Fehlerbehebung bei gängigen DMVPN-Problemen

Inhalt

Einleitung

In diesem Dokument werden die häufigsten Lösungen für Probleme mit Dynamic Multipoint VPN (DMVPN) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der DMVPN-Konfiguration auf Cisco IOS®-Routern verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco IOS

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.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

In diesem Dokument werden die häufigsten Lösungen für Probleme mit Dynamic Multipoint VPN (DMVPN) beschrieben. Viele dieser Lösungen können implementiert werden, bevor eine gründliche Fehlerbehebung für die DMVPN-Verbindung erfolgt. Dieses Dokument stellt eine Checkliste gängiger Vorgehensweisen dar, die Sie ausprobieren sollten, bevor Sie mit der Fehlerbehebung für eine Verbindung beginnen und den technischen Support von Cisco anrufen.

Weitere Informationen finden Sie im Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T .

Unter Debugbefehle zur Problembehandlung bei IPsec verstehen und verwenden finden Sie eine Erläuterung häufiger Debugbefehle, die zur Fehlerbehebung bei IPsec-Problemen verwendet werden.

DMVPN-Konfiguration funktioniert nicht

Problem

Eine kürzlich konfigurierte oder geänderte DMVPN-Lösung funktioniert nicht.

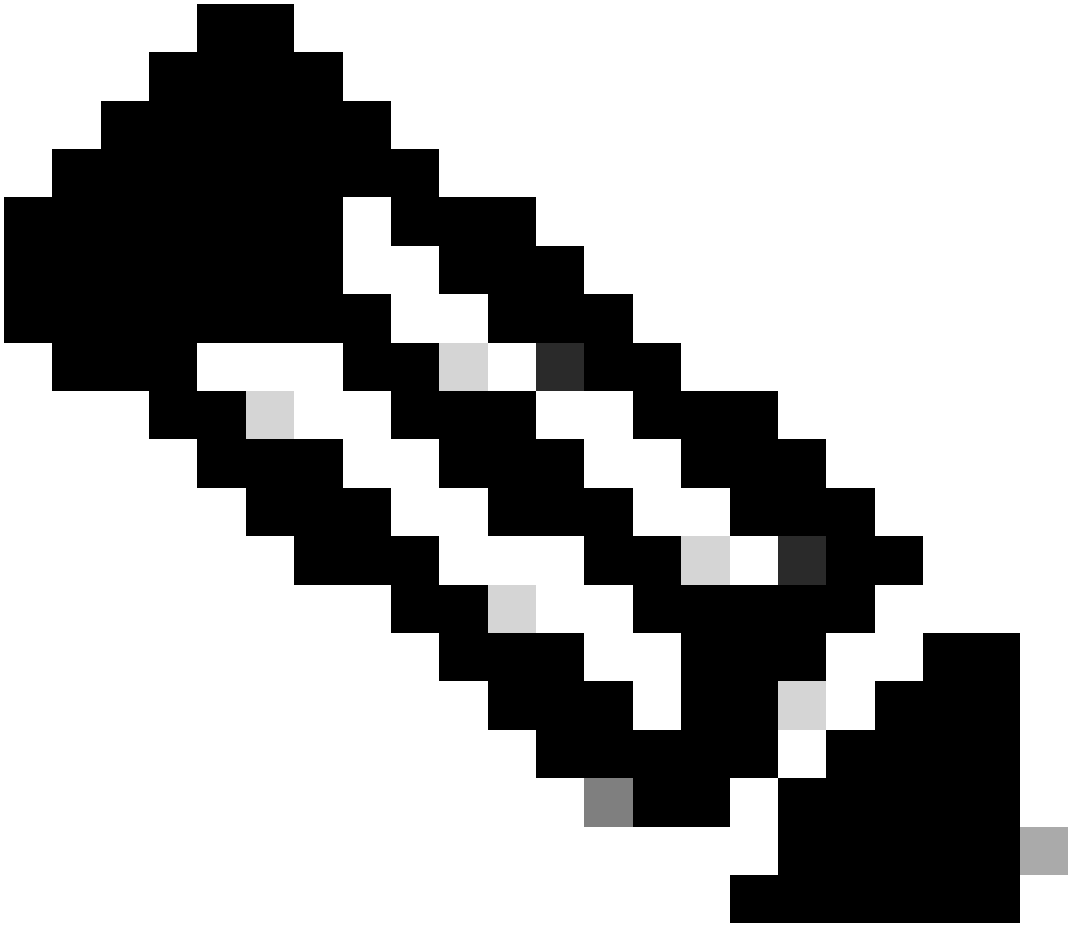
Eine aktuelle DMVPN-Konfiguration funktioniert nicht mehr.

Lösungen

Dieser Abschnitt enthält Lösungen für die häufigsten DMVPN-Probleme.

Diese Lösungen (in keiner bestimmten Reihenfolge) können als Checkliste für Punkte verwendet werden, die Sie überprüfen oder ausprobieren sollten, bevor Sie eine detaillierte Fehlerbehebung durchführen:

- Häufige Probleme
- Überprüfen Sie, ob Internet Security Association and Key Management Protocol (ISAKMP)-Pakete vom Internet Service Provider (ISP) blockiert werden.
- Überprüfen Sie, ob Generic Routing Encapsulation (GRE) funktioniert, wenn der Tunnelschutz entfernt wurde.
- Next-Hop Resolution Protocol (NHRP)-Registrierung fehlgeschlagen.
- Überprüfen Sie, ob die Lebensdauer richtig konfiguriert ist.
- Überprüfen Sie, ob der Datenverkehr nur in eine Richtung fließt.
- Überprüfen Sie, ob der Routing-Protokollnachbar eingerichtet ist.



Hinweis: Bevor Sie beginnen, überprüfen Sie die folgenden Schritte:

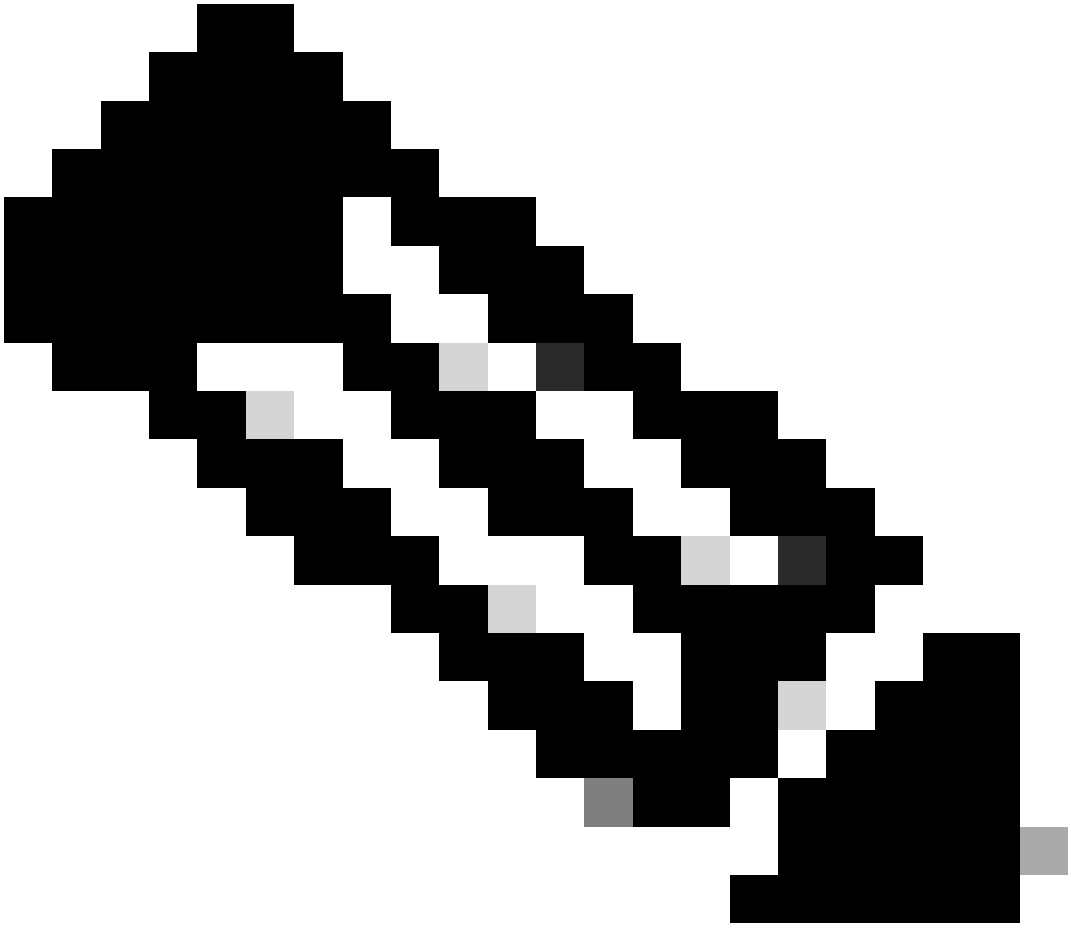
1. Zeitstempel zwischen Hub und Spoke synchronisieren
2. Aktivieren Sie die msec-Debug- und Protokoll-Zeitstempel:

```
Router(config)#service Zeitstempel Debugging DatumZeit ms

Router(config)#service Zeitstempel Log DatumZeit ms
```

3. Zeitstempel der exec-Terminalaufforderung für die Debugsitzungen aktivieren:

```
Zeitstempel der Router#terminal exec-Eingabeaufforderung
```



Hinweis: Auf diese Weise können Sie die Debug-Ausgabe leicht mit der Ausgabe des Befehls show korrelieren.

Häufige Probleme

Überprüfen der grundlegenden Verbindungen

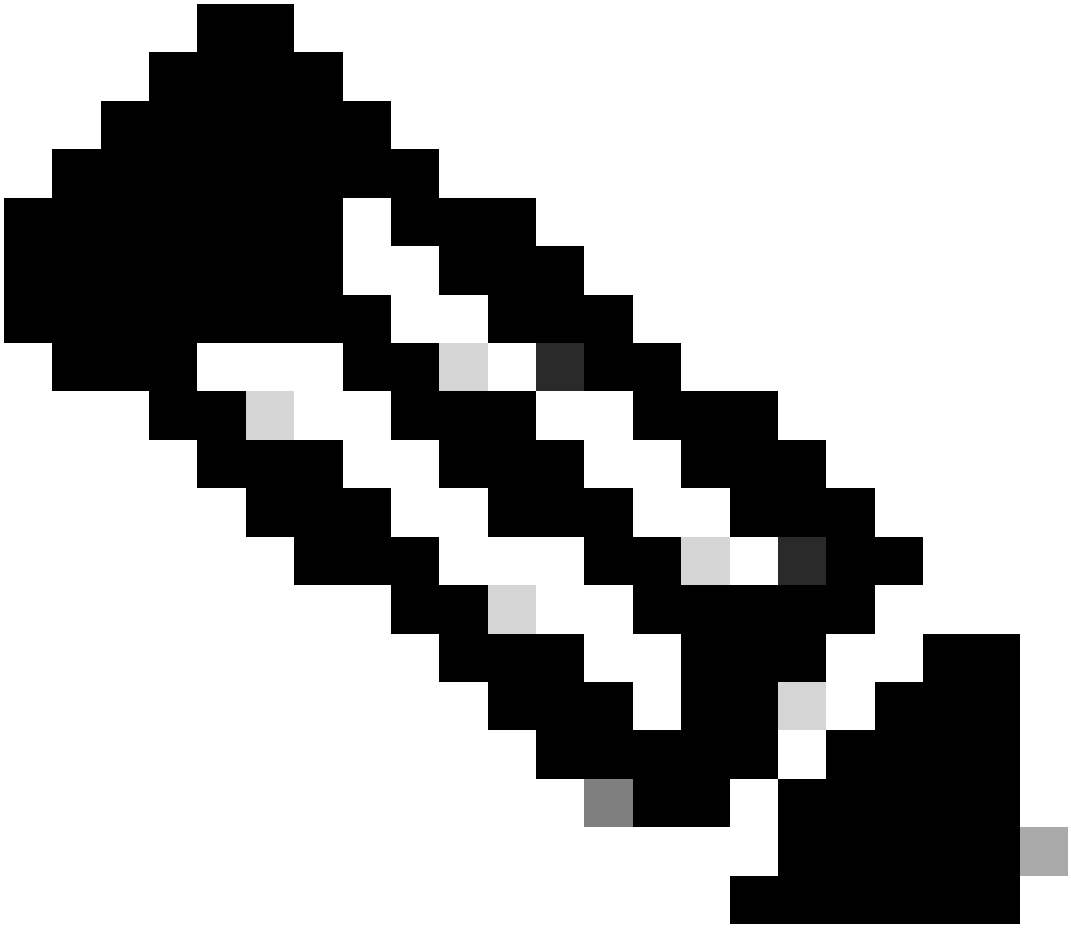
1. Senden Sie einen Ping-Befehl vom Hub an die Spoke mit NBMA-Adressen und umgekehrt.

   Diese Pings müssen direkt über die physische Schnittstelle und nicht über den DMVPN-Tunnel gesendet werden. Hoffentlich gibt es keine Firewall, die Ping-Pakete blockiert. Wenn dies nicht funktioniert, überprüfen Sie das Routing und alle Firewalls zwischen Hub- und Spoke-Routern.

2. Verwenden Sie außerdem traceroute, um den Pfad der verschlüsselten Tunnelpakete zu überprüfen.

3. Verwenden Sie die Befehle debug und show, um zu überprüfen, ob keine Verbindung besteht:

   - debug ip icmp
   - debug ip packet



Hinweis: Der Befehl debug ip packet generiert eine große Menge an Ausgabe und verwendet eine große Menge an Systemressourcen. Dieser Befehl muss in Produktionsnetzwerken mit Vorsicht verwendet werden. Verwenden Sie den Befehl "access-list" immer. Weitere Informationen zur Verwendung der Zugriffsliste mit debug ip packet finden Sie unter Problembehandlung bei IP-Zugriffslisten.

Überprüfung auf inkompatible ISAKMP-Richtlinie

Wenn die konfigurierten ISAKMP-Richtlinien nicht mit der vorgeschlagenen Richtlinie des Remote-Peers übereinstimmen, versucht der Router, die Standardrichtlinie von 65535 zu verwenden.

Wenn diese beiden Werte nicht übereinstimmen, schlägt die ISAKMP-Aushandlung fehl.

Der Befehl show crypto isakmp sa gibt an, dass sich die ISAKMP-SA in MM_NO_STATE befindet, was bedeutet, dass der Hauptmodus fehlgeschlagen ist.

Überprüfen Sie, ob ein falscher Schlüssel für den Pre-Shared Key vorliegt.

Wenn die vorab geteilten Geheimnisse nicht auf beiden Seiten gleich sind, scheitern die Verhandlungen.

Der Router gibt die Meldung "Plausibilitätsprüfung fehlgeschlagen" zurück.

Überprüfen auf inkompatiblen IPsec-Transformationssatz

Wenn der IPsec-Transformationssatz auf den beiden IPsec-Geräten nicht kompatibel ist oder nicht übereinstimmt, schlägt die IPsec-Aushandlung fehl.

Der Router gibt die Meldung atts not accept (Nicht akzeptabel) für den IPsec-Vorschlag zurück.

Überprüfen Sie, ob ISAKMP-Pakete beim ISP blockiert sind.

<#root>

```
Router#
```

show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
Dst                src                  state       conn-id      slot       status
172.17.0.1      172.16.1.1        MM_NO_STATE         0               0       ACTIVE
172.17.0.1      172.16.1.1        MM_NO_STATE         0               0       ACTIVE (deleted)
172.17.0.5        172.16.1.1        MM_NO_STATE      0             0       ACTIVE
172.17.0.5        172.16.1.1        MM_NO_STATE      0             0       ACTIVE (deleted)
```

Im vorherigen Beispiel wird das Flapping des VPN-Tunnels veranschaulicht.

Überprüfen Sie außerdem, debug crypto isakmp ob der Spoke-Router ein UDP 500-Paket sendet:

<#root>

```
Router#
```

debug crypto isakmp

<#root>

```
04:14:44.450: ISAKMP:(0):Old State = IKE_READY
                         New State = IKE_I_MM1
```

04:14:44.450: ISAKMP:(0): beginning Main Mode exchange

```
04:14:44.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:44.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
```

04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE..

```
.
04:14:54.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 1 of 5: retransmit phase 1
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
04:14:54.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:54.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
```

04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE..

```
.
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:15:04.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 2 of 5: retransmit phase 1
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
```

Die vorherige debug Ausgabe zeigt, dass der Spoke-Router alle 10 Sekunden ein UDP 500-Paket sendet.

Erkundigen Sie sich beim ISP, ob der Spoke-Router direkt mit dem ISP-Router verbunden ist, um sicherzustellen, dass der UDP 500-Datenverkehr zugelassen wird.

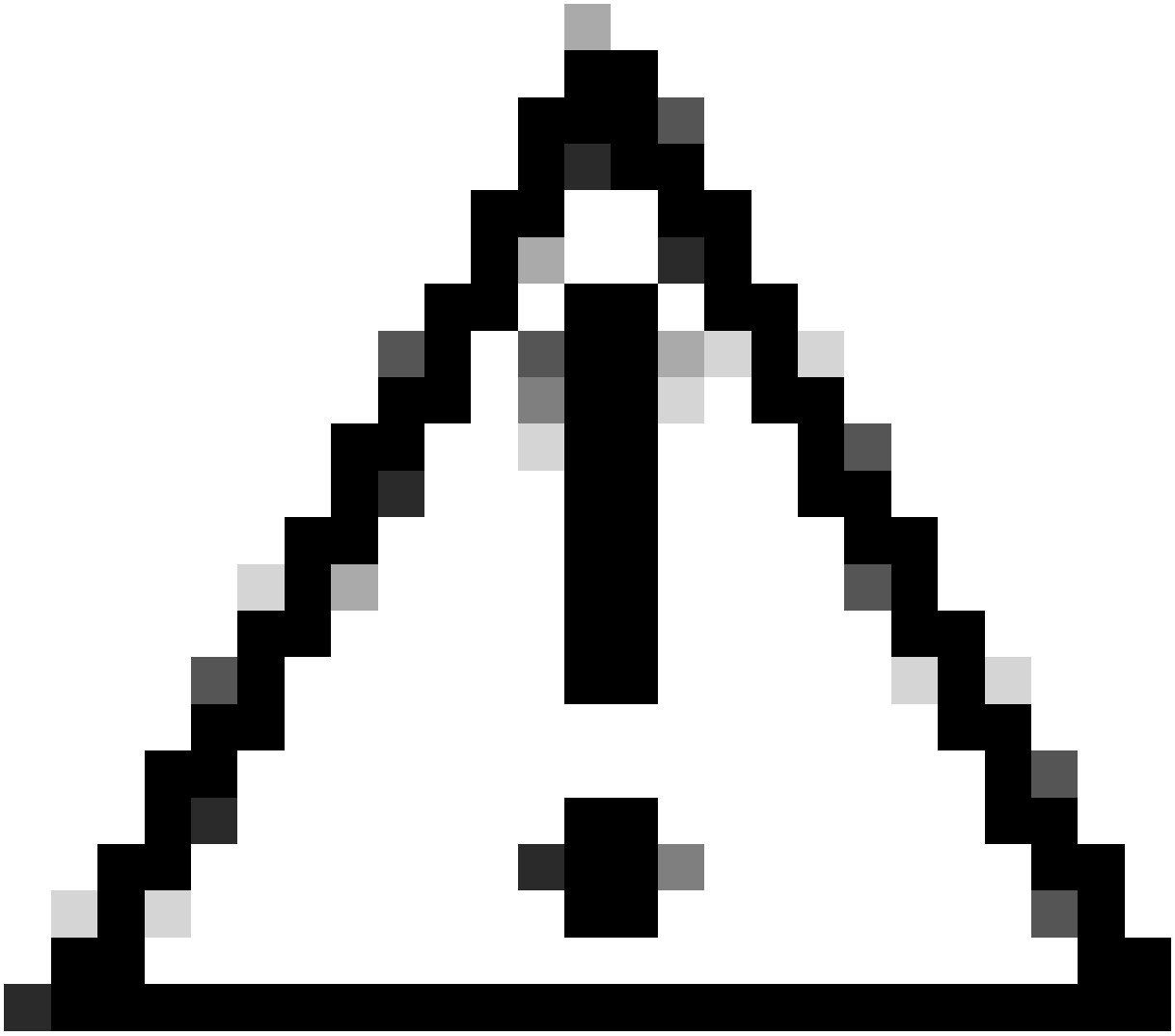
Nachdem der ISP udp 500 zugelassen hat, fügen Sie in der Ausgangsschnittstelle eine eingehende ACL hinzu. Dies ist eine Tunnelquelle, damit udp 500 sicher stellen kann, dass der udp 500-Datenverkehr in den Router gelangt. Verwenden Sie den show access-listBefehl, um zu überprüfen, ob die Anzahl der Treffer erhöht wird.

<#root>

Router#

show access-lists 101

Extended IP access list 101
10 permit udp host 172.17.0.1 host 172.16.1.1 eq isakmp log (4 matches)
20 permit udp host 172.17.0.5 host 172.16.1.1 eq isakmp log (4 matches)
30 permit ip any any (295 matches)



Achtung: Stellen Sie sicher, dass Sie ip any any allowed in Ihrer Zugriffsliste haben. Andernfalls kann der gesamte andere Datenverkehr als eingehende Zugriffsliste an der Ausgangsschnittstelle blockiert werden.

Überprüfen Sie, ob GRE funktioniert, wenn der Tunnelschutz entfernt wird.

Wenn DMVPN nicht funktioniert, stellen Sie vor der Fehlerbehebung mit IPsec sicher, dass die GRE-Tunnel ohne IPsec-Verschlüsselung einwandfrei funktionieren.

Weitere Informationen finden Sie unter How to Configure a GRE Tunnel.

NHRP-Registrierung fehlgeschlagen

Der VPN-Tunnel zwischen Hub und Spoke ist aktiv, kann jedoch keinen Datenverkehr weiterleiten:

```
<#root>

Router#

show crypto isakmp sa

        dst             src             state          conn-id  slot   status
        172.17.0.1      172.16.1.1      QM_IDLE           1082    0    ACTIVE

<#root>

Router#

show crypto IPSEC sa

local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)

#pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
```

```
inbound esp sas:
spi: 0xF830FC95(4163959957)
outbound esp sas:
spi: 0xD65A7865(3596253285)

!--- !--- Output is truncated !---
```

Es zeigt, dass der rückwärtige Verkehr nicht vom anderen Ende des Tunnels zurückkommt.

Überprüfen Sie den NHS-Eintrag im Spoke-Router:

```
<#root>

Router#

show  ip nhrp nhs detail

Legend: E=Expecting replies, R=Responding
Tunnel0: 172.17.0.1  E  req-sent 0

 req-failed 30

 repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 4371, Ret 64  NHS 172.17.0.1
```

Es zeigt, dass die NHS-Anfrage fehlgeschlagen ist. Um dieses Problem zu beheben, stellen Sie sicher, dass die Konfiguration auf der Spoke-Router-Tunnelschnittstelle korrekt ist.

Konfigurationsbeispiel:

<#root>

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
```

ip nhrp nhs 172.17.0.1

!--- !--- Output is truncated !---

Konfigurationsbeispiel mit dem richtigen Eintrag für den NHS-Server:

<#root>

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
```

ip nhrp nhs 10.0.0.1

!--- !--- Output is truncated !---

Überprüfen Sie nun die NHS-Eingabe und die IPsec-Verschlüsselungs-/Entschlüsselungszähler:

<#root>

```
Router#
```

show ip nhrp nhs detail

```
Legend: E=Expecting replies, R=Responding
Tunnel0:        10.0.0.1 RE  req-sent 4
```

req-failed 0

```
repl-recv 3 (00:01:04 ago)

Router#
```

show crypto IPSec sa

```
local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
```

#pkts encaps: 121, #pkts encrypt: 121, #pkts digest: 121
#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

```
inbound esp sas:
spi: 0x1B7670FC(460747004)
outbound esp sas:
spi: 0x3B31AA86(993110662)

!--- !--- Output is truncated !---
```

Überprüfen der ordnungsgemäßen Konfiguration der Lebensdauer

Verwenden Sie diese Befehle, um die aktuelle SA-Lebensdauer und den Zeitpunkt für die nächste Neuverhandlung zu überprüfen:

- **crypto isakmp sa detail anzeigen**
- **show crypto ipsec sa peer<NBMA-address-peer>**

Beachten Sie die SA-Lebensdauerwerte. Wenn sie sich in der Nähe der konfigurierten Lebensdauer befinden (der Standardwert ist 24 Stunden für ISAKMP und 1 Stunde für IPsec), bedeutet dies, dass diese SAs kürzlich ausgehandelt wurden. Wenn Sie es sich etwas später anschauen und sie wieder ausgehandelt wurden, dann können ISAKMP und/oder IPsec auf und ab springen.

<#root>

```
Router#
```

show crypto ipsec security-assoc lifetime

Security association lifetime: 4608000 kilobytes/3600 seconds

```
Router#
```

show crypto isakmp policy

```
Global IKE policy
Protection suite of priority 1
Encryption algorithm: DES-Data Encryption Standard (65 bit keys)
Hash algorithm: Message Digest 5
Authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
```

Lifetime: 86400 seconds, no volume limit

```
Default protection suite
 Encryption algorithm: DES- Data Encryption Standard (56 bit keys)
 Hash algorithm: Secure Hash Standard
 Authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group: #1 (768 bit)
 Lifetime: 86400 seconds, no volume limit

Router#
```

show crypto ipsec sa

```
interface: Ethernet0/3
    Crypto map tag: vpn, local addr. 172.17.0.1
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
   current_peer: 172.17.0.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.0.1
     path mtu 1500, media mtu 1500
     current outbound spi: 8E1CB77A

 inbound esp sas:
      spi: 0x4579753B(1165587771)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
```

sa timing: remaining key lifetime (k/sec): (4456885/3531)

```
        IV size: 8 bytes
        replay detection support: Y
outbound esp sas:
      spi: 0x8E1CB77A(2384246650)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
```

sa timing: remaining key lifetime (k/sec): (4456885/3531)

```
        IV size: 8 bytes
        replay detection support: Y
```

Überprüfen, ob der Datenverkehr nur in eine Richtung fließt

Der VPN-Tunnel zwischen dem Spoke-to-Spoke-Router ist aktiv, kann jedoch keinen Datenverkehr weiterleiten.

<#root>

```
Spoke1#
```

show crypto ipsec sa peer 172.16.2.11

```
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
```

```
#pkts encaps: 110, #pkts encrypt: 110
    #pkts decaps: 0, #pkts decrypt: 0,



local crypto endpt.: 172.16.1.1,
remote crypto endpt.: 172.16.2.11
      inbound esp sas:
      spi: 0x4C36F4AF(1278669999)
      outbound esp sas:
      spi: 0x6AC801F4(1791492596)

!--- !--- Output is truncated !---


Spoke2#



sh crypto ipsec sa peer 172.16.1.1



   local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)



 #pkts encaps: 116, #pkts encrypt: 116,
   #pkts decaps: 110, #pkts decrypt: 110,



local crypto endpt.: 172.16.2.11,
remote crypto endpt.: 172.16.1.1
     inbound esp sas:
     spi: 0x6AC801F4(1791492596)
     outbound esp sas:
     spi: 0x4C36F4AF(1278669999

!--- !--- Output is truncated !---
```

In Spoke1 sind keine Decappakete vorhanden, d. h., ESP-Pakete werden irgendwo im Pfad verworfen, der von Spoke2 zu Spoke1 zurückkehrt.

Der Spoke2-Router zeigt sowohl Encap als auch Decap an, was bedeutet, dass der ESP-Datenverkehr gefiltert wird, bevor er Spoke2 erreicht. Dies kann am ISP-Ende an Spoke2 oder an einer beliebigen Firewall im Pfad zwischen Spoke2-Router und Spoke1-Router geschehen. Nachdem sie ESP (IP-Protokoll 50) zugelassen haben, zeigen Spoke1 und Spoke2 Zähler für Encaps und Decaps an.

<#root>

spoke1#

show crypto ipsec sa peer 172.16.2.11

local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)

#pkts encaps: 300, #pkts encrypt: 300
#pkts decaps: 200, #pkts decrypt: 200

!--- !--- Output is truncated !---

spoke2#

sh crypto ipsec sa peer 172.16.1.1

local ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)

#pkts encaps: 316, #pkts encrypt: 316,
#pkts decaps: 300, #pkts decrypt: 310

!--- !--- Output is truncated !---

Stellen Sie sicher, dass der Routing-Protokoll-Nachbar eingerichtet ist.

Spokes können keine Nachbarbeziehung zum Routing-Protokoll herstellen:

<#root>

Hub#

show ip eigrp neighbors

```
H   Address     Interface   Hold Uptime     SRTT    RTO       Q      Seq
                                (sec)             (ms)  Cnt     Num
2   10.0.0.9     Tu0         13  00:00:37     1    5000       1      0
0   10.0.0.5     Tu0         11     00:00:47   1587   5000       0     1483
1   10.0.0.11    Tu0         13     00:00:56     1    5000       1      0
```

Syslog message:
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10:
Neighbor 10.0.0.9 (Tunnel0) is down: retry limit exceeded

Hub#

show ip route eigrp

```
    172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Überprüfen Sie, ob die NHRP-Multicast-Zuordnung im Hub ordnungsgemäß konfiguriert ist.

Für den Hub muss in der Hub-Tunnelschnittstelle eine dynamische NHRP-Multicast-Zuordnung konfiguriert sein.

Konfigurationsbeispiel:

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test
 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint

!--- !--- Output is truncated !---
```

Konfigurationsbeispiel mit dem richtigen Eintrag für die dynamische NHRP-Multicast-Zuordnung:

<#root>

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test
```

ip nhrp map multicast dynamic

```
 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint

!--- !--- Output is truncated !---
```

Dadurch kann NHRP den Multicast-NHRP-Zuordnungen automatisch Spoke-Router hinzufügen.

Weitere Informationen finden Sie unter dem ip nhrp map multicast dynamic Befehl in der Befehlsreferenz für Cisco IOS IP Addressing Services.

<#root>

Hub#

show ip eigrp neighbors

```
IP-EIGRP neighbors for process 10
H   Address     Interface   Hold   Uptime   SRTT    RTO     Q     Seq
                                            (sec)    (ms)   Cnt    Num
2   10.0.0.9     Tu0         12   00:16:48   13     200     0     334
1   10.0.0.11    Tu0         13   00:17:10   11     200     0     258
0   10.0.0.5     Tu0         12   00:48:44  1017    5000    0     1495
```

Hub#

show ip route

```
     172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
```

D   192.168.11.0/24 [90/2944000] via 10.0.0.11, 00:16:12, Tunnel0

```
     10.0.0.0/24 is subnetted, 1 subnets
```

```
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
```

```
D    192.168.2.0/24 [90/2818560] via 10.0.0.9, 00:15:45, Tunnel0
```

```
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Routen zu den Stationen werden mithilfe des eigrp-Protokolls erfasst.

Problem mit Remote-Access-VPN mit DMVPN-Integration

Problem

DMVPN funktioniert einwandfrei, kann das RAVPN jedoch nicht herstellen.

Lösung

Verwenden Sie ISAKMP-Profile und IPsec-Profile, um dies zu erreichen. Erstellen Sie separate Profile für DMVPN und RAVPN.

Weitere Informationen finden Sie unter Konfigurationsbeispiel für DMVPN und Easy VPN-Server mit ISAKMP-Profilen.

Problem mit Dual-Hub-Dual-DMVPN

Problem

Problem mit Dual-Hub-Dual-DMVPN. Insbesondere Tunnel fallen und können nicht neu verhandeln.

Lösung

Verwenden Sie das Schlüsselwort "shared" im IPsec-Schutz des Tunnels sowohl für die Tunnelschnittstellen auf dem Hub als auch auf dem Spoke.

Konfigurationsbeispiel:

```
interface Tunnel43
 description <<tunnel to primary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---

interface Tunnel44
 description <<tunnel to secondary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---
```

Weitere Informationen finden Sie in dem **tunnel protection** Befehl in der Cisco IOS Security Command Reference (A-C).

Probleme bei der Anmeldung bei einem Server über DMVPN

Problem

Auf den Problemverkehr über den DMVPN-Netzwerkserver kann nicht zugegriffen werden.

Lösung

Das Problem kann mit der MTU und der MSS-Größe des Pakets zusammenhängen, das GRE und IPsec verwendet.

Die Paketgröße könnte ein Problem mit der Fragmentierung sein. Um dieses Problem zu beheben, verwenden Sie die folgenden Befehle:

<#root>

```
ip mtu 1400
ip tcp adjust-mss 1360
crypto IPSec fragmentation after-encryption (global)
```

Sie können den **tunnel path-mtu-discovery**Befehl auch so konfigurieren, dass die MTU-Größe dynamisch erkannt wird.

Eine ausführlichere Erklärung finden Sie unter Beheben von IP-Fragmentierung, MTU, MSS und PMTUD-Problemen mit GRE und IPSEC.

Zugriff auf die Server auf DMVPN über bestimmte Ports nicht möglich

Problem

Über bestimmte Ports kann nicht auf Server in DMVPN zugegriffen werden.

Lösung

So deaktivieren Sie die Cisco IOS-Firewall und prüfen, ob sie funktioniert:

Wenn alles reibungslos funktioniert, liegt das Problem in der Cisco IOS Firewall-Konfiguration und nicht in der DMVPN-Konfiguration.

Zugehörige Informationen

- **Dynamic Multipoint VPN (DMVPN)**
- **IPSec-Aushandlung/IKE-Protokolle**
- **Technischer Support und Downloads von Cisco**

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.