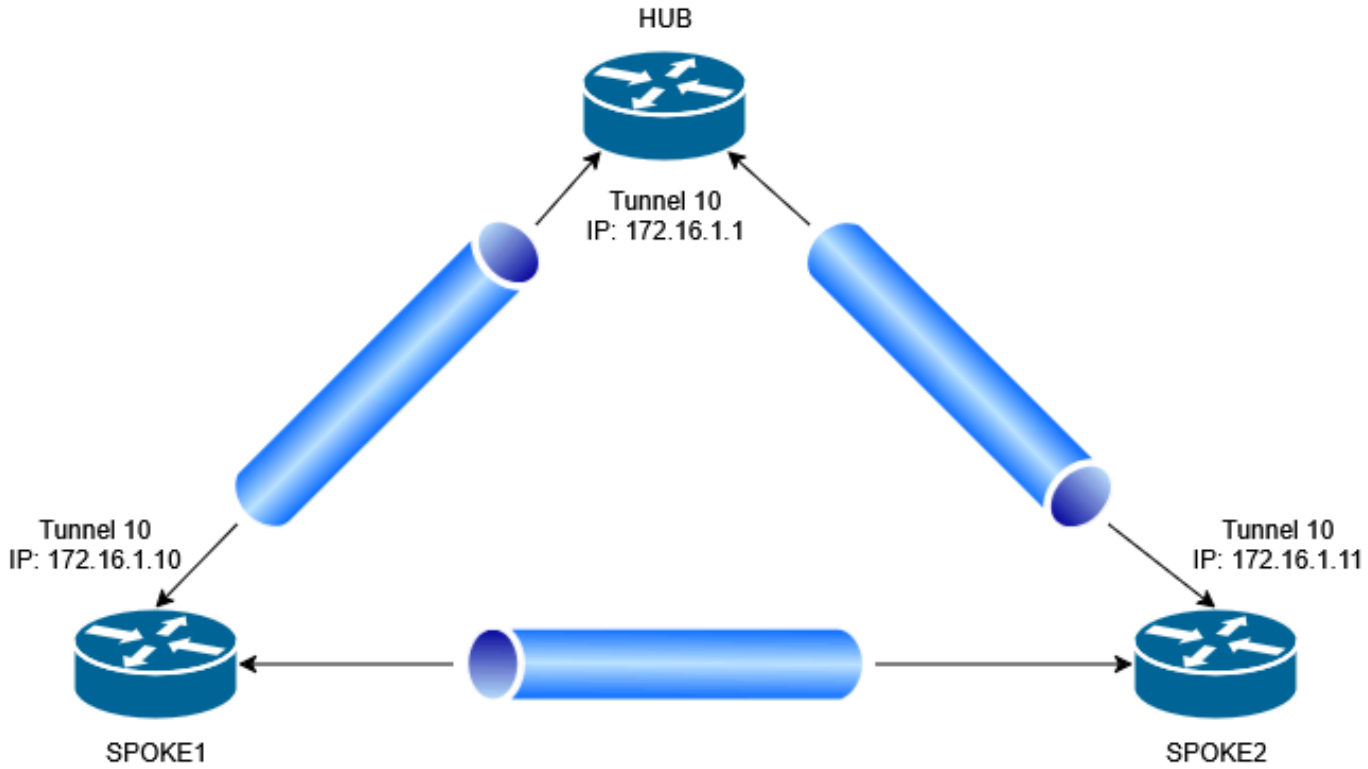
Informations générales

DMVPN (Dynamic Multipoint VPN) Phase 3 introduit la connectivité satellite à satellite directe, permettant aux réseaux VPN de fonctionner plus efficacement en contournant le concentrateur pour la plupart des chemins de trafic. Cette conception réduit la latence et optimise l'utilisation des ressources. L'utilisation du protocole NHRP (Next Hop Resolution Protocol) permet aux rayons de s'identifier dynamiquement les uns les autres et de créer des tunnels directs, prenant en charge des topologies de réseau complexes et de grande taille.
Internet Key Exchange version 2 (IKEv2) fournit le mécanisme sous-jacent pour établir des tunnels sécurisés dans cet environnement. Par rapport aux protocoles précédents, IKEv2 offre des mesures de sécurité avancées, des processus de réinitialisation plus rapides et une prise en charge améliorée de la mobilité et des connexions multiples. Son intégration avec DMVPN Phase 3 garantit que la configuration du tunnel et la gestion des clés sont gérées de manière sécurisée et efficace.
Pour renforcer encore la sécurité du réseau, IKEv2 prend en charge l'authentification par certificat numérique. Cette approche permet aux périphériques de vérifier les identités entre eux à l'aide de certificats, ce qui simplifie la gestion et réduit les risques associés aux secrets partagés. La confiance basée sur les certificats est particulièrement utile dans les déploiements étendus où la gestion des clés individuelles serait difficile.
Dans l'ensemble, DMVPN Phase 3, IKEv2 et l'authentification de certificat fournissent un cadre VPN robuste. Cette solution répond aux besoins des entreprises modernes en garantissant une connectivité flexible, une protection renforcée des données et une rationalisation des opérations.

Configurer

Cette section fournit des instructions pas à pas pour configurer DMVPN Phase 3 avec IKEv2 à l'aide de l'authentification basée sur certificat. Suivez ces étapes pour activer une connectivité VPN sécurisée et évolutive entre les routeurs Hub et Spoke.

Diagramme du réseau



Configurations

Préparer l'infrastructure de certificat

Assurez-vous que tous les périphériques (concentrateurs et satellites) disposent des certificats numériques nécessaires. Ces certificats doivent être émis par une autorité de certification approuvée et correctement inscrits sur chaque périphérique pour permettre l'authentification sécurisée des certificats IKEv2.
Pour inscrire un certificat sur les routeurs Hub and Spoke, procédez comme suit :

1. Configurez un point de confiance avec les informations requises à l'aide de la commande crypto pki trustpoint <Nom du point de confiance>.

<#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. Authentifiez le point de confiance à l'aide de la commande crypto pki authenticate <Nom du point de confiance>.

<#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
```

Remarque : après avoir exécuté la commande crypto pki authenticate, vous devez coller le certificat de l'autorité de certification (CA) qui est utilisée pour signer les certificats du périphérique. Cette étape est essentielle pour établir la confiance entre le périphérique et l'autorité de certification avant de procéder à l'inscription des certificats sur les routeurs Hub et Spoke.

---

3. Générez la clé privée et la demande de signature de certificat (CSR) à l'aide de la commande crypto pki enroll <Nom du point de confiance>.

<#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+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]:
```

Remarque : La clé privée utilisée au cours de ce processus est la clé privée par défaut générée par le routeur. Toutefois, l'utilisation de clés privées personnalisées est également prise en charge, si nécessaire.

4. Après avoir généré le CSR, envoyez-le à l’autorité de certification (AC) à signer.

5. Une fois le certificat signé, utilisez la commande crypto pki import <Nom du point de confiance> certificate pour importer le certificat signé associé au point de confiance créé.

<#root>

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


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

6. Collez le certificat signé par l’autorité de certification au format PEM.

Crypto IKEv2 et configuration IPSec

La configuration de Crypto IKEv2 et IPSec peut être identique sur les rayons et le concentrateur. En effet, des éléments tels que les propositions et les chiffres utilisés doivent toujours correspondre sur tous les périphériques pour garantir que le tunnel peut être établi avec succès. Cette cohérence garantit l'interopérabilité et la sécurité des communications dans l'environnement DMVPN Phase 3.

1. Configurez une proposition IKEv2.

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

2. Configurez un profil 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
```

Remarque : C'est ici que l'authentification de certificat PKI est définie et que le point de confiance est utilisé pour l'authentification.

3. Configurez un profil IPSec et un jeu de transformation.

```
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
```

Configuration du tunnel

Cette section traite de la configuration des tunnels pour le concentrateur et les rayons, en se concentrant plus particulièrement sur la phase 3 de la configuration DMVPN.

1. Configuration du tunnel de concentrateur.

```
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. Configuration du 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. Configuration du 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
```

Vérifier

Pour vérifier que le réseau DMVPN Phase 3 fonctionne correctement, utilisez ces commandes :

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

Avec la commande show dmvpn interface <Tunnel Name>, vous pouvez voir les sessions actives entre le concentrateur et les rayons. Du point de vue de Spoke1, le résultat peut refléter ces connexions établies.

<#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
```

La commande show crypto ikev2 sa affiche les tunnels IKEv2 formés entre les rayons et le concentrateur, confirmant ainsi la réussite des négociations de Phase 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
```

À l'aide de la commande show crypto ipsec sa peer <peer IP>, vous pouvez vérifier les tunnels IPSec établis entre les rayons et le concentrateur, assurant ainsi un transport de données sécurisé au sein du réseau 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:
```

Dépannage

Pour le dépannage, vous pouvez utiliser ces commandes :

- debug dmvpn condition peer [nbma/tunnelIP], active le débogage conditionnel pour les sessions DMVPN spécifiques à une adresse IP NBMA ou de tunnel d'un homologue, aidant à isoler les problèmes liés à cet homologue.
- debug dmvpn all all, permet un débogage complet pour tous les aspects de DMVPN, y compris NHRP, crypto IKE, IPsec, la protection de tunnel et les sockets de chiffrement. Il est recommandé d'utiliser cette commande avec un filtre conditionnel pour éviter de saturer le routeur avec des informations de débogage excessives.
- show dmvpn, Affiche l'état DMVPN actuel, y compris les interfaces de tunnel, les mappages NHRP et les informations d'homologue.
- show crypto ikev2 sa, Montre l'état des associations de sécurité IKEv2, utile pour vérifier les négociations VPN de Phase 1.
- show crypto ipsec sa, Affiche les associations de sécurité IPsec, montrant l'état du tunnel de Phase 2 et les statistiques de trafic.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.