Konfigurieren von DMVPN Phase 3 mithilfe von IKEv2 mit Zertifikatauthentifizierung

Inhalt

Einleitung

In diesem Dokument werden Informationen zur Konfiguration von Dynamic Multipoint VPN (DMVPN) Phase 3 mit Zertifikatsauthentifizierung unter Verwendung von IKEv2 beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit den folgenden Themen vertraut zu machen:

- Grundkenntnisse von DMVPN
- Grundkenntnisse des EIGRP.
- Grundkenntnisse der Public Key Infrastructure (PKI).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der folgenden Softwareversion:

- Cisco C8000v (VXE) mit Cisco IOS® Version 17.3.8a

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

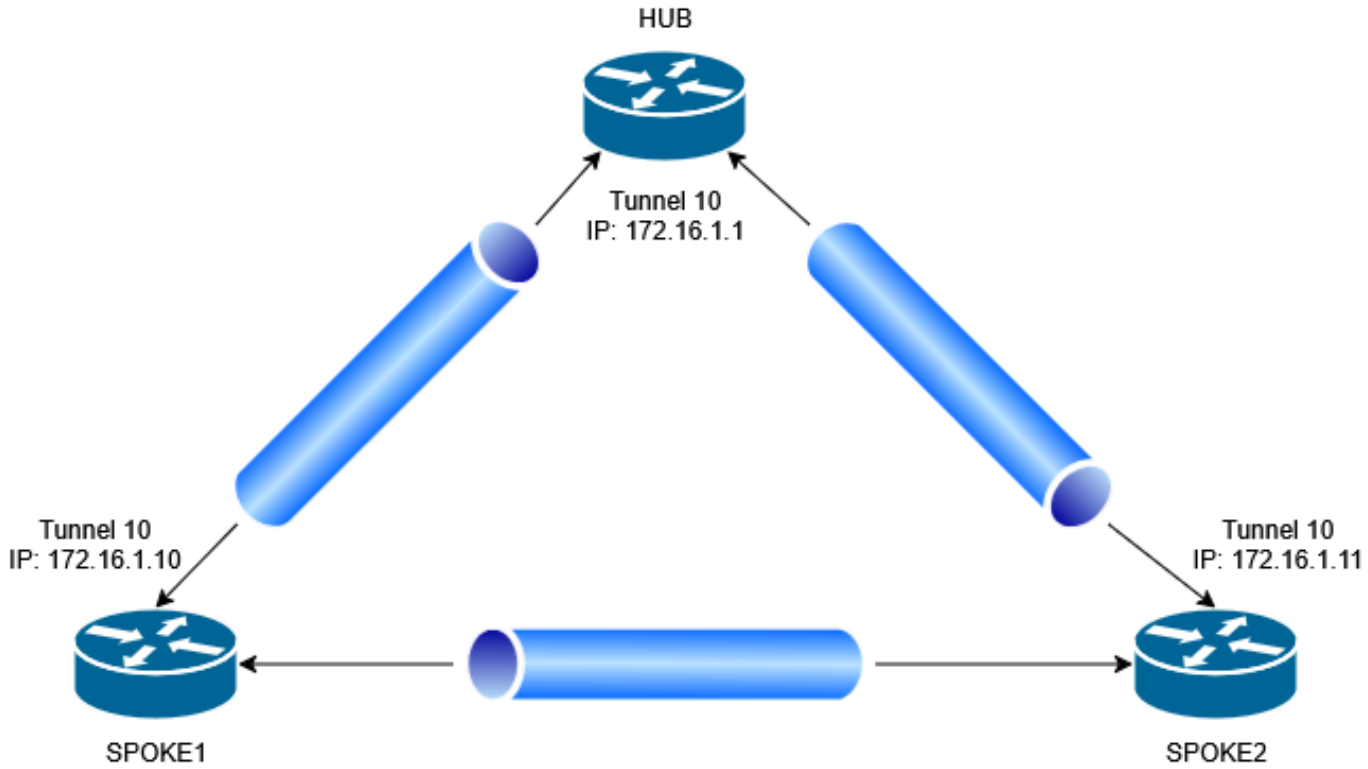
Hintergrundinformationen

Dynamic Multipoint VPN (DMVPN) Phase 3 führt die direkte Verbindung zwischen Spoke und Spoke ein, sodass VPN-Netzwerke effizienter arbeiten können, indem der Hub für die meisten Datenverkehrspfade umgangen wird. Dieses Design minimiert Latenz und optimiert die Ressourcenauslastung. Mithilfe des Next Hop Resolution Protocol (NHRP) können sich Stationen dynamisch identifizieren und direkte Tunnel erstellen. Dadurch werden große und komplexe Netzwerktopologien unterstützt.
Internet Key Exchange Version 2 (IKEv2) stellt den zugrunde liegenden Mechanismus zum Einrichten sicherer Tunnel in dieser Umgebung bereit. Im Vergleich zu früheren Protokollen bietet IKEv2 erweiterte Sicherheitsmaßnahmen, schnellere Neueingaben und verbesserte Unterstützung für Mobilität und mehrere Verbindungen. Durch die Integration mit DMVPN Phase 3 werden Tunneleinrichtung und Schlüsselmanagement sicher und effektiv durchgeführt.
Zur weiteren Verbesserung der Netzwerksicherheit unterstützt IKEv2 die digitale Zertifikatsauthentifizierung. Dieser Ansatz ermöglicht es Geräten, anhand von Zertifikaten Identitäten untereinander zu überprüfen. Dies vereinfacht die Verwaltung und reduziert die Risiken, die mit gemeinsam genutzten Geheimnissen verbunden sind. Zertifikatsbasierte Vertrauensstellung ist besonders in umfangreichen Bereitstellungen hilfreich, in denen die Verwaltung einzelner Schlüssel eine Herausforderung darstellt.
Insgesamt bilden DMVPN Phase 3, IKEv2 und die Zertifikatsauthentifizierung ein robustes VPN-Framework. Diese Lösung erfüllt die Anforderungen moderner Unternehmen, indem sie eine flexible Konnektivität, einen starken Schutz von Daten und optimierte Betriebsabläufe gewährleistet.

Konfigurieren

In diesem Abschnitt finden Sie schrittweise Anleitungen für die Konfiguration von DMVPN Phase 3 mit IKEv2 mithilfe der zertifikatbasierten Authentifizierung. Führen Sie diese Schritte aus, um sichere und skalierbare VPN-Verbindungen zwischen Hub-and-Spoke-Routern zu ermöglichen.

Netzwerkdiagramm



Konfigurationen

Vorbereiten der Zertifikatsinfrastruktur

Stellen Sie sicher, dass alle Geräte (Hubs und Spokes) über die erforderlichen digitalen Zertifikate verfügen. Diese Zertifikate müssen von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt und auf jedem Gerät ordnungsgemäß registriert werden, um eine sichere IKEv2-Zertifikatauthentifizierung zu ermöglichen.
Gehen Sie wie folgt vor, um ein Zertifikat auf Hub-and-Spoke-Routern zu registrieren:

1. Konfigurieren Sie einen Vertrauenspunkt mit den erforderlichen Informationen mithilfe des Befehls crypto pki trustpoint <Vertrauenspunktname>.

<#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. Authentifizieren Sie den Vertrauenspunkt mit dem Befehl crypto pki authentication <Vertrauenspunktname>.

<#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
```

Hinweis: Nach der Ausgabe des Befehls crypto pki Authenticate müssen Sie das Zertifikat von der Zertifizierungsstelle (Certificate Authority, CA) einfügen, das zum Signieren der Gerätezertifikate verwendet wird. Dieser Schritt ist wichtig, um die Vertrauenswürdigkeit zwischen dem Gerät und der Zertifizierungsstelle herzustellen, bevor mit der Zertifikatregistrierung auf Hub- und Spoke-Routern fortgefahren wird.

---

3. Generieren Sie den privaten Schlüssel und die Zertifikatsanforderung (Certificate Signing Request, CSR) mithilfe des Befehls 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/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]:
```

Anmerkung: Der bei diesem Vorgang verwendete private Schlüssel ist der vom Router generierte private Standardschlüssel. Die Verwendung benutzerdefinierter privater Schlüssel wird jedoch bei Bedarf ebenfalls unterstützt.

4. Nachdem Sie die CSR erstellt haben, senden Sie sie zur Signatur an die Zertifizierungsstelle (Certificate Authority, CA).

5. Sobald das Zertifikat signiert ist, verwenden Sie den Befehl crypto pki import <Trustpoint Name> certificate, um das signierte Zertifikat zu importieren, das dem erstellten Trustpoint zugeordnet ist.

<#root>

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


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

6. Fügen Sie das von der Zertifizierungsstelle signierte Zertifikat im PEM-Format ein.

Konfiguration von Krypto-IKEv2 und IPSec

Die Konfiguration für Krypto IKEv2 und IPSec kann auf den Stationen und im Hub identisch sein. Denn Elemente wie die Vorschläge und die verwendeten Chiffren müssen immer auf allen Geräten übereinstimmen, damit der Tunnel erfolgreich eingerichtet werden kann. Diese Konsistenz gewährleistet Interoperabilität und sichere Kommunikation innerhalb der DMVPN Phase 3-Umgebung.

1. Konfigurieren Sie einen IKEv2-Vorschlag.

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

2. Konfigurieren Sie ein IKEv2-Profil.

<#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
```

Anmerkung: Hier wird die PKI-Zertifikatauthentifizierung definiert, und der Vertrauenspunkt wird für die Authentifizierung verwendet.

3. Konfigurieren Sie ein IPSec-Profil und einen Transformationssatz.

```
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
```

Tunnelkonfiguration

In diesem Abschnitt wird die Konfiguration von Tunneln sowohl für den Hub als auch für die Spokes behandelt. Der Schwerpunkt liegt dabei auf Phase 3 der DMVPN-Einrichtung.

1. Konfiguration des Hub-Tunnels

```
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. Konfiguration des Spoke1-Tunnels

```
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. Konfiguration des Spoke2-Tunnels

```
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
```

Überprüfung

Verwenden Sie die folgenden Befehle, um sicherzustellen, dass das DMVPN Phase 3-Netzwerk ordnungsgemäß funktioniert:

- show dmvpn interface <Tunnelname>
- show crypto ikev2 sa
- show crypto ipsec sa peer <Peer-IP>

Mit dem Befehl show dmvpn interface <Tunnelname> können Sie die aktiven Sitzungen zwischen dem Hub und den Stationen anzeigen. Aus der Perspektive von Spoke1 kann der Ausgang diese bestehenden Verbindungen widerspiegeln.

<#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
```

Der Befehl show crypto ikev2 sa zeigt die IKEv2-Tunnel an, die zwischen den Stationen und dem Hub gebildet wurden, und bestätigt erfolgreiche Verhandlungen in 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

Mit dem Befehl show crypto ipsec sa peer <peer IP> können Sie die zwischen den Stationen und dem Hub eingerichteten IPSec-Tunnel überprüfen und so einen sicheren Datentransport innerhalb des DMVPN-Netzwerks sicherstellen.

<#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:
```

Fehlerbehebung

Zur Fehlerbehebung können Sie die folgenden Befehle verwenden:

- debug dmvpn condition peer [nbma/tunnelIP]: Ermöglicht bedingtes Debugging für DMVPN-Sitzungen, die für eine NBMA- oder Tunnel-IP-Adresse spezifisch sind, von einem Peer, sodass Probleme im Zusammenhang mit diesem Peer isoliert werden können.
- debug dmvpn all ermöglicht umfassendes Debugging für alle Aspekte von DMVPN, einschließlich NHRP, Krypto-IKE, IPsec, Tunnelschutz und Krypto-Sockets. Es wird empfohlen, diesen Befehl mit einem bedingten Filter zu verwenden, um zu vermeiden, dass der Router mit übermäßig großen Debugging-Informationen überlastet wird.
- show dmvpn: Zeigt den aktuellen DMVPN-Status an, einschließlich Tunnelschnittstellen, NHRP-Zuordnungen und Peer-Informationen.
- show crypto ikev2 sa, Zeigt den Status von IKEv2-Sicherheitszuordnungen, nützlich zur Verifizierung von Phase-1-VPN-Verhandlungen.
- show crypto ipsec sa, Zeigt IPsec-Sicherheitszuordnungen an und zeigt den Tunnelstatus und die Datenverkehrsstatistik für Phase 2 an.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.