Konfiguration von BGP über DMVPN Phase 3

Inhalt

Einleitung

In diesem Dokument werden die Konfiguration und der Betrieb von DMVPN Phase 3 mithilfe von BGP beschrieben, einschließlich der mehrschichtigen Fehlerbehebung für IPsec über DMVPN-Tunnel.

Voraussetzungen

Für die Konfigurations- und Debug-Befehle in diesem Dokument werden zwei Cisco Router benötigt, auf denen Cisco IOS® Version 15.3(3)M oder höher ausgeführt wird. Allgemein ist für eine einfache Dynamic Multipoint VPN (DMVPN) Phase 3 Cisco IOS Version 12.4(6)T erforderlich, obwohl die in diesem Dokument beschriebenen Funktionen und Fehlerbehebungen nicht vollständig unterstützt werden.

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- IKEV1/IKEV2 und IPsec
- DMVPN-Komponenten:

- Next Hop Resolution Protocol (NHRP): Erstellung einer verteilten (NHRP) Mapping-Datenbank für den gesamten Spoke-Tunnel zu realen (öffentlichen Schnittstellen) Adressen
- mGRE-Tunnelschnittstelle (Multipoint Generic Routing Encapsulation): Eine zentrale Generic Routing Encapsulation (GRE)-Schnittstelle zur Unterstützung mehrerer GRE/IPsec-Tunnel, vereinfacht die Größe und Komplexität der Konfiguration und unterstützt die dynamische Tunnelerstellung
- IPsec-Tunnelschutz: Dynamische Erstellung und Anwendung von Verschlüsselungsrichtlinien
- Routing: Dynamische Netzwerke Nahezu alle Routing-Protokolle (EIGRP (Enhanced Interior Gateway Routing Protocol), RIP (Routing Information Protocol), OSPF (Open Shortest Path First), BGP, ODR) werden unterstützt.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Cisco Aggregation Services Routern der Serie ASR 1000, Version 17.6.5 (MD).

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

Was ist DMVPN?

DMVPN ist eine Cisco IOS-Softwarelösung für den einfachen, dynamischen und skalierbaren Aufbau von IPsec+GRE-VPNs. Es ist eine Lösung zum Aufbau eines VPN-Netzwerks mit mehreren Standorten, ohne dass alle Geräte statisch konfiguriert werden müssen. Es handelt sich um ein "Hub and Spoke"-Netzwerk, bei dem die Stationen direkt miteinander kommunizieren können, ohne den Hub durchlaufen zu müssen. Die Verschlüsselung wird durch IPsec unterstützt, wodurch DMVPN eine beliebte Wahl für die Verbindung verschiedener Standorte über reguläre Internetverbindungen ist.

Wie funktioniert DMVPN?

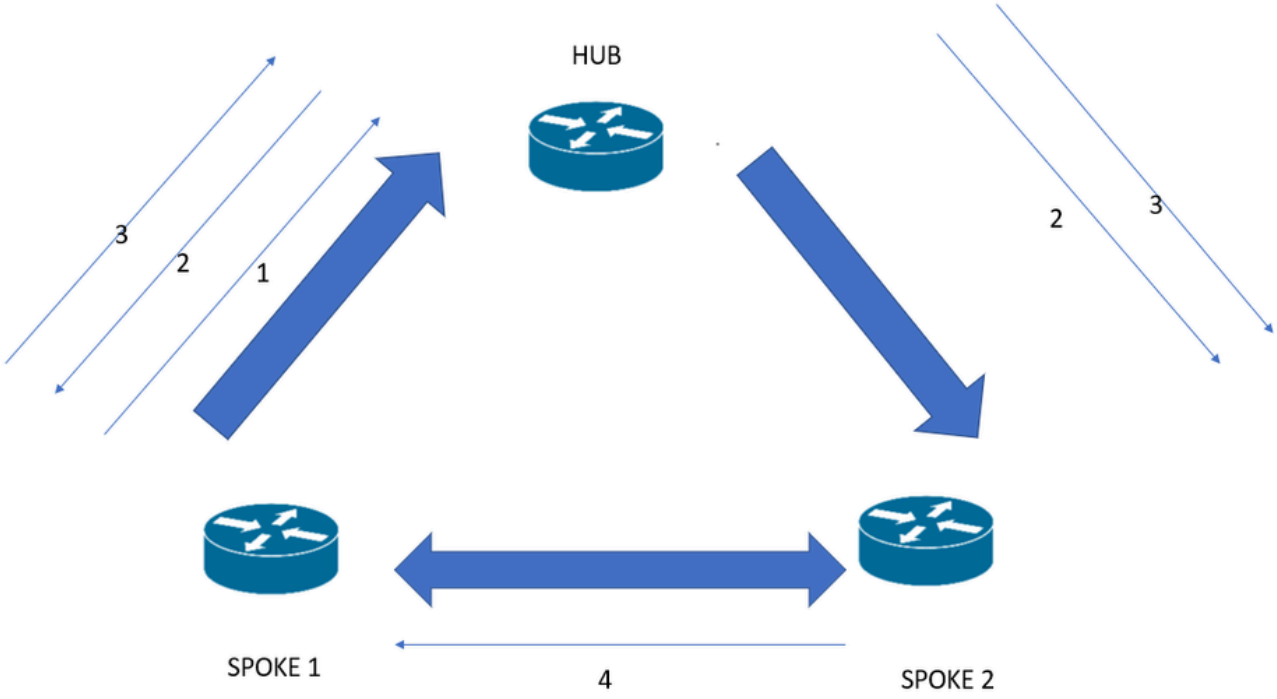
- Spokes erstellen einen dynamischen permanenten GRE/IPsec-Tunnel zum Hub, aber nicht zu anderen Stationen. Sie registrieren sich als Clients des NHRP-Servers (Hubs).
- Wenn ein Spoke ein Paket an ein (privates) Zielsubnetz hinter einem anderen Spoke senden muss, fragt er über NHRP die tatsächliche (externe) Adresse des Ziel-Spoke ab.
- Der ursprüngliche Spoke kann jetzt einen dynamischen GRE/IPsec-Tunnel zum Ziel-Spoke initiieren (da er die Peer-Adresse kennt).
- Der dynamische Spoke-to-Spoke-Tunnel wird über die mGRE-Schnittstelle aufgebaut.
- Bei Beendigung des Datenverkehrs wird der Spoke-to-Spoke-Tunnel entfernt.

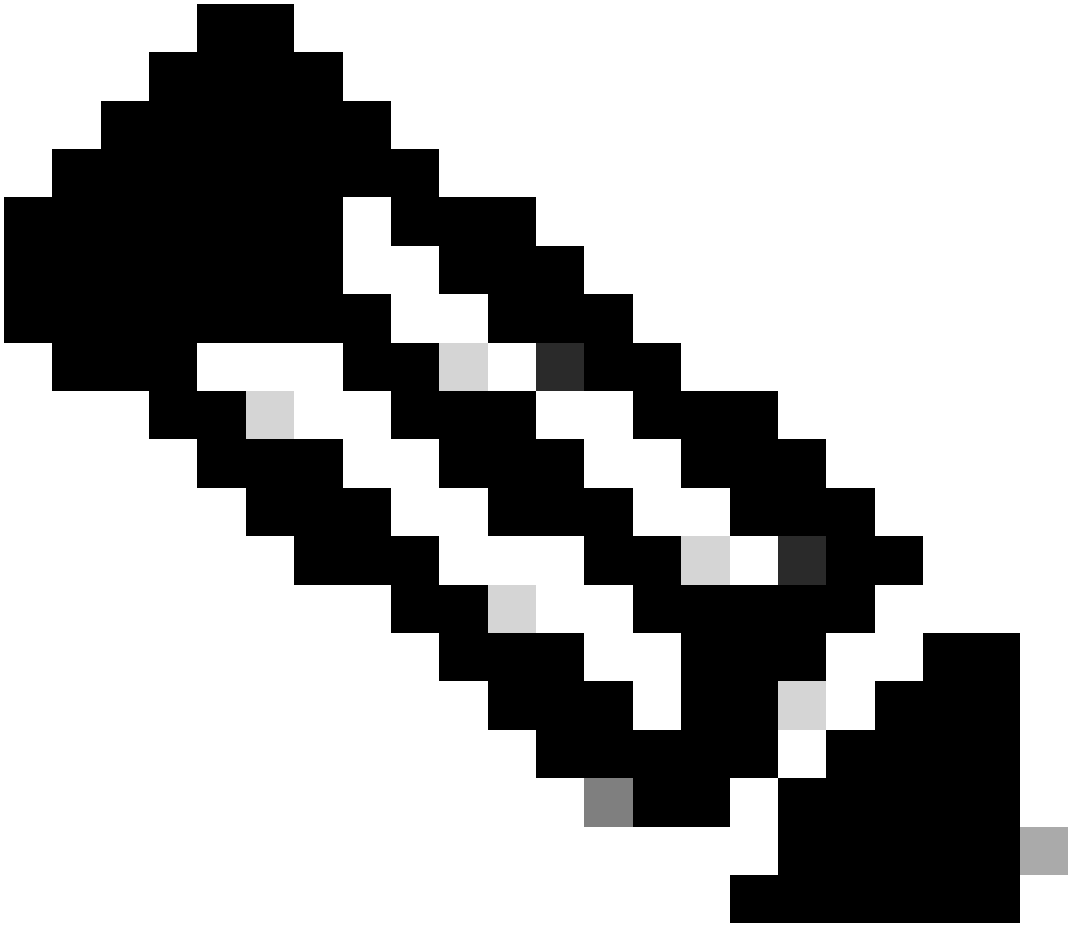
Welche DMVPN-Typen gibt es?

1. DMVPN-Phase I: In dieser Phase ist eine einzelne mGRE-Schnittstelle am Hub erforderlich, und alle Stationen sind nach wie vor statische Tunnel, sodass keine dynamischen Spoke-to-Spoke-Verbindungen entstehen.
2. DMVPN-Phase II: In dieser Phase wird jeder Standort mit einer mGRE-Schnittstelle konfiguriert, sodass Sie eine dynamische Spoke-to-Spoke-Verbindung erhalten.
3. DMVPN Phase III: Diese Phase erweitert die Skalierbarkeit des DMVPN-Netzwerks. Dies umfasst eine Zusammenfassung in der DMVPN-Cloud. Neben der Konfiguration von NHRP-Umleitungen und NHRP-Shortcut-Switching NHRP-Umleitungen weisen die Quelle an, einen besseren Pfad zu dem Ziel zu finden, das sie zu erreichen versucht. Über NHRP-Verknüpfungen kann DMVPN Informationen zu anderen Netzwerken hinter anderen DMVPN-Routern abrufen.

Datenverkehrsfluss für DMVPN Phase 3

1. Das Paket wird (entsprechend der Routing-Tabelle) vom 1-Netzwerk von Spoke über den Hub an die 2-Netzwerke von Spoke gesendet.
2. Der Hub leitet das Paket an Spoke2 weiter, sendet aber parallel die NHRP-Umleitungsnachricht an Spoke1 zurück, die Informationen über den suboptimalen Pfad zu Spoke2 und die Tunnel-IP-Adresse von Spoke2 enthält.
3. Anschließend sendet Spoke1 die NHRP-Auflösungsanforderung der 2 NBMA-IP-Adresse (Nonbroadcast Multiaccess) von Spoke an den Next Hop Server (NHS) mit der Ziel-IP-Adresse des 2-Tunnels von Spoke. Diese NHRP-Auflösungsanforderung wird über NHS gezielt an Spoke2 gesendet (gemäß Routing-Tabelle). Hierbei handelt es sich um einen normalen Hop-by-Hop-NHRP-Weiterleitungsprozess.
4. Spoke2 sendet nach Erhalt der Auflösungsanfrage einschließlich der NBMA-IP von Spoke1 die NHRP-Auflösungsantwort direkt an Spoke1 - Die Antwort durchläuft nicht den Hub!
5. Spoke1 überschreibt nach dem Empfang der korrekten NBMA-IP von Spoke2 den CEF-Eintrag für das Zielpräfix - dieses Verfahren wird als NHRP-Verknüpfung bezeichnet.
6. Spokes lösen kein NHRP aus, indem sie Adjacencies entfernen, aber NHRP-Antworten aktualisieren die CEF.


HUB
3
2
1
2
3
SPOKE 1
4
SPOKE 2

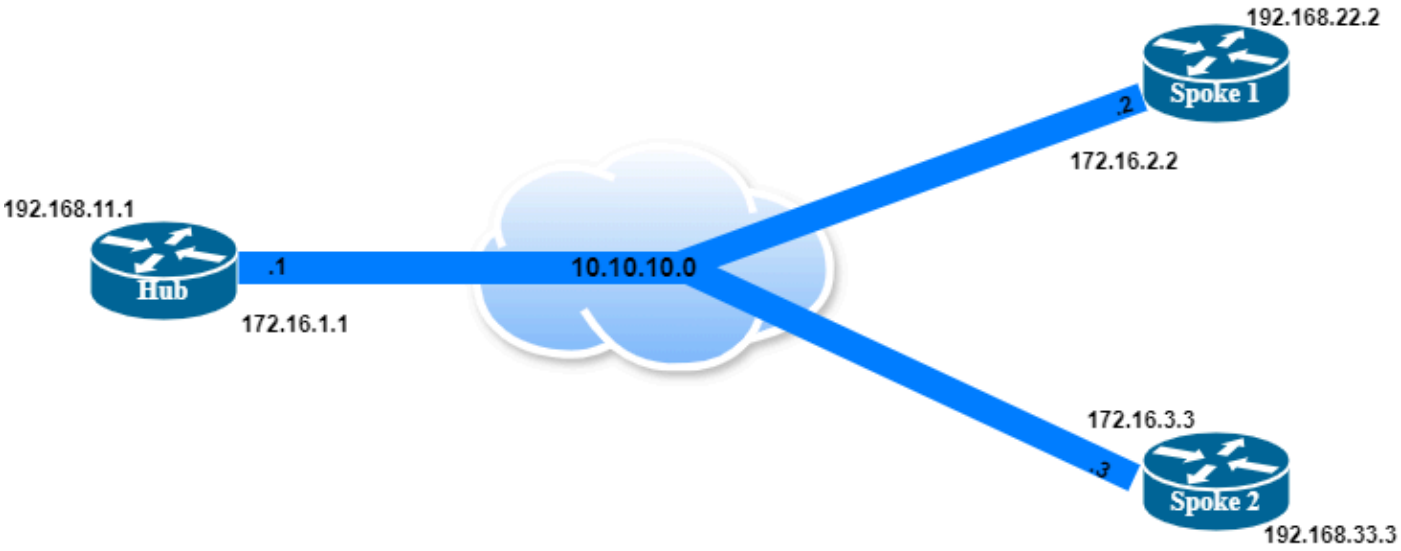


Anmerkung:

DMVPN-Phase 2: In dieser Phase wird das ursprüngliche Spoke-to-Spoke-Paket tatsächlich prozessgeschaltet, da sich die CEF-Adjacency im "Glean"-Zustand befindet. Dies bedeutet, dass der Router nicht über genügend Informationen verfügt, um das Paket mithilfe von CEF weiterzuleiten, und dass ein ressourcenintensiveres Prozess-Switching verwendet werden muss, um den nächsten Hop mithilfe von NHRP (Next Hop Resolution Protocol) aufzulösen.

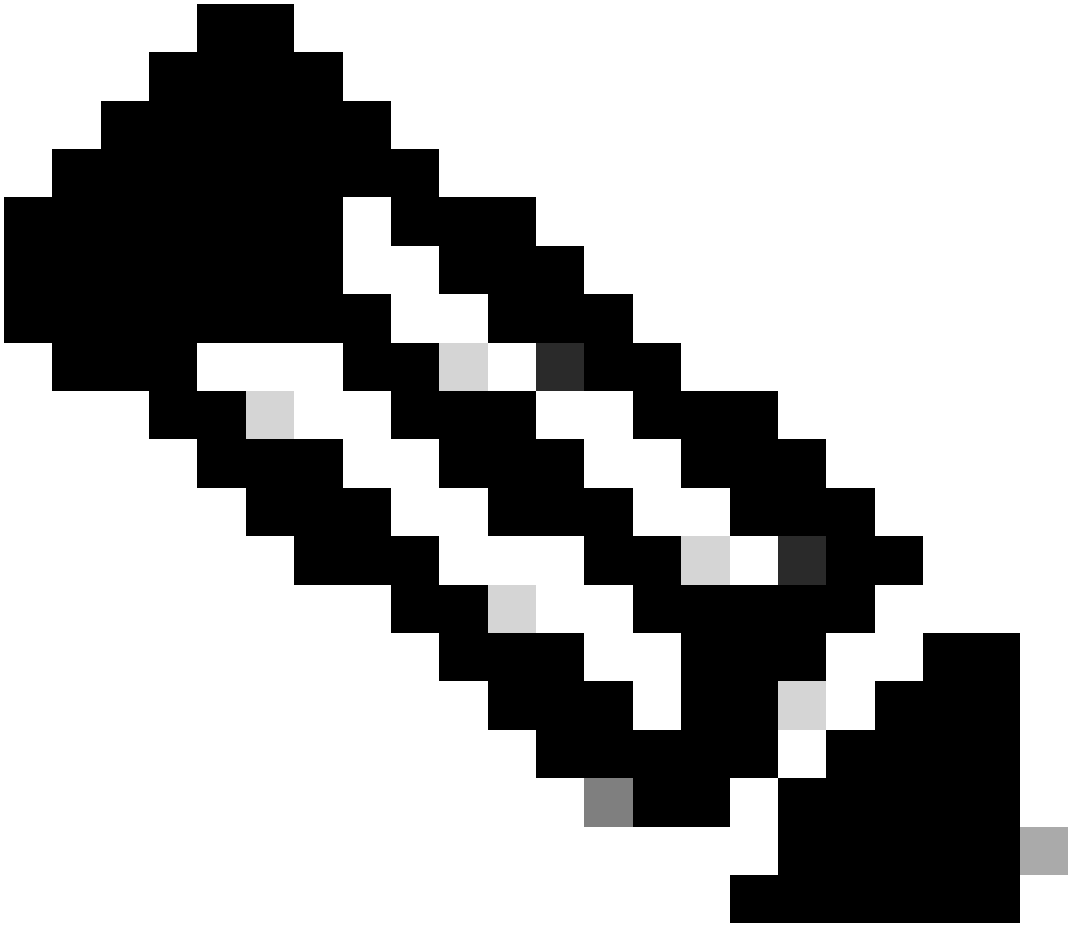
DMVPN-Phase 3: Diese Phase verbessert sich gegenüber Phase 2, da das erste Spoke-to-Spoke-Paket von Anfang an mithilfe von CEF geswitcht werden kann. Dies wird durch die Verwendung der Funktionen NHRP Redirect und NHRP Shortcut erreicht, die den schnellen Aufbau direkter Spoke-to-Spoke-Tunnel ermöglichen. Dadurch wird CEF konsistenter eingesetzt und die Abhängigkeit vom Prozess-Switching verringert.

Netzwerkdiagramm



Konfigurationen

Krypto-Konfigurationen



Anmerkung: Dies ist auf der Nabe und allen Speichen gleich.

1. Konfigurieren Sie ein Ikev2-Angebot und einen Keyring.

```
crypto ikev2 vorschlag DMVPN
Verschlüsselung aes-cbc-256
Integrität sha256
Gruppe 14
crypto ikev2 keyring IKEV2-KEYRING
Beliebige
Adresse 0.0.0.0 0.0.0.0
pre-shared-key CISCO123
!
```

2. Konfigurieren Sie das Ikev2-Profil, das alle verbindungsbezogenen Informationen enthält.

```
crypto ikev2-Profil IKEV2-PROF
```

Anpassungsadresse lokale Schnittstelle GigabitEthernet0/0/0
Übereinstimmung Identität Remote-Adresse 0.0.0.0
Authentifizierung lokale Pre-Share
Authentifizierung Remote Pre-Share
Schlüsselbund lokal IKEV2-KEYRING

Hier sind die Details der Befehle, die im ikev2-Profil verwendet werden:

- match address local interface GigabitEthernet0/0/0: Lokale externe Schnittstelle, an der das VPN endet, in diesem Fall GigabitEthernet0/0/0
- match identity remote address 0.0.0.0: Da der Remote-Peer mehrere sein kann, kann 0.0.0.0 verwendet werden, was einen beliebigen Peer angibt.
- Authentifizierung lokale Pre-Share: Der Authentifizierungsmodus am lokalen Standort ist vorab freigegeben.
- Authentifizierung Remote Pre-Share: Der Authentifizierungsmodus am lokalen Standort ist vorab freigegeben.
- keyring local IKEV2-KEYRING: Verwenden Sie denselben Keyring, den Sie zuvor erstellt haben.

3. Konfigurieren des IPsec-Profils

crypto ipsec transform-set T-SET esp-aes 256 esp-sha256-hmac
Modetunnel

crypto ipsec-Profil IPSEC-IKEV2

set transformation-set T-SET
IKEV2-PROF als ikev2-Profil festlegen

Erstellen Sie einen Transformationssatz für die IPsec-Tunnelaushandlung, und rufen Sie den Transformationssatz und das Ikev2-Profil unter dem IPsec-Profil auf.

DMVPN-Konfiguration

1. Konfigurieren Sie die externe Schnittstelle.

interface GigabitEthernet0/0/0

ip address 172.16.1.1 255.255.255.0
Verhandlungsauto
CDP aktivieren

2. Konfigurieren Sie den Hub-Router für die mGRE- und IPsec-Integration (d. h. verknüpfen Sie den Tunnel mit dem IPsec-Profil, das im vorherigen Verfahren konfiguriert wurde).

interface Tunnel0
ip address 10.10.10.1 255.255.255.0
no ip redirects

IP NHRP-Authentifizierung DMVPN
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp redirect <-------- Obligatorisch zur Aktivierung von DMVPN Phase 3 auf dem Hub-Router
tunnel source GigabitEthernet0/0/0
Tunnelbetriebsart-Mehrpunkt
Tunnelschutz IPSec-Profil IPSEC-IKEV2
!

Diese Befehle werden in der Tunnelschnittstellenkonfiguration verwendet:

- ip nhrp authentication DMVPN: In diesem Fall muss die Authentifizierungszeichenfolge "DMVPN" auf allen Hubs und Stationen, die Teil desselben DMVPN-Netzwerks sind, denselben Wert aufweisen.
- ip nhrp map multicast dynamic: Ermöglicht NHRP das dynamische Hinzufügen von Stationen zur NHRP-Multicast-Zuordnung.
- ip nhrp network-id 1: 32-Bit-Netzwerkkennung zur Aktivierung von NHRP auf einer Schnittstelle
- IP NHRP-Umleitung: Ermöglicht die Umleitung der Datenverkehrsanzeige, wenn Datenverkehr mit dem NHRP-Netzwerk weitergeleitet wird.
- tunnel source GigabitEthernet0/0/0: Legt die Quelladresse für eine Tunnelschnittstelle fest, hier wird die IP-Adresse GigaEthernet 0/0/0 verwendet.
- tunnel mode gre multipoint: Setzt den Kapselungsmodus für diese Tunnelschnittstelle auf mGRE.
- tunnel protection ipsec-Profil IPSEC-IKEV2: Ordnet eine Tunnelschnittstelle dem IPsec-Profil zu, das bereits in Krypto-Konfigurationen erstellt wurde.

3. Konfigurieren von Spoke-Routern für die mGRE- und IPsec-Integration zusammen mit einer externen Schnittstelle und Loopback zum Testen der Border Gateway Protocol (BGP)-Verbindung

SPOKE X: (Eine ähnliche Konfiguration kann in allen Speichen verwendet werden.)

interface GigabitEthernet0/0/0
ip address 172.16.3.3 255.255.255.0
Geschwindigkeit 1000
keine Verhandlungsautos

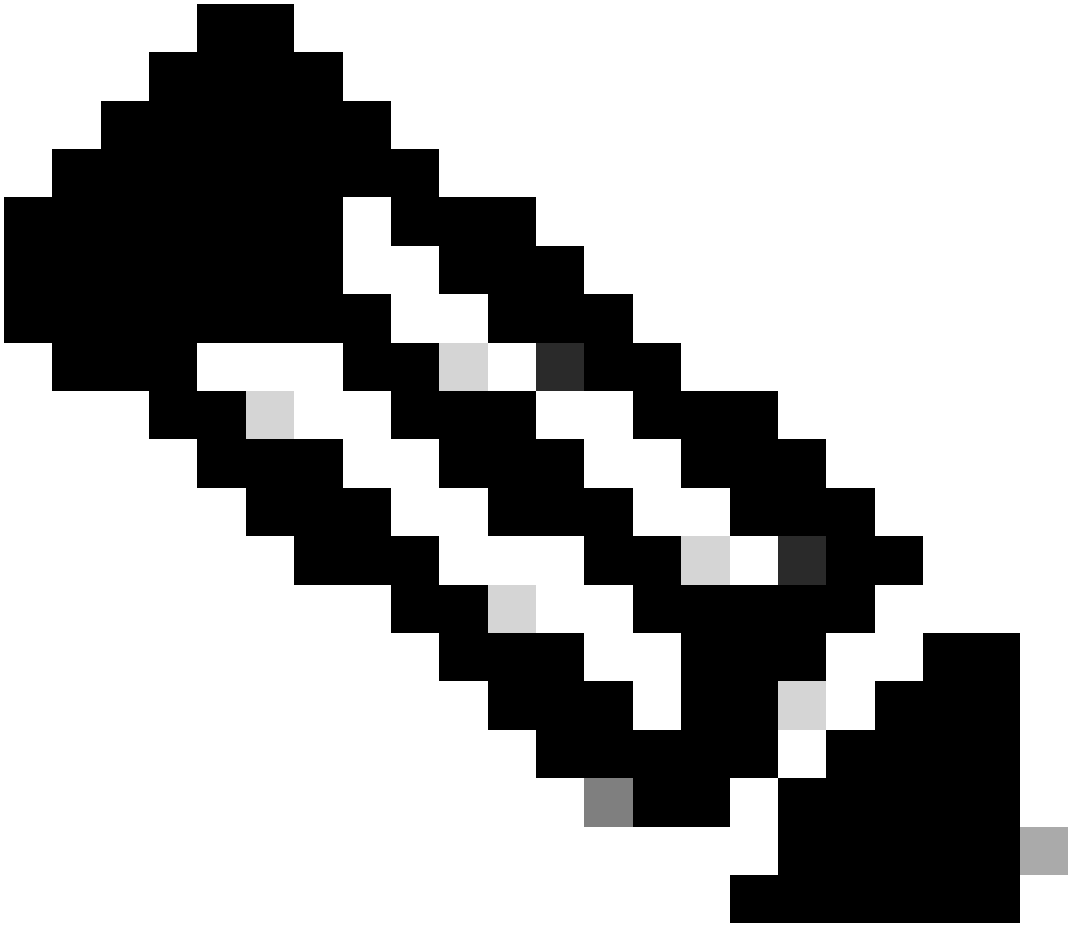
!

Schnittstelle Loopback10
ip address 192.168.33.3 255.255.255.0
!
interface Tunnel0
ip address 10.10.10.3 255.255.255.0
no ip redirects
IP NHRP-Authentifizierung DMVPN
ip nhrp map 10,10,10,1 172,16,1,1

ip nhrp map multicast 172.16.1.1
ip nhrp network-id 1
ip nhrp nhs 10,10,10,1
ip nhrp shortcut <-------- Obligatorisch zur Aktivierung von DMVPN Phase 3 auf Spoke Router
tunnel source GigabitEthernet0/0/0
Tunnelbetriebsart-Mehrpunkt
Tunnelschutz IPSec-Profil IPSEC-IKEV2

Diese Befehle werden in der Tunnelschnittstellenkonfiguration verwendet:

- ip nhrp authentication DMVPN: In diesem Fall muss die Authentifizierungszeichenfolge "DMVPN" auf allen Hubs und Stationen, die Teil desselben DMVPN-Netzwerks sind, denselben Wert aufweisen.
- ip nhrp map 10.10.10.1 172.16.1.1: Ordnet die Hub-NBMA-IP-Adresse manuell der Tunnel-Schnittstellen-IP-Adresse zu.
- ip nhrp map multicast 172.16.1.1: Leitet den gesamten Multicast-Verkehr zum Hub um.
- ip nhrp network-id 1: 32-Bit-Netzwerkkennung zur Aktivierung von NHRP auf einer Schnittstelle
- ip nhrp nhs 10.10.10.1: Der nächste Hop-Server, der unser Hub ist, wird mit diesem Befehl konfiguriert.
- IP NHRP-Verknüpfung: Aktiviert das NHRP-Shortcut-Switching auf einer Schnittstelle.
- tunnel source GigabitEthernet0/0/0: Legt die Quelladresse für eine Tunnelschnittstelle fest, hier wird die IP-Adresse GigaEthernet 0/0/0 verwendet.
- tunnel mode gre multipoint: Setzt den Kapselungsmodus für diese Tunnelschnittstelle auf mGRE.
- tunnel protection ipsec-Profil IPSEC-IKEV2: Ordnet eine Tunnelschnittstelle dem IPsec-Profil zu, das bereits in Krypto-Konfigurationen erstellt wurde.



Anmerkung: Der Befehl ip nhrp redirect sendet die Nachricht an die Spokes, die besagt: "Es gibt eine bessere Route zum Ziel-Spoke als über den Hub", und die Verknüpfung ip nhrp zwingt die Installation dieser Route in der Weiterleitungs-Informationsdatenbank (FIB) auf den Spokes auf.

BGP-Konfiguration

Es gibt verschiedene Variationen, aus denen Sie wählen können:

- eBGP mit einer anderen AS-Nummer in jeder Station
- eBGP mit derselben AS-Nummer in jeder Station
- iBGP

Die Erläuterung aller drei Szenarien wird in diesem Dokument nicht behandelt.

Ein eBGP mit einer anderen AS-Nummer auf allen Stationen ist konfiguriert, sodass dynamische Nachbarn nicht verwendet werden können. Daher müssen Sie die Nachbarn manuell

konfigurieren.

eBGP mit unterschiedlichen AS auf den Spokes

1. BGP-Konfiguration auf HUB:

Hub(config)#router bgp 65010

Hub(config-router)#bgp log-neighbor-changes

Hub(config-router)#network 192.168.11.1 Maske 255.255.255.255

Hub(config-router)#neighbor 10,10.10,2 remote-as 65011

Hub(config-router)#neighbor 10,10.10,3 remote-as 65012

!

Die folgenden Befehle werden in der BGP-Konfiguration auf dem Hub verwendet:

- Router BGP 65010: Konfigurieren eines BGP-Routing-Prozesses Verwenden Sie das Argument "Autonomous-System-number" (autonome Systemnummer), das das Gerät gegenüber anderen BGP-Routern identifiziert.
- Netzwerk 192.168.11.1 Maske 255.255.255.255: Gibt ein lokales Netzwerk für dieses autonome System an und fügt es der BGP-Routing-Tabelle hinzu.
- neighbor 10.10.10.2 remote-as 65011: Fügt die IP-Adresse des Nachbarn Spoke 1 im angegebenen autonomen System zur IPv4-BGP-Tabelle mit mehreren Protokollen des Nachbarn des lokalen Geräts hinzu.
- neighbor 10.10.10.3 remote-as 65012: Fügt die IP-Adresse des Nachbarn Spoke 2 im angegebenen autonomen System zur IPv4-BGP-Nachbartabelle des lokalen Geräts hinzu.

2. BGP-Konfiguration in Spoke X:

Spoke2(config)#router BGP 65012

Spoke2(config-router) #bgp Protokoll-Nachbarn-Änderungen

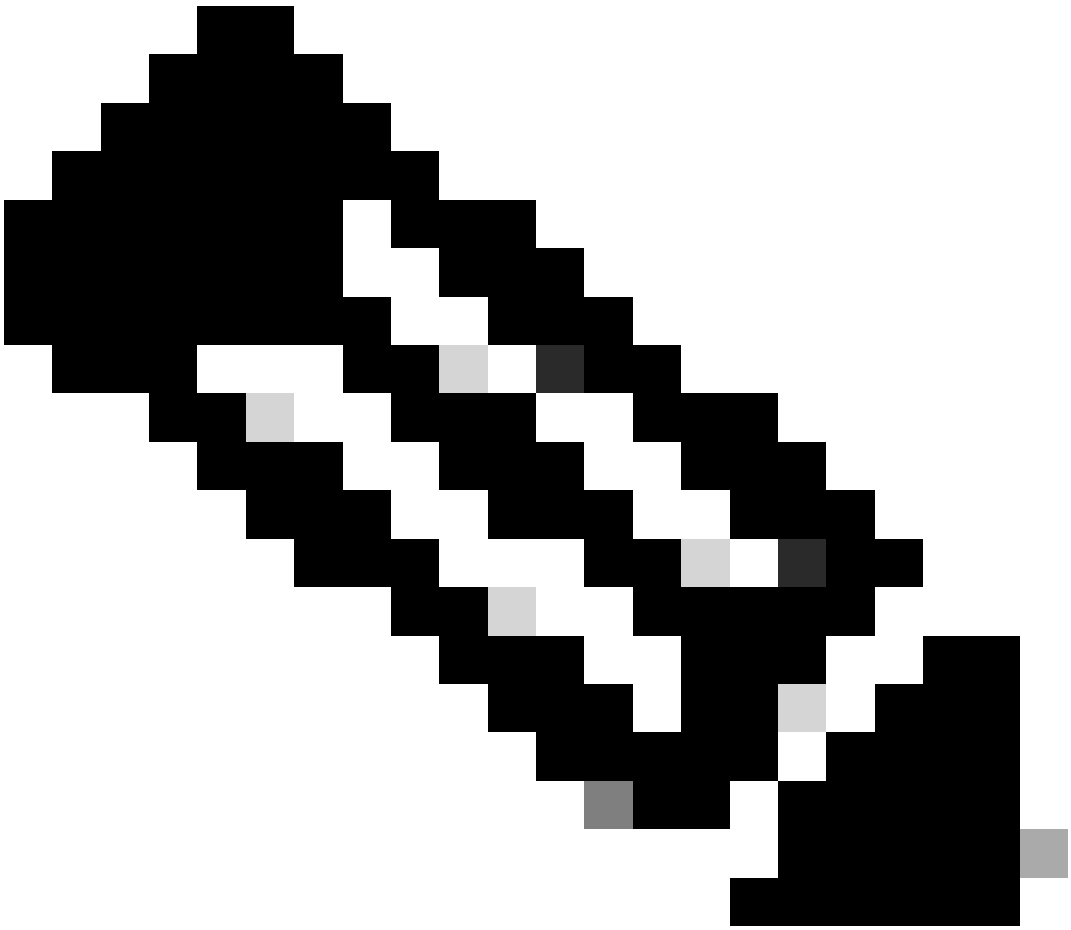
Spoke2(config-router)# Netzwerk 192.168.33.3 Maske 255.255.255.255

Spoke2(config-router)# Nachbar 10.10.10.1 remote-as 65010

Diese Befehle werden in der BGP-Konfiguration von Spoke X verwendet:

- Router BGP 65012: Konfigurieren eines BGP-Routing-Prozesses Verwenden Sie das Argument "Autonomous-System-number" (autonome Systemnummer), das das Gerät gegenüber anderen BGP-Routern identifiziert.
- Netzwerk 192.168.33.3 Maske 255.255.255.255: Gibt ein lokales Netzwerk für dieses autonome System an und fügt es der BGP-Routing-Tabelle hinzu.
- neighbor 10.10.10.1 remote-as 65010: Fügt die IP-Adresse des Hub im angegebenen autonomen System der IPv4-BGP-Nachbartabelle für mehrere Protokolle des lokalen Geräts

hinzu.



Anmerkung: Eine ähnliche Konfiguration muss auf allen Stationen im DMVPN-Netzwerk vorgenommen werden.

Überprüfung

1. Überprüfungsbefehle auf Hub-Gerät:

HUB#sh dmvpn

Zeigt DMVPN-spezifische Sitzungsinformationen an.

Legende: Attrb —> S - Statisch, D - Dynamisch, I - Unvollständig
N - NATed, L - Lokal, X - Kein Socket
T1 - Route Installed (Route Installiert), T2 - Nexthop-override
C - CTS-fähig

Ent —> Anzahl der NHRP-Einträge mit demselben NBMA-Peer
NHS-Status: E —> Antworten werden erwartet, R —> Antworten, W —> Warten
UpDn-Zeit —> Up- oder Down-Zeit für einen Tunnel
==========

Schnittstelle: Tunnel0, IPv4 NHRP-Details
Type:Hub, NHRP Peers:2, <<<<<<<<<<<<<<<<<<<< Informiert, dass das Gerät als Hub agiert und zwei NHRP-Peers mit diesem HUB verbunden sind.

Ent Peer-NBMA-Adr-Peer-Tunnel Add State UpDN TM ATTRB
----- --------------- --------------- ----- -------- -----
1 172.16.2.2 10.10.10.2 UP 01:47:08 D <<<<<<<<<<<<<<<<<< Beide Peers sind dynamisch beim Hub registriert und befinden sich im UP-Status.
1 172.16.3.3 10.10.10.3 UP 01:08:58 D

HUB#sh ip nhrp

Zeigt die NBMA-Adresszuordnung zur Tunnelschnittstellen-IP aller mit dem Hub verbundenen NHRP-Peers an. Der Hub verwaltet die Datenbank aller Stationen.

10.10.10.2/32 über 10.10.10.2
Tunnel0 erstellt 01:47:22, ablaufen 01:32:27
Typ: dynamisch, Flags: einzigartig registrierter verwendeter NHop
NBMA-Adresse: 172.16.2.2
10.10.10.3/32 über 10.10.10.3
Tunnel0 erstellt 01:09:11, ablaufen 01:29:58
Typ: dynamisch, Flags: einzigartig registrierter verwendeter NHop
NBMA-Adresse: 172.16.3.3

HUB#sh ip nhrp multicast

Zeigt Informationen zur NHRP-Multicast-Zuordnung an.

I/F-NBMA-Adresse
Tunnel0 172.16.2.2 Flags: dynamisch (aktiviert)
Tunnel0 172.16.3.3 Flags: dynamisch (aktiviert)

HUB#sh Krypto-Sockets

Anzahl der Crypto Socket-Verbindungen 2

Tu0-Peers (lokal/remote): 172.16.1.1/172.16.2.2
Lokale ID (Adresse/Maske/Port/Port): (172.16.1.1/255.255.255.255/0/47)
Remote-ID (Adresse/Maske/Port/Port): (172.16.2.2/255.255.255.255/0/47)
IPSec-Profil: "IPSEC-IKEV2"
Socket-Status: Offen
Kunde: "TUNNEL SEC" (Client-Status: Aktiv)

Tu0-Peers (lokal/remote): 172.16.1.1/172.16.3.3
Lokale ID (Adresse/Maske/Port/Port): (172.16.1.1/255.255.255.255/0/47)
Remote-ID (Adresse/Maske/Port/Port): (172.16.3.3/255.255.255.255/0/47)
IPSec-Profil: "IPSEC-IKEV2"
Socket-Status: Offen
Kunde: "TUNNEL SEC" (Client-Status: Aktiv)
Krypto-Sockets im Listen-Status:
Kunde: Profil "TUNNEL SEC": "IPSEC-IKEV2" Kartenname: "Tunnel0-head-0"

HUB#sh cry ikev2 sa

IPv4-Verschlüsselung für IKEv2 SA

Tunnel-ID Lokaler Remote-FVRF/IVRF-Status
1 172.16.1.1/500 172.16.2.2/500 EINZELNE/KEINE BEREIT
Registrieren: AES-CBC, Keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth-Zeichen: PSK, Auth-Verifizierung: PSK
Lebensdauer/Aktivzeit: 86400/6524 s

Tunnel-ID Lokaler Remote-FVRF/IVRF-Status
2 172.16.1.1/500 172.16.3.3/500 EINZELNE/KEINE BEREIT
Registrieren: AES-CBC, Keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth-Zeichen: PSK, Auth-Verifizierung: PSK
Lebensdauer/Aktivzeit: 86400/4234 s

IPv6-Verschlüsselung IKEv2 SA

HUB#sh ip bgp Zusammenfassung

Zeigt den aktuellen Status der BGP-Sitzung bzw. die Anzahl der Präfixe an, die der Router von einem Nachbarn oder einer Peer-Gruppe erhalten hat.

BGP-Router-ID: 192.168.11.1, lokale AS-Nummer 65010
Die Version der BGP-Tabelle ist 4, die Version der Routing-Tabelle ist 4.
3 Netzwerkeinträge mit 432 Byte Speicher
3 Pfadeinträge mit 252 Byte Speicher
3/3 BGP-Pfad/bestpath-Attributeinträge mit 480 Byte Speicher
2 BGP AS-PATH-Einträge mit 48 Byte Speicher
0 BGP-route-map-Cacheeinträge, die 0 Byte Speicher verwenden
0 BGP-Filterlisten-Cacheeinträge, die 0 Byte Speicher verwenden
BGP mit insgesamt 1.212 Byte Speicher
BGP-Aktivität 3/0-Präfixe, 3/0-Pfade, Scan-Intervall 60 Sekunden

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.2 4 65011 33 33 4 0 0 00:25:35 1
10.10.10.3 4 65012 21 25 4 0 0 00:14:58 1

Hub#sh ip route bgp

Codes: L - lokal, C - verbunden, S - statisch, R - RIP, M - mobil, B - BGP
D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA extern Typ 1, N2 - OSPF NSSA extern Typ 2
E1 - externer OSPF-Typ 1, E2 - externer OSPF-Typ 2
i - IS-IS, su - IS-IS-Zusammenfassung, L1 - IS-IS-Ebene-1, L2 - IS-IS-Ebene-2
ia - IS-IS interarea, * - candidate default, U - per user static route
o - ODR, P - periodische heruntergeladene statische Route, H - NHRP, l - LISP
a - Anwendungsweg
+ - replizierte Route, % - Next Hop Override, p - Overrides von PfR

Gateway der letzten Instanz ist 172.16.1.2 zum Netzwerk 0.0.0.0

192.168.0.0/16 ist variabel subnetziert, 4 Subnetze, 2 Masken
B 192.168.22.0/24 [20/0] via 10.10.10.2, 00:29:15 <<<<<<<<<<<<Eintrag für angekündigte Spoke 1-Routen
B 192.168.33.0/24 [20/0] via 10.10.10.3, 00:18:37 <<<<<<<<<<<<Entry for Spoke 2 advertised routing

2. Überprüfungsbefehle für Spoke 1:

Spoke1#sh dmvpn

Legende: Attrb —> S - Statisch, D - Dynamisch, I - Unvollständig
N - NATed, L - Lokal, X - Kein Socket
T1 - Route Installed (Route Installiert), T2 - Nexthop-override
C - CTS-fähig, I2 - Temporär
Ent —> Anzahl der NHRP-Einträge mit demselben NBMA-Peer
NHS-Status: E —> Antworten werden erwartet, R —> Antworten, W —> Warten
UpDn-Zeit —> Up- oder Down-Zeit für einen Tunnel
==========

Schnittstelle: Tunnel0, IPv4 NHRP-Details
Typ:Spoke, NHRP-Peers:2,

Ent Peer-NBMA-Adr-Peer-Tunnel Add State UpDN TM ATTRB
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1 UP 01:32:09 S <<<<<<<<<<<<<<Hub wird als S- statisch angezeigt, da wir ihn unter der Tunnelschnittstelle als statischen Eintrag konfiguriert haben.
1 172.16.3.3 10.10.10.3 UP 00:19:34 D <<<<<<<<<<<<<<Dynamischer On-Demand-Spoke-to-Spoke-Tunnel nach dem Senden von Datenverkehr an Spoke 2

Spoke1#sh ip bgp Zusammenfassung

BGP-Router-ID 192.168.22.2, lokale AS-Nummer 65011
Die Version der BGP-Tabelle ist 4, die Version der Routing-Tabelle ist 4.
3 Netzwerkeinträge mit 744 Byte Speicher
3 Pfadeinträge mit 432 Byte Speicher

3/3 BGP-Pfad/bestpath-Attributeinträge mit 864 Byte Speicher
2 BGP AS-PATH-Einträge mit 64 Byte Speicher
0 BGP-route-map-Cacheeinträge, die 0 Byte Speicher verwenden
0 BGP-Filterlisten-Cacheeinträge, die 0 Byte Speicher verwenden
BGP mit insgesamt 2104 Byte Speicher
BGP-Aktivität 3/0-Präfixe, 3/0-Pfade, Scan-Intervall 60 Sekunden
3 Netze erreicht ihren Höhepunkt um 08:16:54 Jun 2 2022 UTC (vor 01:11:51.732)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.1 4 65010 85 85 4 0 01:12:21 2 **<<<<<<<<<<<<<<<** Wir haben 2 Präfixe von Hub erhalten, jeweils für Hub-Loopback und Spoke2-Loopback.

Spoke1#sh IP-Route BGP

Codes: L - lokal, C - verbunden, S - statisch, R - RIP, M - mobil, B - BGP
D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA extern Typ 1, N2 - OSPF NSSA extern Typ 2
E1 - externer OSPF-Typ 1, E2 - externer OSPF-Typ 2, m - OMP
n - NAT, Ni - NAT innen, Nein - NAT außen, Nd - NAT DIA
i - IS-IS, su - IS-IS-Zusammenfassung, L1 - IS-IS-Ebene-1, L2 - IS-IS-Ebene-2
ia - IS-IS interarea, * - candidate default, U - per user static route
H - NHRP, G - NHRP registriert, G - NHRP Registrierungszusammenfassung
o - ODR, P - regelmäßig heruntergeladene statische Route, l - LISP
a - Anwendungsweg
+ - replizierte Route, % - Next Hop Override, p - Overrides von PfR

Das Gateway der letzten Instanz ist 172.16.2.10 zu Netzwerk 0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:16 **>>>>>>>>>>** Hub-Netzwerk direkt über Hub erreichbar

B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:46 **>>>>>>>>>>** Spoke-Netzwerk direkt über Spoke-Tunnel-IP erreichbar.

Spoke1#sh IP-Route

Codes: L - lokal, C - verbunden, S - statisch, R - RIP, M - mobil, B - BGP
D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA extern Typ 1, N2 - OSPF NSSA extern Typ 2
E1 - externer OSPF-Typ 1, E2 - externer OSPF-Typ 2, m - OMP
n - NAT, Ni - NAT innen, Nein - NAT außen, Nd - NAT DIA
i - IS-IS, su - IS-IS-Zusammenfassung, L1 - IS-IS-Ebene-1, L2 - IS-IS-Ebene-2
ia - IS-IS interarea, * - candidate default, U - per user static route
H - NHRP, G - NHRP registriert, G - NHRP Registrierungszusammenfassung
o - ODR, P - regelmäßig heruntergeladene statische Route, l - LISP
a - Anwendungsweg
+ - replizierte Route, % - Next Hop Override, p - Overrides von PfR

Das Gateway der letzten Instanz ist 172.16.2.10 zu Netzwerk 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.2.10
172.16.2.0/24 ist variabel subnetziert, 2 Subnetze, 2 Masken
C 172.16.2.0/24 ist direkt angeschlossen, GigabitEthernet2
L 172.16.2.2/32 ist direkt angeschlossen, GigabitEthernet2
10.0.0.0/8 ist variabel subnettiert, 2 Subnetze, 2 Masken
C 10.10.10.0/24 ist direkt angeschlossen, Tunnel0
L 10.10.10.2/32 ist direkt angeschlossen, Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:21
192.168.22.0/24 ist variabel subnetziert, 2 Subnetze, 2 Masken
C 192.168.22.0/24 ist direkt angeschlossen, Loopback10
L 192.168.22.2/32 ist direkt angeschlossen, Loopback10
B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:51

Spoke1#sh ip nhrp nhs

Legende: E=Antworten werden erwartet, R=Antworten, W=Warten, D=Dynamisch
Tunnel0:
10.10.10.1 RE priority = 0 cluster = 0 **>>>>>>>>** Nur ein Next Hop Server ist konfiguriert

Spoke1#sh ip nhrp-Datenverkehr

Tunnel0: Max. Sendegrenze:10000Pkte/10Sek., Nutzung:0%
Gesendet: Insgesamt 52
1 Abwicklungsanforderung 0 Lösung Antwort 51 Registrierungsanforderung **<<<<<<<<<<** Anzahl der an Hub gesendeten Registrierungsanforderungen
0 Registrierungsantwort 0 Löschanforderung 0 Löschantwort
0 Fehleranzeige 0 Datenverkehrsanzeige 0 Umleitungsunterdrückung
Empf.: Insgesamt 25
0 Abwicklungsanfrage 1 Lösung Antwort 0 Registrierungsanfrage **<<<<<<<<<<<<** Anzahl der Antworten auf diese Registrierungsanfragen
24 Registrierung Antwort 0 Löschanforderung 0 Löschantwort
0 Fehleranzeige 0 Datenverkehrsanzeige 0 Umleitungsunterdrückung

Spoke1#sh ip nhrp multicast

I/F-NBMA-Adresse
Tunnel0 172.16.1.1 Flags: static (Enabled) **<<<<<<<<<** Multicast-Datenverkehr wird für die Weiterleitung an das Hub-NBMA konfiguriert.

Spoke1#sh Kryptografie-Sockets

Anzahl der Crypto Socket-Verbindungen 2

Tu0-Peers (lokal/remote): 172.16.2.2/172.16.1.1
Lokale ID (Adresse/Maske/Port/Port): (172.16.2.2/255.255.255.255/0/47)
Remote-ID (Adresse/Maske/Port/Port): (172.16.1.1/255.255.255.255/0/47)
IPSec-Profil: "IPSEC-IKEV2"
Socket-Status: Öffnen Sie <<<<<<<<<<<<<<<<<< Status des Sockets für diesen bestimmten Peer.
Kunde: "TUNNEL SEC" (Client-Status: Aktiv)
Tu0-Peers (lokal/remote): 172.16.2.2/172.16.3.3
Lokale ID (Adresse/Maske/Port/Port): (172.16.2.2/255.255.255.255/0/47)
Remote-ID (Adresse/Maske/Port/Port): (172.16.3.3/255.255.255.255/0/47)
IPSec-Profil: "IPSEC-IKEV2"
Socket-Status: Offen
Kunde: "TUNNEL SEC" (Client-Status: Aktiv)
Krypto-Sockets im Listen-Status:
Kunde: Profil "TUNNEL SEC": "IPSEC-IKEV2" Kartenname: "Tunnel0-head-0"

Spoke1#sh cry ikev2 sa

IPv4-Verschlüsselung für IKEv2 SA

Tunnel-ID Lokaler Remote-FVRF/IVRF-Status
2 172.16.2.2/500 172.16.3.3/500 EINZELNE/KEINE BEREIT
Registrieren: AES-CBC, Keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth-Zeichen: PSK, Auth-Verifizierung: PSK
Lebensdauer/Aktivzeit: 86400/287 s

Tunnel-ID Lokaler Remote-FVRF/IVRF-Status
1 172.16.2.2/500 172.16.1.1/500 EINZELNE/KEINE BEREIT
Registrieren: AES-CBC, Keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth-Zeichen: PSK, Auth-Verifizierung: PSK
Lebensdauer/Aktivzeit: 86400/4643 s

IPv6-Verschlüsselung IKEv2 SA

Spoke1#traceroute 192.168.33.3 source lo10

Geben Sie Escape-Sequenz ein, um den Vorgang abzubrechen.
Verfolgung der Route bis 192.168.33.3
VRF-Informationen: (VRF in Name/ID, VRF out Name/ID)
1 10.10.10.3 3 ms 4 ms * <<<<<<<<<<<<<<<< Der Datenverkehr geht direkt zum Spoke 2-Router, ohne den Hub zu passieren.

Spoke2#sh dmvpn

Legende: Attrb —> S - Statisch, D - Dynamisch, I - Unvollständig
N - NATed, L - Lokal, X - Kein Socket
T1 - Route Installed (Route Installiert), T2 - Nexthop-override

C - CTS-fähig, I2 - Temporär
Ent —> Anzahl der NHRP-Einträge mit demselben NBMA-Peer
NHS-Status: E —> Antworten werden erwartet, R —> Antworten, W —> Warten
UpDn-Zeit —> Up- oder Down-Zeit für einen Tunnel
==========

Schnittstelle: Tunnel0, IPv4 NHRP-Details
Typ:Spoke, NHRP-Peers:2,

Ent Peer-NBMA-Adr-Peer-Tunnel Add State UpDN TM ATTRB
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1 UP 01:20:26 S
1 172.16.2.2 10.10.10.2 UP 00:07:51 D

3. Überprüfungsbefehle an Spoke 2:

Spoke2#sh IP NHRP

10.10.10.1/32 über 10.10.10.1
Tunnel0 erstellt 01:36:06, niemals ablaufen
Typ: static, Flags:
NBMA-Adresse: 172.16.1.1
10.10.10.2/32 über 10.10.10.2
Tunnel0 erstellt 00:08:09, ablaufen 00:01:50
Typ: dynamisch, Flags: Router implizit
NBMA-Adresse: 172.16.2.2
10.10.10.3/32 über 10.10.10.3
Tunnel0 erstellt 00:08:09, ablaufen 00:01:50
Typ: dynamisch, Flags: Router eindeutig lokal
NBMA-Adresse: 172.16.3.3
(kein Socket)
Spoke2#sh ip nhrp mul
Spoke2#sh ip nhrp multicast
I/F-NBMA-Adresse
Tunnel0 172.16.1.1 Flags: statisch (aktiviert)
Spoke 2#

Spoke2#sh Krypto-Sockets

Anzahl der Crypto Socket-Verbindungen 2

Tu0-Peers (lokal/remote): 172.16.3.3/172.16.1.1
Lokale ID (Adresse/Maske/Port/Port): (172.16.3.3/255.255.255.255/0/47)
Remote-ID (Adresse/Maske/Port/Port): (172.16.1.1/255.255.255.255/0/47)
IPSec-Profil: "IPSEC-IKEV2"
Socket-Status: Öffnen Sie <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Status von Socket für diesen bestimmten Peer.

Kunde: "TUNNEL SEC" (Client-Status: Aktiv)
Tu0-Peers (lokal/remote): 172.16.3.3/172.16.2.2
Lokale ID (Adresse/Maske/Port/Port): (172.16.3.3/255.255.255.255/0/47)
Remote-ID (Adresse/Maske/Port/Port): (172.16.2.2/255.255.255.255/0/47)
IPSec-Profil: "IPSEC-IKEV2"
Socket-Status: Offen
Kunde: "TUNNEL SEC" (Client-Status: Aktiv)
Krypto-Sockets im Listen-Status:
Kunde: Profil "TUNNEL SEC": "IPSEC-IKEV2" Kartenname: "Tunnel0-head-0"

Spoke2#sh cry ikev2 sa

IPv4-Verschlüsselung für IKEv2 SA

Tunnel-ID Lokaler Remote-FVRF/IVRF-Status
2 172.16.3.3/500 172.16.2.2/500 EINZELNE/KEINE BEREIT
Registrieren: AES-CBC, Keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth-Zeichen: PSK, Auth-Verifizierung: PSK
Lebensdauer/Aktivzeit: 86400/509 s

Tunnel-ID Lokaler Remote-FVRF/IVRF-Status
1 172.16.3.3/500 172.16.1.1/500 EINZELNE/KEINE BEREIT
Registrieren: AES-CBC, Keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth-Zeichen: PSK, Auth-Verifizierung: PSK
Lebensdauer/Aktivzeit: 86400/4866 s

IPv6-Verschlüsselung IKEv2 SA

Spoke2#sh IP BGP - Zusammenfassung

BGP-Router-ID 192.168.33.3, lokale AS-Nummer 65012
Die Version der BGP-Tabelle ist 4, die Version der Routing-Tabelle ist 4.
3 Netzwerkeinträge mit 744 Byte Speicher
3 Pfadeinträge mit 432 Byte Speicher
3/3 BGP-Pfad/bestpath-Attributeinträge mit 864 Byte Speicher
2 BGP AS-PATH-Einträge mit 64 Byte Speicher
0 BGP-route-map-Cacheeinträge, die 0 Byte Speicher verwenden
0 BGP-Filterlisten-Cacheeinträge, die 0 Byte Speicher verwenden
BGP mit insgesamt 2104 Byte Speicher
BGP-Aktivität 3/0-Präfixe, 3/0-Pfade, Scan-Intervall 60 Sekunden
3 Netze erreicht ihren Höhepunkt um 08:16:54 Jun 2 2022 UTC (vor 01:20:43.775)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.1 465010 97 94 4 0 0 01:21:07 2 **>>>>>>>>>>>>>>>>>>>**. Wir haben 2 Präfixe von Hub erhalten, jeweils für Hub-Loopback und Spoke2-Loopback.

Spoke2#sh IP-Route

Codes: L - lokal, C - verbunden, S - statisch, R - RIP, M - mobil, B - BGP
D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA extern Typ 1, N2 - OSPF NSSA extern Typ 2
E1 - externer OSPF-Typ 1, E2 - externer OSPF-Typ 2, m - OMP
n - NAT, Ni - NAT innen, Nein - NAT außen, Nd - NAT DIA
i - IS-IS, su - IS-IS-Zusammenfassung, L1 - IS-IS-Ebene-1, L2 - IS-IS-Ebene-2
ia - IS-IS interarea, * - candidate default, U - per user static route
H - NHRP, G - NHRP registriert, G - NHRP Registrierungszusammenfassung
o - ODR, P - regelmäßig heruntergeladene statische Route, l - LISP
a - Anwendungsweg
+ - replizierte Route, % - Next Hop Override, p - Overrides von PfR

Das Gateway der letzten Instanz ist 172.16.3.10 zum Netzwerk 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.3.10
172.16.3.0/24/8 ist variabel subnetziert, 2 Subnetze, 2 Masken
C 172.16.3.0/24 ist direkt angeschlossen, GigabitEthernet3
L 172.16.3.3/32 ist direkt angeschlossen, GigabitEthernet3
10.0.0.0/8 ist variabel subnettiert, 2 Subnetze, 2 Masken
C 10.10.10.0/24 ist direkt angeschlossen, Tunnel0
L 10.10.10.3/32 ist direkt angeschlossen, Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:47:08
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:46:45
192.168.33.0/24 ist variabel subnetziert, 2 Subnetze, 2 Masken
C 192.168.33.0/24 ist direkt angeschlossen, Loopback10
L 192.168.33.3/32 ist direkt angeschlossen, Loopback10

Spoke2#sh IP-Route BGP

Codes: L - lokal, C - verbunden, S - statisch, R - RIP, M - mobil, B - BGP
D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA extern Typ 1, N2 - OSPF NSSA extern Typ 2
E1 - externer OSPF-Typ 1, E2 - externer OSPF-Typ 2, m - OMP
n - NAT, Ni - NAT innen, Nein - NAT außen, Nd - NAT DIA
i - IS-IS, su - IS-IS-Zusammenfassung, L1 - IS-IS-Ebene-1, L2 - IS-IS-Ebene-2
ia - IS-IS interarea, * - candidate default, U - per user static route
H - NHRP, G - NHRP registriert, G - NHRP Registrierungszusammenfassung
o - ODR, P - regelmäßig heruntergeladene statische Route, l - LISP
a - Anwendungsweg
+ - replizierte Route, % - Next Hop Override, p - Overrides von PfR

Das Gateway der letzten Instanz ist 172.16.3.10 zum Netzwerk 0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:21:11 >>>>>>>>>>>>>>Hub-Netzwerk direkt über Hub erreichbar
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:20:48 >>>>>>>>>>> Spoke-Netzwerk direkt über

Spoke-Tunnel-IP erreichbar.

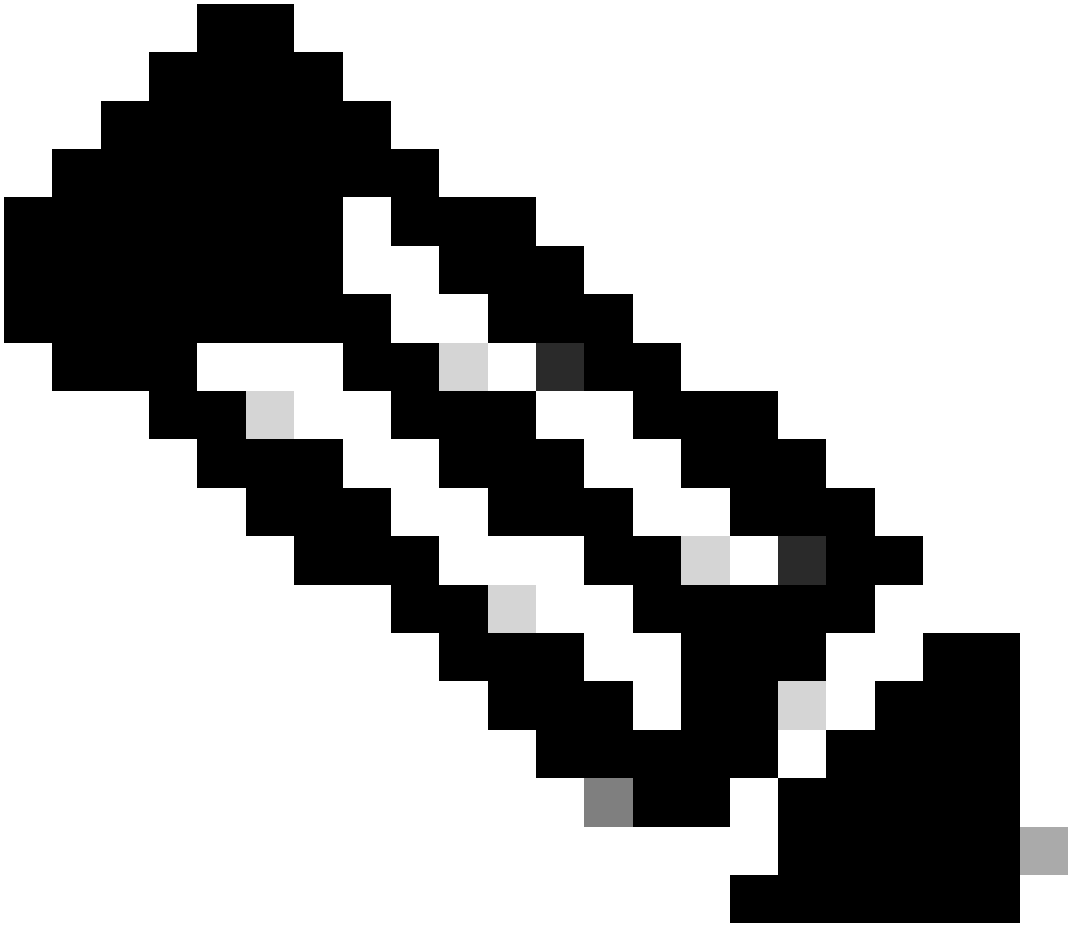
Spoke2#sh IP NHRP NHS

Legende: E=Antworten werden erwartet, R=Antworten, W=Warten, D=Dynamisch
Tunnel0:
10.10.10.1 RE priority = 0 cluster = 0 >>>>>>>>>>>> Nur ein Next Hop Server ist konfiguriert

Spoke2#traceroute 192.168.22.2 Quell-Loopback 10

Geben Sie Escape-Sequenz ein, um den Vorgang abzubrechen.
Verfolgung der Route bis 192.168.22.2
VRF-Informationen: (VRF in Name/ID, VRF out Name/ID)
1 10.10.10.2 4 ms 4 ms * <<<<<<<<<<<<<<<< Der Datenverkehr geht direkt zum Spoke 1-Router, ohne den Hub zu passieren.

Fehlerbehebung



Anmerkung: Es wird immer empfohlen, bedingtes Debuggen zu verwenden, da sich das Ausführen von nicht bedingtem Debuggen auf den Prozessor und damit auf die Produktionsumgebung auswirken kann. Die NBMA-Adresse entspricht der 'äußeren IP-Adresse' (IP-Adresse, die für die Quellenangabe der Tunnelschnittstelle verwendet wird) und die Tunnel-IP-Adresse der 'logischen IP-Adresse, d. h. der IP-Adresse der Tunnelschnittstelle'.

debug dmvpn condition peer <nmbma/tunnel> <NMBA IP- oder Tunnel IP-Adresse des Peers>
debug crypto condition peer ipv4 <WAN-IP des Peers>
debug nhrp condition peer <nbma/tunnel> <NBMA- oder Tunnel-IP-Adresse des Peers>

Für die DMVPN-Fehlerbehebung ist ein mehrschichtiger Ansatz erforderlich:

debug dmvpn detail all

1. Verschlüsselungsebene: Nach der Bestätigung der physischen Verbindung zwischen zwei Peers muss die Verschlüsselung überprüft werden. Diese Ebene verschlüsselt/entschlüsselt GRE-Pakete.

Allgemeine Debug-Befehle zum Überprüfen des Verschlüsselungsteils:

debugging crypto condition peer ipv4 <WAN-IP-Adresse des Peers>

debuggen crypto ikev2

debug crypto ikev2 error

debugging crypto ikev2 internal

debugging crypto ikev2 packet

debuggen crypto ipsec

debuggen crypto ipsec-Fehler

ODER

debug dmvpn condition peer <nmbma/tunnel> <NMBA IP- oder Tunnel IP-Adresse des Peers>

debug crypto condition peer ipv4 <WAN-IP des Peers>

debuggen dmvpn detail crypto

Ausführliche Informationen zur Fehlerbehebung auf der Verschlüsselungsebene finden Sie über den folgenden externen Link:

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html

2. GRE/NHRP: Zu den häufigsten Problemen gehören ein Fehler bei der NHRP-Registrierung und dynamische NBMA-Adressänderungen in Spoke, die zu einer inkonsistenten NHRP-Zuordnung im Hub führen.

Allgemeine Debug-Befehle zum Überprüfen der NHRP-Zuordnung:

debug nhrp condition peer <nbma/tunnel> <NBMA- oder Tunnel-IP-Adresse des Peers>

debug nhrp cache

debugging nhrp packet

Fehlersuche nhrp detail

debugging nhrp error

Informationen zu den gängigsten Lösungen zur DMVPN-Fehlerbehebung finden Sie über den folgenden externen Link:

https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html

3. Routing: Das Routing-Protokoll überwacht den Status von Spoke-Spoke-Tunnel auf Anforderung nicht.

IP-Routing-Updates und IP-Multicast-Datenpakete durchlaufen nur die Hub-and-Spoke-Tunnel.

Unicast-IP-Datenpakete durchlaufen sowohl den Hub-and-Spoke- als auch den On-Demand-Spoke-Tunnel.

Fehlersuche: Verschiedene Debug-Befehle, abhängig vom Routing-Protokoll.

Weitere Informationen zum BGP-Routing finden Sie über den externen Link:

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

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.