Configuración de la fase 3 de DMVPN mediante IKEv2 con autenticación de certificados

Contenido

Introducción

Este documento describe la información sobre cómo configurar Dynamic Multipoint VPN (DMVPN) phase 3 con autenticación de certificados mediante IKEv2.

Prerequisites

Requirements

Cisco recomienda tener conocimiento de los temas:

- Conocimientos básicos de DMVPN.
- Conocimientos básicos de EIGRP.
- Conocimiento básico de la infraestructura de clave pública (PKI).

Componentes Utilizados

La información de este documento se basa en esta versión del software:

- Cisco C8000v (VXE) con Cisco IOS® versión 17.3.8a.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

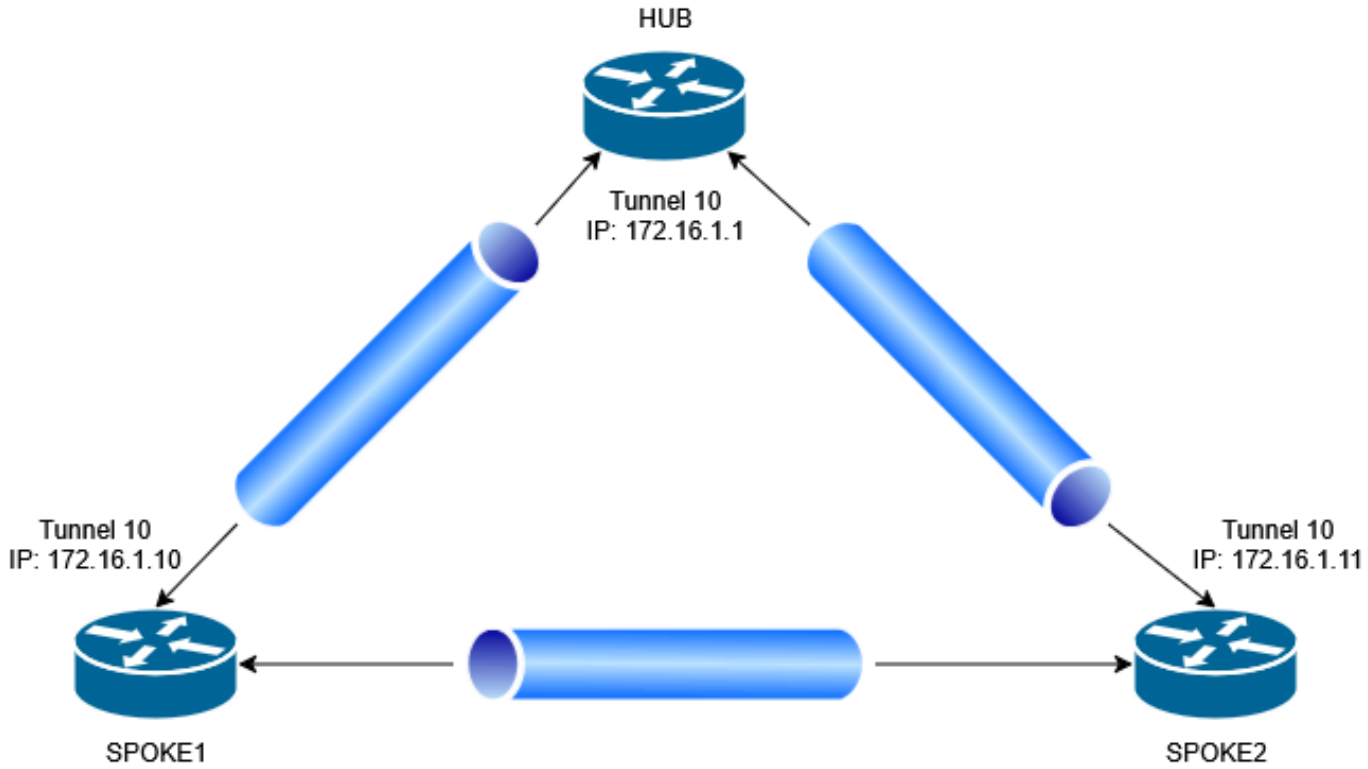
Antecedentes

La fase 3 de la VPN multipunto dinámica (DMVPN) introduce la conectividad directa de radio a radio, lo que permite que las redes VPN funcionen de forma más eficaz al omitir el concentrador para la mayoría de las rutas de tráfico. Este diseño minimiza la latencia y optimiza la utilización de los recursos. El uso del protocolo de resolución de próximo salto (NHRP) permite que los radios se identifiquen entre sí de forma dinámica y creen túneles directos, lo que admite topologías de red complejas y de gran tamaño.
Intercambio de claves de Internet versión 2 (IKEv2) proporciona el mecanismo subyacente para establecer túneles seguros en este entorno. En comparación con los protocolos anteriores, IKEv2 ofrece medidas de seguridad avanzadas, procesos de regeneración de claves más rápidos y compatibilidad mejorada tanto para la movilidad como para conexiones múltiples. Su integración con DMVPN Phase 3 garantiza que la configuración del túnel y la gestión de claves se gestionan de forma segura y eficaz.
Para reforzar aún más la seguridad de la red, IKEv2 admite la autenticación de certificados digitales. Este enfoque permite a los dispositivos verificar las identidades entre sí mediante certificados, lo que simplifica la gestión y reduce los riesgos asociados a los secretos compartidos. La confianza basada en certificados resulta especialmente beneficiosa en implementaciones expansivas en las que la gestión de claves individuales sería un reto.
En conjunto, la fase 3 de DMVPN, IKEv2 y la autenticación de certificados ofrecen un marco de VPN sólido. Esta solución satisface los requisitos de las empresas modernas al garantizar una conectividad flexible, una sólida protección de los datos y operaciones simplificadas.

Configurar

Esta sección proporciona instrucciones paso a paso para configurar la fase 3 de DMVPN con IKEv2 mediante la autenticación basada en certificados. Complete estos pasos para habilitar la conectividad VPN segura y escalable entre los routers Hub y Spoke.

Diagrama de la red



Configuraciones

Preparar infraestructura de certificados

Asegúrese de que todos los dispositivos (concentradores y radios) tienen instalados los certificados digitales necesarios. Estos certificados deben ser emitidos por una CA de confianza e inscritos correctamente en cada dispositivo para habilitar la autenticación de certificados IKEv2 seguros.
Para inscribir un certificado en los routers de concentrador y radio, siga estos pasos:

1. Configure un punto de confianza con la información requerida mediante el comando crypto pki trustpoint <Nombre del punto de confianza>.

<#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. Autentique el punto de confianza mediante el comando crypto pki authenticate <nombre de punto de confianza>.

<#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: Después de ejecutar el comando crypto pki authenticate, debe pegar el certificado de la Autoridad de Certificación (CA) que se utiliza para firmar los certificados de dispositivo. Este paso es esencial para establecer la confianza entre el dispositivo y la CA antes de continuar con la inscripción de certificados en los routers Hub y Spoke.

---

3. Genere la clave privada y la Solicitud de firma de certificado (CSR) mediante el comando crypto pki enroll <Nombre de punto de confianza>.

<#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]:
```

Nota: La clave privada utilizada durante este proceso es la clave privada predeterminada generada por el router. Sin embargo, también se admite el uso de claves privadas personalizadas, si es necesario.

4. Después de generar el CSR, envíelo a la autoridad certificadora (CA) que se firmará.

5. Una vez firmado el certificado, utilice el comando crypto pki import <nombre de punto de confianza> para importar el certificado firmado asociado con el punto de confianza creado.

<#root>

```
Hub(config)#
```

crypto pki import myCertificate certificate

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

6. Pegue el certificado firmado por la CA en formato PEM.

Configuración de IKEv2 e IPSec criptográfica

La configuración para Crypto IKEv2 e IPSec puede ser la misma tanto en los radios como en el concentrador. Esto se debe a que elementos como las propuestas y los cifrados utilizados deben coincidir siempre en todos los dispositivos para garantizar que el túnel se pueda establecer correctamente. Esta coherencia garantiza la interoperabilidad y la comunicación segura en el entorno DMVPN de fase 3.

1. Configure una propuesta IKEv2.

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

2. Configure un perfil 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: Aquí es donde se define la autenticación del certificado PKI y el punto de confianza que se utiliza para la autenticación.

3. Configure un perfil IPSec y un conjunto de transformación.

```
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
```

Configuración del túnel

Esta sección trata sobre la configuración de túneles tanto para el hub como para los radios, centrándose específicamente en la fase 3 de la configuración de DMVPN.

1. Configuración del túnel del 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. Configuración del túnel 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. Configuración del túnel 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
```

Verificación

Para confirmar que la red DMVPN de fase 3 funciona correctamente, utilice estos comandos:

- show dmvpn interface <Tunnel Name>
- show crypto ikev2 sa
- show crypto ipsec sa peer <peer IP>

Con el comando show dmvpn interface <Tunnel Name>, puede ver las sesiones activas entre el concentrador y los radios. Desde la perspectiva de Spoke1, el resultado puede reflejar estas conexiones establecidas.

<#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
```

El comando show crypto ikev2 sa muestra los túneles IKEv2 formados entre los spokes y el Hub, confirmando negociaciones exitosas de la 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
```

Con el comando show crypto ipsec sa peer <peer IP>, puede verificar los túneles IPSec establecidos entre los radios y el concentrador, asegurando el transporte seguro de datos dentro de la red 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:
```

Troubleshoot

Para la resolución de problemas, puede utilizar estos comandos:

- debug dmvpn condition peer [nbma/tunnelIP], permite la depuración condicional para sesiones DMVPN específicas de una dirección IP de túnel o NBMA desde un peer, lo que ayuda a aislar los problemas relacionados con ese peer.
- debug dmvpn all all, permite la depuración completa de todos los aspectos de DMVPN, incluidos NHRP, IKE criptográfico, IPsec, protección de túneles y sockets criptográficos. Se recomienda utilizar este comando con un filtro condicional para evitar sobrecargar el router con información de depuración excesiva.
- show dmvpn, Muestra el estado actual de DMVPN, incluidas las interfaces de túnel, las asignaciones NHRP y la información de peer.
- show crypto ikev2 sa, Muestra el estado de las Asociaciones de Seguridad IKEv2, útil para verificar las negociaciones de la Fase 1 de VPN.
- show crypto ipsec sa, Muestra Asociaciones de Seguridad IPSec, mostrando el estado del túnel de Fase 2 y las estadísticas de tráfico.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).