Fehlerbehebungsleitfaden für DMVPN Phase 1

Inhalt

Einführung

In diesem Dokument werden die Fehlermeldungen beschrieben, die Sie beim Hub-and-Spoke-Angriff auf eine DMVPN-Phase 1-Bereitstellung (Dynamic Multipoint Virtual Private Network) erhalten würden.

Voraussetzungen

Für die Konfigurations- und Debugbefehle in diesem Dokument sind zwei Cisco Router erforderlich, auf denen Cisco IOS® Release 12.4(9)T oder höher ausgeführt wird. Im Allgemeinen erfordert eine grundlegende DMVPN-Phase 1 die Cisco IOS-Version 12.2(13)T oder höher oder Version 12.2(33)XNC für den Aggregation Services Router (ASR), obwohl die in diesem Dokument beschriebenen Funktionen und Debugging möglicherweise nicht unterstützt werden.

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Generic Routing Encapsulation (GRE)
- Next Hop Resolution Protocol (NHRP)
- Internet Security Association und Key Management Protocol (ISAKMP)
- Internet Key Exchange (IKE)
- Internet Protocol Security (IPSec)
- Mindestens eines dieser Routing-Protokolle: Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP) und Border Gateway Protocol (BGP)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco 2911 Integrated Services Routers (ISRs), auf denen Cisco IOS Release 15.1(4)M4 ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Erhebliche Verbesserungen

Diese Cisco IOS-Versionen enthielten wichtige Funktionen oder Fixes für DMVPN Phase 1:

- Version 12.2(18)SXF5 - bessere Unterstützung für ISAKMP bei der Verwendung der Public Key Infrastructure (PKI)
- Version 12.2(33)XNE - ASR, IPSec-Profile, Tunnelschutz, IPSec Network Address Translation (NAT) Traversal
- Version 12.3(7)T - Unterstützung von Virtual Routing and Forwarding (iVRF)
- Version 12.3(11)T - Unterstützung für Virtual Routing and Forwarding (fVRF) an der Vorderseite
- Version 12.4(9)T - Unterstützung verschiedener DMVPN-bezogener Debug- und Befehlen
- Version 12.4(15)T - Gemeinsamer Tunnelschutz
- Version 12.4(20)T - IPv6 über DMVPN
- Version 15.0(1)M - NHRP Tunnel Health Monitoring

Konventionen

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

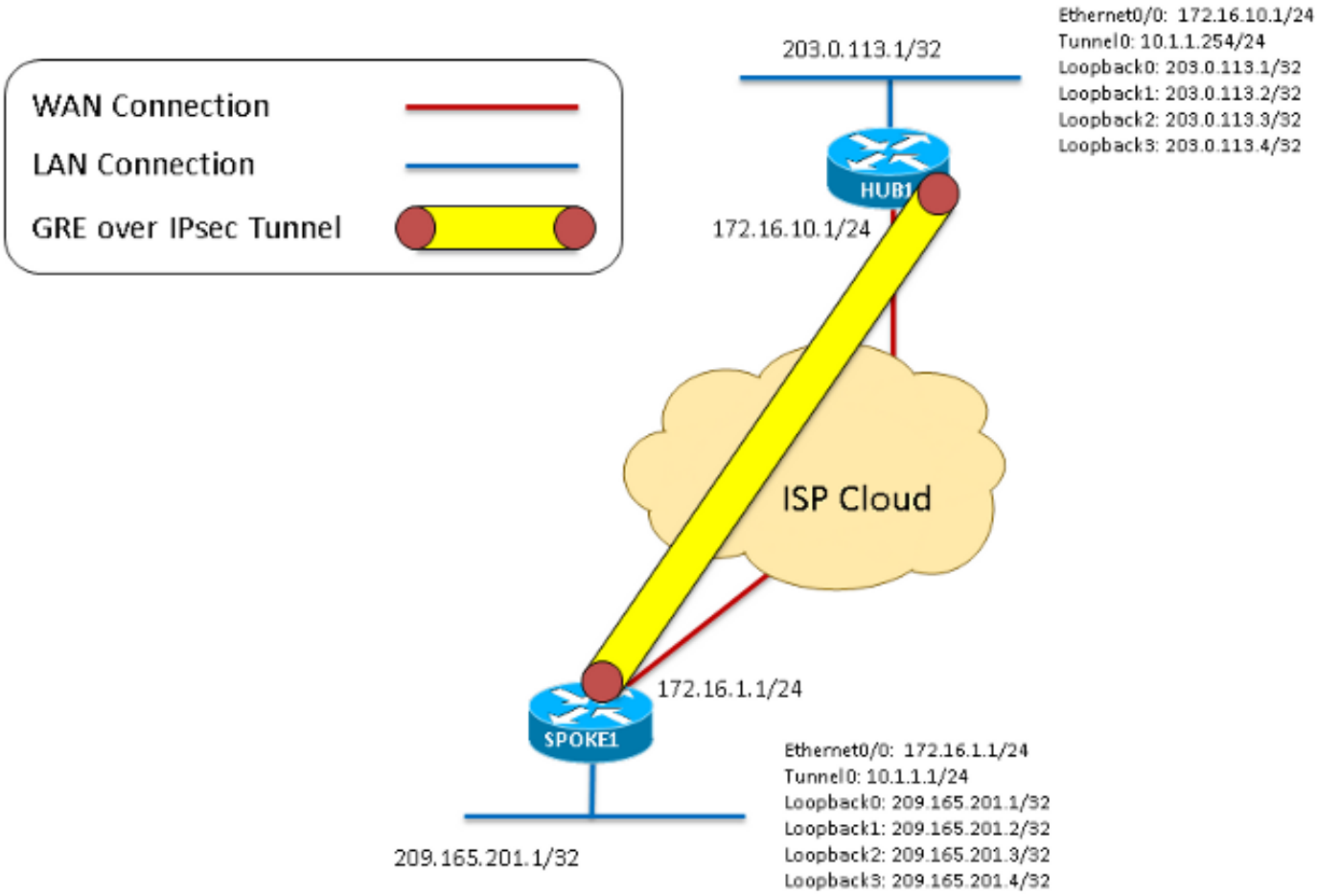
Relevante Konfiguration

Topologieübersicht

Für diese Topologie wurden zwei 2911 ISRs mit Version 15.1(4)M4 für DMVPN Phase 1 konfiguriert: eine als Hub und eine als Spoke. Ethernet0/0 wurde als "Internet"-Schnittstelle auf jedem Router verwendet. Die vier Loopback-Schnittstellen werden so konfiguriert, dass sie lokale Netzwerke simulieren, die am Hub- oder Spoke-Standort leben. Da es sich um eine DMVPN

Phase 1-Topologie mit nur einem Spoke handelt, wird der Spoke-Topologie mit einem Punkt-zu-Punkt-GRE-Tunnel anstelle eines Mehrpunkt-GRE-Tunnels konfiguriert. Für jeden Router wurde dieselbe Verschlüsselungskonfiguration (ISAKMP und IPSec) verwendet, um sicherzustellen, dass sie genau übereinstimmen.

Abbildung 1



Krypto

Dies ist auf dem Hub und dem Spoke identisch.

```
crypto isakmp policy 1
encr 3des
hash sha
authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set DMVPN-TSET esp-3des esp-sha-hmac
mode transport
crypto ipsec profile DMVPN-IPSEC
set transform-set DMVPN-TSET
```

Hub

```
interface Tunnel0
ip address 10.1.1.254 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication NHRPAUTH
```

```
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip tcp adjust-mss 1360
no ip split-horizon eigrp 1
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
end

interface Ethernet0/0
ip address 172.16.10.1 255.255.255.0
end

interface Loopback0
ip address 203.0.113.1 255.255.255.255
interface Loopback1
ip address 203.0.113.2 255.255.255.255
interface Loopback2
ip address 203.0.113.3 255.255.255.255
interface Loopback3
ip address 203.0.113.4 255.255.255.255

router eigrp 1
network 10.1.1.0 0.0.0.255
network 203.0.113.1 0.0.0.0
network 203.0.113.2 0.0.0.0
network 203.0.113.3 0.0.0.0
network 203.0.113.4 0.0.0.0
```

Spoke

```
interface Tunnel0
ip address 10.1.1.1 255.255.255.0
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map 10.1.1.254 172.16.10.1
ip nhrp network-id 1
ip nhrp nhs 10.1.1.254
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.16.10.1
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
end

interface Ethernet0/0
ip address 172.16.1.1 255.255.255.0
end

interface Loopback0
ip address 209.165.201.1 255.255.255.255
interface Loopback1
ip address 209.165.201.2 255.255.255.255
interface Loopback2
ip address 209.165.201.3 255.255.255.255
interface Loopback3
ip address 209.165.201.4 255.255.255.255

router eigrp 1
network 209.165.201.1 0.0.0.0
network 209.165.201.2 0.0.0.0
network 209.165.201.3 0.0.0.0
```

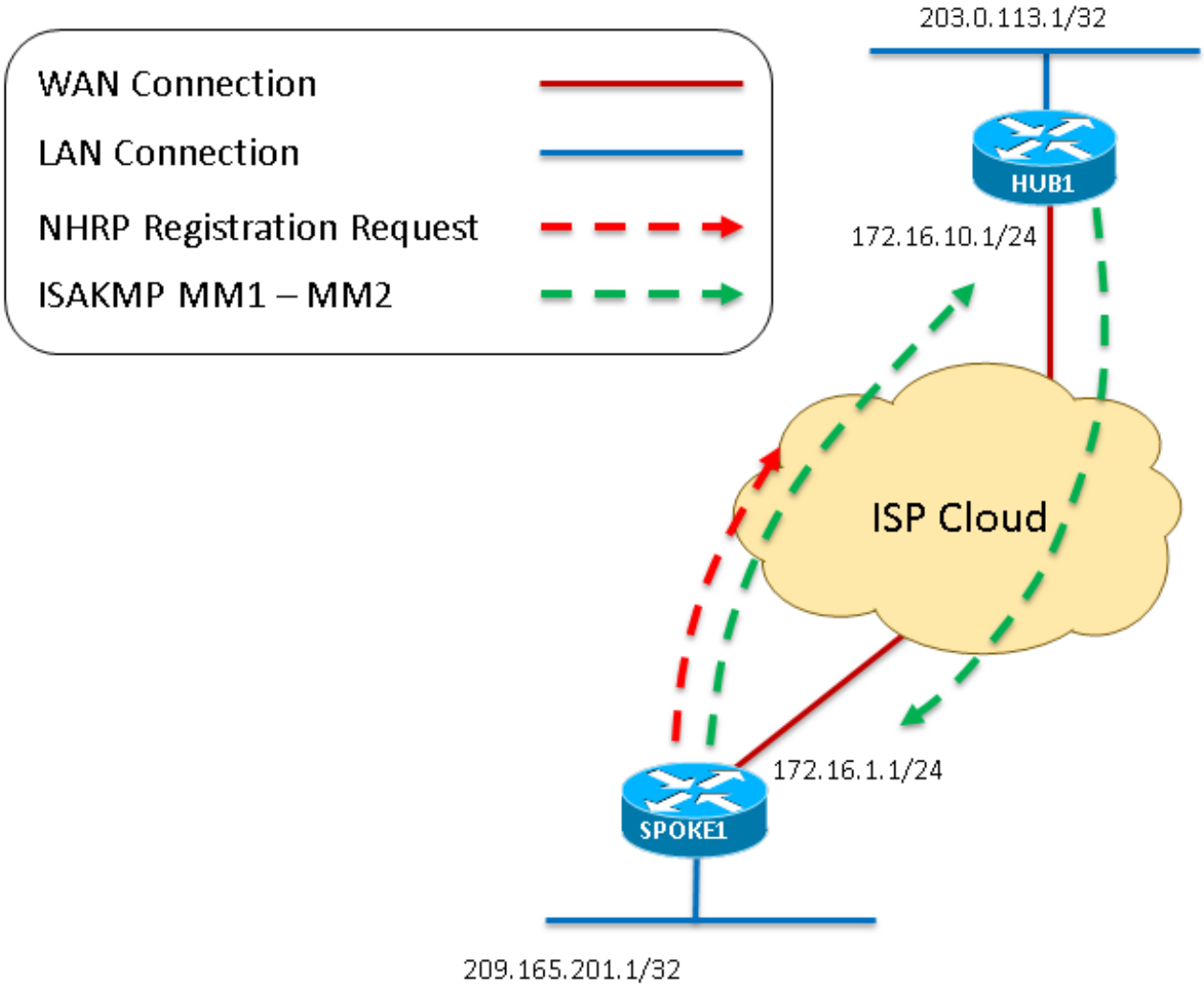
```
network 209.165.201.4 0.0.0.0
network 10.1.1.0 0.0.0.255
```

Debugger

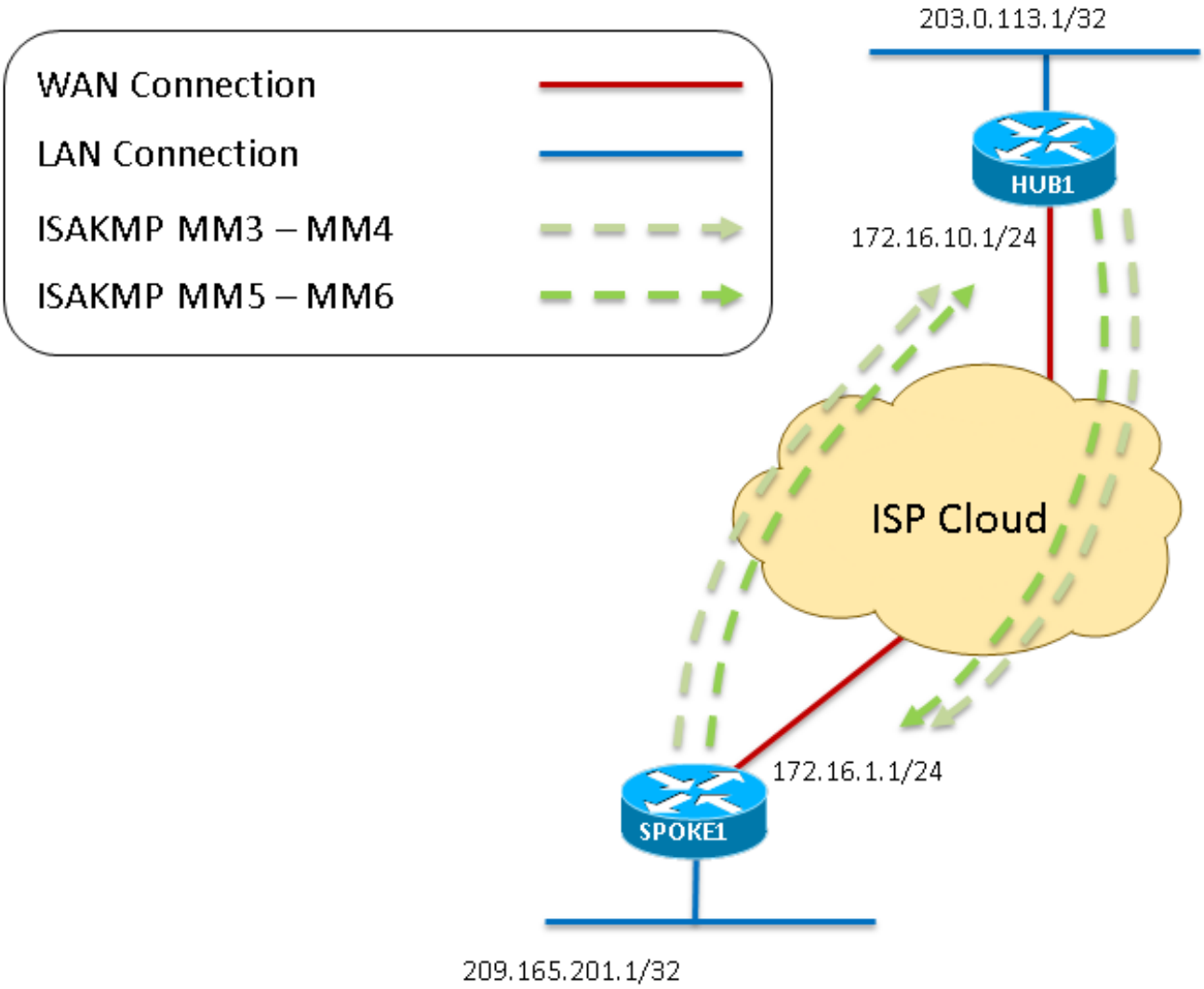
Paketfluss-Visualisierung

Dies ist eine Visualisierung des gesamten DMVPN-Paketflusses, wie in diesem Dokument beschrieben. Ausführlichere Debugging-Anweisungen, die die einzelnen Schritte erläutern, sind ebenfalls enthalten.

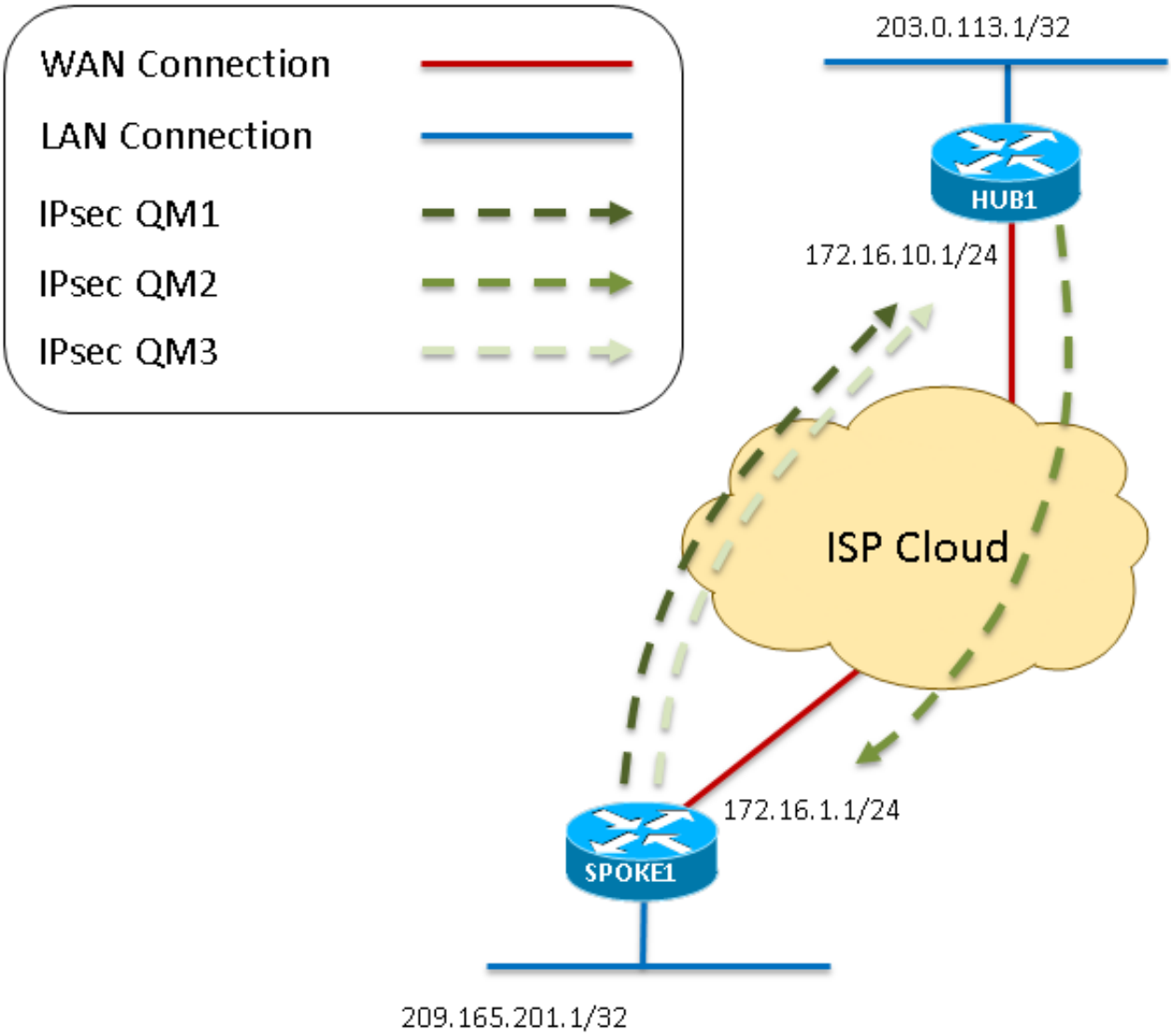
1. Wenn der Tunnel auf dem Spoke "no shutdown" (Kein Herunterfahren) ist, wird eine NHRP-Registrierungsanfrage generiert, die den DMVPN-Prozess startet. Da die Konfiguration des Hub vollständig dynamisch ist, muss der Spoke der Endpunkt sein, der die Verbindung initiiert.
2. Die NHRP-Registrierungsanforderung wird dann in GRE gekapselt, wodurch der Krypto-Prozess gestartet wird.
3. An diesem Punkt wird die erste ISAKMP-Hauptmodus-Meldung - ISAKMP MM1 - vom Spoke an den Hub auf dem UDP500-Port gesendet.
4. Der Hub empfängt und verarbeitet MM1 und reagiert mit ISAKMP MM2, da er über eine entsprechende ISAKMP-Richtlinie verfügt.
   Abbildung 2 - bezieht sich auf die Schritte 1 bis 4



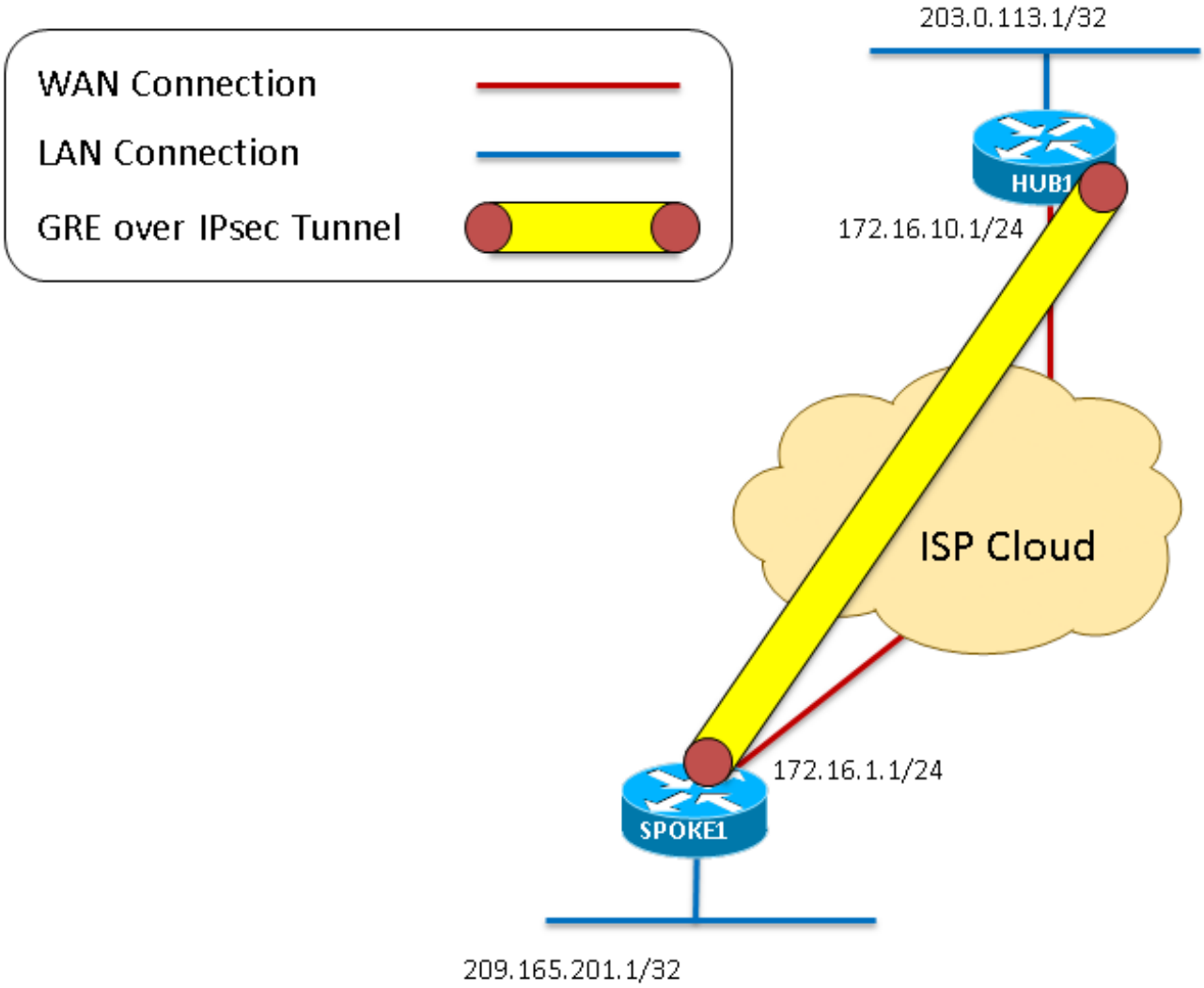
5. Sobald der Spoke den MM2 empfängt, reagiert er mit MM3. Wie bei MM1 bestätigt der Spoke, dass die erhaltene ISAKMP-Richtlinie gültig ist.
6. Der Hub empfängt MM3 und antwortet mit MM4.
7. An diesem Punkt der ISAKMP-Aushandlung reagiert der Spoke möglicherweise auf Port UDP4500, wenn NAT im Transitpfad erkannt wird. Wird jedoch keine NAT erkannt, setzt Spoke fort und sendet MM5 auf UDP500. Schließlich antwortet der Hub mit MM6, um den Hauptmodus-Austausch abzuschließen.
   Abbildung 3 - bezieht sich auf die Schritte 5 bis 7



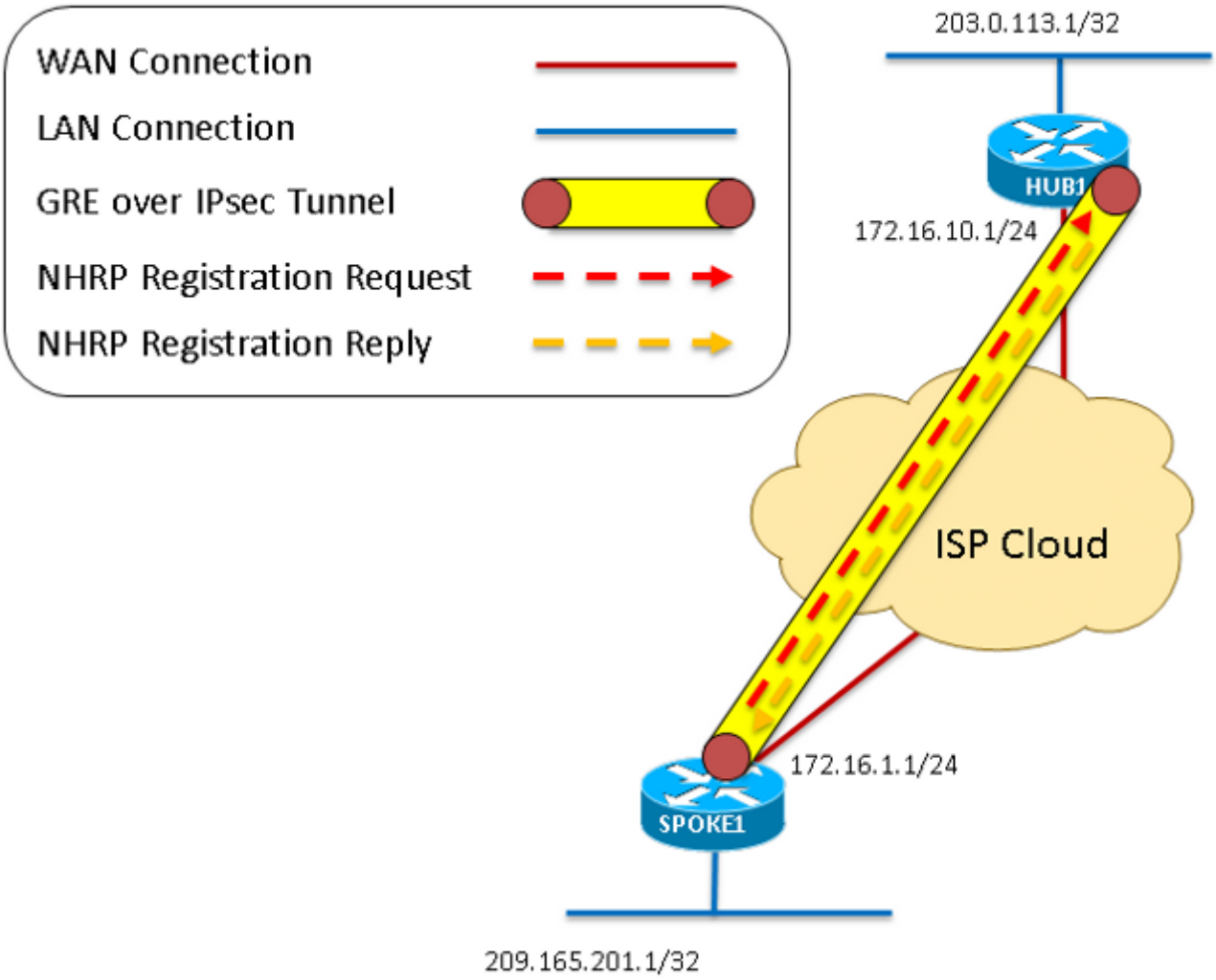
8. Sobald der Spoke MM6 vom Hub empfängt, sendet er QM1 an den Hub auf dem UDP500, um den Quick Mode zu starten.
9. Der Hub empfängt QM1 und antwortet mit QM2, da alle empfangenen Attribute akzeptiert werden. An diesem Punkt erstellt der Hub die Phase-2-SAs für diese Sitzung.
10. Als letzter Schritt der Schnellmodus-Aushandlung wird QM2 vom Spoke empfangen. Der Spoke erstellt dann die SAs der Phase 2 und sendet QM3 als Antwort. Damit ist die ISAKMP- und IPSec-Aushandlung abgeschlossen. Es gibt jetzt eine IPSec-Sitzung, die den GRE-Datenverkehr zwischen diesen beiden Peers verschlüsselt.
    Abbildung 4 - bezieht sich auf die Schritte 8 bis 10



11. Nachdem die Crypto-Sitzung aktiviert ist und Datenverkehr weitergeleitet werden kann, werden diese Pakete in der GRE über den IPSec-Tunnel gekapselt.
    Abbildung 5 - bezieht sich auf Schritt
    11



12. Wie in den ersten Schritten gezeigt, generiert Spoke einen NHRP-Registrierungsantrag, der über den IPSec-Tunnel über die GRE gesendet wird.
13. Der Hub empfängt die NHRP-Registrierungsanfragen und sendet eine NHRP-Registrierungsantwort, sobald bestätigt wird, dass der Spoke über eine gültige Tunnel- und Nonbroadcast Multiaccess (NBMA)-Adresse verfügt. Der Spoke erhält diese NHRP-Registrierungsantwort, die den Registrierungsvorgang abschließt.
    Abbildung 6 - bezieht sich auf die Schritte 12 bis 13



Diese Debuggen sind das Ergebnis, wenn der Befehl **debug dmvpn für alle** Befehle auf den Hub-and-Spoke-Routern eingegeben wird. Dieser Befehl aktiviert diese Gruppe von Debuggen:

```
Spoke1#debug dmvpn all all
DMVPN all level debugging is on
Spoke1#show debug


NHRP:
NHRP protocol debugging is on
NHRP activity debugging is on
NHRP extension processing debugging is on
NHRP cache operations debugging is on
NHRP routing debugging is on
NHRP rate limiting debugging is on
NHRP errors debugging is on
IKEV2:
IKEV2 error debugging is on
IKEV2 terse debugging is on
IKEV2 event debugging is on
IKEV2 packet debugging is on
IKEV2 detail debugging is on



Cryptographic Subsystem:
Crypto ISAKMP debugging is on
Crypto ISAKMP Error debugging is on
Crypto IPSEC debugging is on
```

```
Crypto IPSEC Error debugging is on
Crypto secure socket events debugging is on
Tunnel Protection Debugs:
Generic Tunnel Protection debugging is on
DMVPN:
DMVPN error debugging is on
DMVPN UP/DOWN event debugging is on
DMVPN detail debugging is on
DMVPN packet debugging is on
DMVPN all level debugging is on
```

Debuggen mit Erläuterung

Da es sich um eine Konfiguration handelt, in der IPSec implementiert ist, werden alle ISAKMP- und IPSec-Debugging-Meldungen angezeigt. Wenn keine Krypto-Funktion konfiguriert ist, ignorieren Sie alle DebuggingInnen, die mit "IPsec" oder "ISAKMP" beginnen.

HUB-DEBUG-ERLÄUTERUNG	DEBUGS IN FOLGE	ERLÄUT
Diese ersten Debug-Meldungen werden durch einen Befehl **no shutdown** generiert, der auf der Tunnelschnittstelle eingegeben wurde. Nachrichten werden durch die initiierten Krypto-, GRE- und NHRP-Dienste generiert. Beim Hub wird ein NHRP-Registrierungsfehler angezeigt, da kein Next-Hop-Server (NHS) konfiguriert ist (der Hub ist der NHS für unsere DMVPN-Cloud). Dies ist zu erwarten.	IPSEC-IFC MGRE/Tu0: Tunnelstatus wird überprüft. **NHRP: if_up: Tunnel0 proto 0** IPSEC-IFC MGRE/Tu0: Tunnel kommt IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start bereits abgehört **%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP ist eingeschaltet.** **NHRP: Registrierung kann nicht gesendet werden - keine NHSs konfiguriert** %LINK-3-UPDOWN: Interface Tunnel0 (Schnittstellentunnel0, Status geändert, hochgefahren) NHRP: if_up: Tunnel0 proto 0 NHRP: Registrierung kann nicht gesendet werden - keine NHSs konfiguriert IPSEC-IFC MGRE/Tu0: Tunnel kommt IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start bereits abgehört **%LINEPROTO-5-UPDOWN: Leitungsprotokoll auf Interface Tunnel0 (Schnittstellentunnel0), Status auf up** IPSEC-IFC GRE/Tu0: Tunnelstatus wird überprüft. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Verbindungssuche zurückgegeben 0 **IPSEC-IFC GRE/Tu0: crypto_ss_listen_start bereits abgehört** **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Öffnen eines Sockels mit dem Profil DMVPN-IPSEC** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Verbindungssuche zurückgegeben 0 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Sofortiges Auslösen des Tunnels IPSEC-IFC GRE/Tu0: Tunnel0-Tunnelschnittstelle zur freigegebenen Liste hinzufügen **NHRP: if_up: Tunnel0 proto 0** **NHRP: Tunnel0: Cache-Add für Ziel 10.1.1.254/32 Next-Hop 10.1.1.254**	Diese erste werden dur **shutdown** g Tunnelschr wurde. Nac initiierten K Diensten ge Darüber hir Server sein einen Eintra NBMA- und

172,16,10,1
IPSEC-IFC GRE/Tu0: Tunnel kommt
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Verbindungssuche zurückgegeben 961D220
IPSEC-IFC GRE/Tu0: crypto_ss_listen_start bereits abgehört
IPSEC-IFC GRE/Tu0: crypto_ss_listen_start bereits abgehört
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Öffnen eines Sockels mit dem Profil DMVPN-IPSEC
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Verbindungssuche zurückgegeben 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Socket wird bereits geöffnet. Ignorieren.
CRYPTO_SS(TUNNEL SEC): Anwendung begann zu hören
Einfügung der Karte in mapdb AVL fehlgeschlagen, Map + Ass Paar existiert bereits auf der mapdb
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP ist eingeschaltet.
CRYPTO_SS(TUNNEL SEC): Aktiv offen, Socketinformationen: local 172.16.1.1 172.16.1.1/255.255.255.255/0, remote 172.16.10.1 172.16.10.1/255.255.255.255/0, , ifc Tu0
BEGINN DER ISAKMP-VERHANDLUNG (PHASE I)
IPSEC(recalculate_mtu): sadb_root 94EFDC0 mtu auf 1500 zurücksetzen
IPSEC(sa_request): ,
(Schlüssel eng. msg.) OUTBOUND local= 172.16.1.1:500, remote= 172.16.10.1:500,
local_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),
remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),
protocol= ESP, transformation= esp-3des esp-sha-hmac (Transport),
lebensdur= 3600s und 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
ISAKMP:(0) Das SA-Anforderungsprofil ist (NULL).
ISAKMP: Peer-Struktur für 172.16.10.1 erstellt, Peer-Port 500
ISAKMP: Neuer Peer erstellt Peer = 0x95F6858 Peer_Handle = 0x8000004
ISAKMP: Sperren der Peer-Struktur 0x95F6858, recount 1 für isakmp_initiator
ISAKMP: Lokaler Port 500, Remote-Port 500
ISAKMP: Setzen Sie den neuen Knoten 0 auf QM_IDLE
ISAKMP:(0):Als erfolgreich einfügen sa = 8A26FB0
ISAKMP:(0):Kann den aggressiven Modus nicht starten und versucht, den Hauptmodus auszuwählen.
ISAKMP:(0):gefundener vorinstallierter Peer-Schlüssel, der mit 172.16.10.1 übereinstimmt

Der erste S
"no shutdo
Verschlüss
starten. Hie
SA-Anforde
aggressive
schlägt bei
Hauptmodu
Modus auf
konfiguriert
Der Spoke
und sendet
Meldung, M
ISAKMP-St
IKE_READ
Die NAT-T-
werden zur
Überbrücku
Diese Meld
der Aushar
erwartet, u
implementi
Meldungen
sind auch c
erwarten.

	ISAKMP:(0) konstruierte NAT-T Vendor-RFC3947-ID ISAKMP:(0) konstruierte NAT-T Vendor-07-ID ISAKMP:(0) konstruierte NAT-T Vendor-03-ID ISAKMP:(0) konstruierte NAT-T Vendor-02 ID **ISAKMP:(0):Eingabe = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM** **ISAKMP:(0):Old State = IKE_READY New State = IKE_I_MM1**
	ISAKMP:(0) Start Main Mode Exchange **ISAKMP:(0) Senden des Pakets an 172.16.10.1 my_port 500 peer_port 500 (I) MM_NO_STATE** ISAKMP:(0):Senden eines IKE-IPv4-Pakets. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Verbindungssuche zurückgegeben 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Gute Socket-fähige Nachricht
Wenn der Tunnel des Spokes "no shutdown" (Kein Herunterfahren) ist, erhält der Hub die Meldung IKE NEW SA (Hauptmodus 1) auf Port 500. Als Responder erstellt der Hub eine ISAKMP Security Association (SA). Der ISAKMP-Status wechselt von IKE_READY zu IKE_R_MM1.	**ISAKMP (0): empfangenes Paket von 172.16.1.1 dport 500 sport 500 Global (N) NEW SA** **ISAKMP: Peer-Struktur für 172.16.1.1 erstellt, Peer-Port 500** ISAKMP: Neuer Peer erstellt = 0x8CACD00 Peer_Handle = 0x80000003 ISAKMP: Sperren der Peer-Struktur 0x8CACD00, RefCount 1 für crypto_isakmp_process_block ISAKMP: Lokaler Port 500, Remote-Port 500 **ISAKMP:(0):Als erfolgreich einfügen sa = 6A5BDE8** ISAKMP:(0):Eingabe = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Old State = IKE_READY New State = IKE_R_MM1**
Die erhaltene Meldung IKE-Hauptmodus 1 wird verarbeitet. Der Hub stellt fest, dass der Peer über passende ISAKMP-Attribute verfügt und in die soeben erstellte ISAKMP SA gefüllt wird. Die Meldungen zeigen, dass der Peer 3DES-CBC für die Verschlüsselung, das Hashing von SHA, Diffie Hellman (DH)-Gruppe 1, den Pre-Shared Key für die Authentifizierung und die standardmäßige SA-Lebensdauer von 86400 Sekunden (0x0 0x1 0x51 0x80 = 0x15180 = 80 Sekunden verwendet). Der ISAKMP-Status lautet weiterhin IKE_R_MM1, da keine Antwort an den Spoke-Server gesendet wurde. Die NAT-T-Anbieter-ID-Nachrichten werden zur Erkennung und Überbrückung von NAT verwendet. Diese Meldungen werden während	ISAKMP:(0) Verarbeitung der SA-Nutzlast. Nachrichten-ID = 0 ISAKMP:(0) Nutzlast der Verarbeitungsanbieter-ID **ISAKMP:(0) Vendor-ID scheint Unity/DPD zu sein, aber 69 Diskrepanzen stimmen nicht überein.** **ISAKMP (0): Vendor-ID: NAT-T RFC 3947** ISAKMP:(0) Nutzlast der Verarbeitungsanbieter-ID ISAKMP:(0) Anbieter-ID scheint Unity/DPD zu sein, aber 245 Divergenzen sind erheblich. ISAKMP (0): Anbieter-ID: NAT-T v7 ISAKMP:(0) Nutzlast der Verarbeitungsanbieter-ID ISAKMP:(0) Vendor-ID scheint Unity/DPD zu sein, aber 157 Divergenzen treten auf ISAKMP:(0) Anbieter-ID: NAT-T v3 ISAKMP:(0) Nutzlast der Verarbeitungsanbieter-ID ISAKMP:(0) Vendor-ID scheint Unity/DPD zu sein, aber 123 Divergenzen treten auf ISAKMP:(0) Anbieter-ID: NAT-T v2 **ISAKMP:(0):gefundener vorinstallierter Peer-Schlüssel, der mit 172.16.1.1 übereinstimmt** **ISAKMP:(0) Lokaler vorinstallierter Schlüssel gefunden**

der Aushandlung von ISAKMP erwartet, unabhängig davon, ob NAT implementiert ist oder nicht. Ähnliche Meldungen werden für Dead Peer Detection (DPD) angezeigt.	ISAKMP: Scanning-Profile für ... **ISAKMP:(0):Überprüfen von ISAKMP-Umwandlung 1 gegen Richtlinie der Priorität 1** **ISAKMP: Verschlüsselung 3DES-CBC** **ISAKMP: Hash SHA** **ISAKMP: Standardgruppe 1** **ISAKMP: auth Pre-Share** **ISAKMP: Life Type in Sekunden** **ISAKMP: Lebensdauer (VPI) von 0x0 0x1 0x51 0x80** **ISAKMP:(0):Atts sind akzeptabel. Nächste Nutzlast: 0** **ISAKMP:(0):Akzeptable Attraktionen:tatsächliche Lebensdauer: 0** **ISAKMP:(0):Akzeptable Attraktionen:Life: 0** **ISAKMP:(0):Fill atts in sa vpi_length:4** **ISAKMP:(0):Fill atts in sa life_in_seconds:86400** **ISAKMP:(0):Zurückgeben der tatsächlichen Lebensdauer: 86400** **ISAKMP:(0)::Started Lifetime Timer: 86400** ISAKMP:(0) Nutzlast der Verarbeitungsanbieter-ID ISAKMP:(0) Vendor-ID scheint Unity/DPD zu sein, aber 69 Diskrepanzen stimmen nicht überein. ISAKMP (0): Vendor-ID: NAT-T RFC 3947 ISAKMP:(0) Nutzlast der Verarbeitungsanbieter-ID ISAKMP:(0) Anbieter-ID scheint Unity/DPD zu sein, aber 245 Divergenzen sind erheblich. ISAKMP (0): Anbieter-ID: NAT-T v7 ISAKMP:(0) Nutzlast der Verarbeitungsanbieter-ID ISAKMP:(0) Vendor-ID scheint Unity/DPD zu sein, aber 157 Divergenzen treten auf ISAKMP:(0) Anbieter-ID: NAT-T v3 ISAKMP:(0) Nutzlast der Verarbeitungsanbieter-ID ISAKMP:(0) Vendor-ID scheint Unity/DPD zu sein, aber 123 Divergenzen treten auf ISAKMP:(0) Anbieter-ID: NAT-T v2 ISAKMP:(0):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM1
MM_SA_SETUP (Hauptmodus 2) wird an den Spoke gesendet, wodurch bestätigt wird, dass MM1 empfangen und als gültiges ISAKMP-Paket akzeptiert wurde. Der ISAKMP-Status ändert sich von IKE_R_MM1 zu IKE_R_MM2.	ISAKMP:(0) konstruierte NAT-T Vendor-RFC3947-ID **ISAKMP:(0) Senden des Pakets an 172.16.1.1 my_port 500 peer_port 500 (R) MM_SA_SETUP** ISAKMP:(0):Senden eines IKE-IPv4-Pakets. ISAKMP:(0):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM2**
	ISAKMP (0): empfangenes Paket von 172.16.10.1 dport 500 sport 500 Global (I) MM_NO_STATE **ISAKMP:(0):Eingabe = IKE_MESG_FROM_PEER, IKE_MM_EXCH** **ISAKMP:(0):Old State = IKE_I_MM1 New State = IKE_I_MM2**

Als Antwort
die an den
kommt MM
wird, dass
Die empfar
Mode 2 wir

	ISAKMP:(0) Verarbeitung der SA-Nutzlast. Nachrichten-ID = 0 ISAKMP:(0) Nutzlast der Verarbeitungsanbieter-ID **ISAKMP:(0) Vendor-ID scheint Unity/DPD zu sein, aber 69 Diskrepanzen stimmen nicht überein.** ISAKMP (0): Vendor-ID: NAT-T RFC 3947 ISAKMP:(0):gefundener vorinstallierter Peer-Schlüssel, der mit 172.16.10.1 übereinstimmt ISAKMP:(0) Lokaler vorinstallierter Schlüssel gefunden ISAKMP: Scanning-Profile für ... **ISAKMP:(0):Überprüfen von ISAKMP-Umwandlung 1 gegen Richtlinie der Priorität 1** **ISAKMP: Verschlüsselung 3DES-CBC** **ISAKMP: Hash SHA** **ISAKMP: Standardgruppe 1** **ISAKMP: auth Pre-Share** **ISAKMP: Life Type in Sekunden** **ISAKMP: Lebensdauer (VPI) von 0x0 0x1 0x51 0x80** **ISAKMP:(0):Atts sind akzeptabel. Nächste Nutzlast: 0** **ISAKMP:(0):Akzeptable Attraktionen:tatsächliche Lebensdauer: 0** **ISAKMP:(0):Akzeptable Attraktionen:Life: 0** **ISAKMP:(0):Fill atts in sa vpi_length:4** **ISAKMP:(0):Fill atts in sa life_in_seconds:86400** **ISAKMP:(0):Zurückgeben der tatsächlichen Lebensdauer: 86400** **ISAKMP:(0)::Started Lifetime Timer: 86400**	stellt fest, d passende I und diese A erstellte ISA Paket zeigt CBC für Ve von SHA, D Gruppe 1, I Authentifizi standardmä von 86400 0x80 = 0x1 verwendet Zusätzlich z gibt es eine festzustelle verwendet. Der ISAKM IKE_I_MM1
	ISAKMP:(0) Nutzlast der Verarbeitungsanbieter-ID ISAKMP:(0) Vendor-ID scheint Unity/DPD zu sein, aber 69 Diskrepanzen stimmen nicht überein. ISAKMP (0): Vendor-ID: NAT-T RFC 3947 ISAKMP:(0):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM2 **ISAKMP:(0) Senden des Pakets an 172.16.10.1 my_port 500 peer_port 500 (I) MM_SA_SETUP** ISAKMP:(0):Senden eines IKE-IPv4-Pakets. ISAKMP:(0):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM3**	MM_SA_SE wird an der bestätigt, d empfangen möchte. Der ISAKM IKE_I_MM2
MM_SA_SETUP (Hauptmodus 3) wird vom Hub empfangen. Der Hub kommt zu dem Schluss, dass der Peer ein anderes Cisco IOS-Gerät ist und keine NAT für uns oder unseren Peer erkannt wird. Der ISAKMP-Status wechselt von IKE_R_MM2 zu IKE_R_MM3.	**ISAKMP (0): empfangenes Paket von 172.16.1.1 dport 500 sport 500 Global (R) MM_SA_SETUP** ISAKMP:(0):Eingabe = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Old State = IKE_R_MM2 New State = IKE_R_MM3** ISAKMP:(0) Verarbeiten der KE-Nutzlast. Nachrichten-	

	ID = 0 ISAKMP:(0) NONCE-Payload wird verarbeitet. Nachrichten-ID = 0 **ISAKMP:(0):gefundener vorinstallierter Peer-Schlüssel, der mit 172.16.1.1 übereinstimmt** ISAKMP: (1002) Nutzlast der Verarbeitungsanbieter-ID ISAKMP: (1002) Anbieter-ID ist DPD ISAKMP: (1002) Nutzlast der Verarbeitungsanbieter-ID **ISAKMP: (1002) mit einer anderen IOS-Box!** ISAKMP: (1002) Nutzlast der Verarbeitungsanbieter-ID ISAKMP: (1002) Anbieter-ID scheint Unity/DPD zu sein, aber 225 Divergenzen sind erheblich. ISAKMP: (1002) Anbieter-ID: XAUTH ISAKMP:Empfangs-Payload-Typ 20 **ISAKMP (1002): Sein Hash stimmt nicht überein - dieser Knoten außerhalb von NAT** ISAKMP:Empfangs-Payload-Typ 20 **ISAKMP (1002): Keine NAT für sich selbst oder Peer gefunden** ISAKMP:(1002):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Alter Zustand = IKE_R_MM3 Neuer Zustand = IKE_R_MM3	
MM_KEY_EXCH (Hauptmodus 4) wird vom Hub gesendet. Der ISAKMP-Status ändert sich von IKE_R_MM3 zu IKE_R_MM4.	**ISAKMP: (1002) Senden des Pakets an 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH** ISAKMP:(1002):Senden eines IKE-IPv4-Pakets. ISAKMP:(1002):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Old State = IKE_R_MM3 New State = IKE_R_MM4**	
	ISAKMP (0): empfangenes Paket von 172.16.10.1 dport 500 sport 500 Global (I) MM_SA_SETUP ISAKMP:(0):Eingabe = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP:(0):Old State = IKE_I_MM3 New State = IKE_I_MM4**	MM_SA_SE wird von Sp Spoke-Sitz Schluss, da Cisco IOS- für uns ode wird.
	ISAKMP:(0) Verarbeiten der KE-Nutzlast. Nachrichten-ID = 0 ISAKMP:(0) NONCE-Payload wird verarbeitet. Nachrichten-ID = 0 **ISAKMP:(0):gefundener vorinstallierter Peer-Schlüssel, der mit 172.16.10.1 übereinstimmt** ISAKMP: (1002) Nutzlast der Verarbeitungsanbieter-ID ISAKMP: (1002) Anbieter-ID ist Unity ISAKMP: (1002) Nutzlast der Verarbeitungsanbieter-ID ISAKMP: (1002) Anbieter-ID ist DPD ISAKMP: (1002) Nutzlast der Verarbeitungsanbieter-ID **ISAKMP: (1002) mit einer anderen IOS-Box!** ISAKMP:Empfangs-Payload-Typ 20 **ISAKMP (1002): Sein Hash stimmt nicht überein - dieser Knoten außerhalb von NAT** ISAKMP:Empfangs-Payload-Typ 20	Der ISAKM IKE_I_MM3

ISAKMP (1002): Keine NAT für sich selbst oder Peer gefunden
ISAKMP:(1002):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Old State = IKE_I_MM4 New State = IKE_I_MM4
ISAKMP:(1002):Erster Kontakt senden
ISAKMP:(1002):SA führt eine vorinstallierte Schlüsselauthentifizierung mithilfe des ID-Typs ID_IPV4_ADDR durch.
ISAKMP (1002): ID-Nutzlast
Next-Payload: 8
Typ: 1
Adresse: 172,16,1,1
Protokoll: 17
Hafen: 500
Länge: 12
ISAKMP:(1002):Gesamtlänge der Payloads: 12
ISAKMP: (1002) Senden des Pakets an 172.16.10.1 my_port 500 peer_port 500 (I) MM_KEY_EXCH
ISAKMP:(1002):Senden eines IKE-IPv4-Pakets.
ISAKMP:(1002):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1002):Old State = IKE_I_MM4 New State = IKE_I_MM5

MM_KEY_E
wird vom S
Der ISAKM
IKE_I_MM4

MM_KEY_EXCH (Hauptmodus 5) wird vom Hub empfangen.
Der ISAKMP-Status wechselt von IKE_R_MM4 zu IKE_R_MM5.
Außerdem wird die "Peer Matches *none* der Profile" angezeigt, da kein ISAKMP-Profil vorhanden ist. Da dies der Fall ist, verwendet ISAKMP kein Profil.

ISAKMP (1002): empfangenes Paket von 172.16.1.1 dport 500 sport 500 Global (R) MM_KEY_EXCH
ISAKMP:(1002):Eingabe = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(1002):Old State = IKE_R_MM4 New State = IKE_R_MM5

ISAKMP: (1002) Nutzlast der Verarbeitungs-ID.
Nachrichten-ID = 0
ISAKMP (1002): ID-Nutzlast
Next-Payload: 8
Typ: 1
Adresse: 172,16,1,1
Protokoll: 17
Hafen: 500
Länge: 12
ISAKMP:(0): Peer-Übereinstimmungen *Keine* der Profile
ISAKMP: (1002) Verarbeitung der HASH-Nutzlast.
Nachrichten-ID = 0
ISAKMP: (1002) NOTIFY INITIAL_CONTACT-Protokoll 1 verarbeiten
spi 0, Nachrichten-ID = 0, sa = 0x6A5BDE8
ISAKMP:(1002):SA-Authentifizierungsstatus:
authentifiziert
ISAKMP:(1002):SA wurde mit 172.16.1.1 authentifiziert
ISAKMP:(1002):SA-Authentifizierungsstatus:

authentifiziert
ISAKMP: (1002) Erstkontakt bearbeiten, Herunterfahren vorhandener SAs der Phasen 1 und 2 mit lokalem 172.16.10.1 Remote-Port 172.16.1.1 500
ISAKMP: Es wird versucht, einen Peer 172.16.10.1/172.16.1.1/500/, einzufügen und erfolgreich 8CACD00 eingefügt.
ISAKMP:(1002):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Alter Zustand = IKE_R_MM5 Neuer Status = IKE_R_MM5

IPSEC(key_engine): Warteschlangenereignis mit 1 KMI-Meldung(en)
ISAKMP:(1002):SA führt eine vorinstallierte Schlüsselauthentifizierung mithilfe des ID-Typs ID_IPV4_ADDR durch.
ISAKMP (1002): ID-Nutzlast
Next-Payload: 8
Typ: 1
Adresse: 172,16,10,1
Protokoll: 17
Hafen: 500
Länge: 12
ISAKMP:(1002):Gesamtlänge der Payloads: 12

Das letzte MM_KEY_EXCH-Paket (Hauptmodus 6) wird vom Hub gesendet. Damit ist die Phase-1-Aushandlung abgeschlossen, die besagt, dass dieses Gerät für Phase 2 bereit ist (IPSec Quick Mode). Der ISAKMP-Status wechselt von IKE_R_MM5 zu IKE_P1_COMPLETE.

ISAKMP: (1002) Senden des Pakets an 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH
ISAKMP:(1002):Senden eines IKE-IPv4-Pakets.
ISAKMP:(1002):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1002):Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE

ISAKMP:(1002):Eingabe = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1002):Alter Status = IKE_P1_COMPLETE Neuer Status = IKE_P1_COMPLETE
ISAKMP (1002): empfangenes Paket von 172.16.10.1 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP: (1002) Nutzlast der Verarbeitungs-ID. Nachrichten-ID = 0
ISAKMP (1002): ID-Nutzlast
Next-Payload: 8
Typ: 1
Adresse: 172,16,10,1
Protokoll: 17
Hafen: 500
Länge: 12
ISAKMP:(0): Peer-Übereinstimmungen *Keine* der Profile
ISAKMP: (1002) Verarbeitung der HASH-Nutzlast. Nachrichten-ID = 0
ISAKMP:(1002):SA-Authentifizierungsstatus:

Das letzte I
(Hauptmod
empfangen
Aushandlu
besagt, das
2 bereit ist
Der ISAKM
IKE_I_MM5
sofort zu IK
Außerdem
none der
ISAKMP-Pr
der Fall ist,
Profil.

authentifiziert
ISAKMP:(1002):SA wurde mit 172.16.10.1 authentifiziert
ISAKMP: Es wird versucht, einen Peer 172.16.1.1/172.16.10.1/500/, einzufügen und erfolgreich 95F6858 eingefügt.
ISAKMP:(1002):Eingabe = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(1002):Alter Zustand = IKE_I_MM5 Neuer Zustand = IKE_I_MM6

ISAKMP:(1002):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Alter Zustand = IKE_I_MM6 Neuer Status = IKE_I_MM6

ISAKMP:(1002):Eingabe = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1002):Alter Zustand = IKE_I_MM6 Neuer Status = IKE_P1_COMPLETE

ENDE DER ISAKMP-VERHANDLUNG (PHASE I), BEGINN DER IPSEC-VERHANDLUNG

ISAKMP:(1002):start Quick Mode Exchange, M-ID of 3464373979
Der Quick I
Austausch
Spokes ser
Nachricht a
ISAKMP:(1002):QM Initiator erhält spi
ISAKMP: (1002) Senden des Pakets an 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1002):Senden eines IKE-IPv4-Pakets.
ISAKMP:(1002):Knoten 3464373979, Eingabe = IKE_MESG_INTERNAL, IKE_INIT_QM
ISAKMP:(1002):Alter Status = IKE_QM_READY New State = IKE_QM_I_QM1
ISAKMP:(1002):Eingabe = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1002):Alter Status = IKE_P1_COMPLETE Neuer Status = IKE_P1_COMPLETE

Der Hub empfängt das erste QM-Paket (Quick Mode), das das IPSec-Angebot enthält. Die empfangenen Attribute geben Folgendes an: encaps-Flag auf 2 (Transportmodus, Flag 1 wäre Tunnelmodus), standardmäßige SA-Lebensdauer von 3600 Sekunden und 4608000 Kilobyte (0x465000 in Hex), HMAC-SHA für Authentifizierung und 3DES für Verschlüsselung festgelegt. Da es sich um dieselben Attribute handelt, die in der lokalen Konfiguration festgelegt wurden, wird das Angebot akzeptiert und die Shell einer IPSec SA erstellt. Da diesen noch keine SPI-Werte (Security Parameter Index) zugeordnet sind, handelt es

ISAKMP (1002): empfangenes Paket von 172.16.1.1 dport 500 sport 500 Global (R) QM_IDLE
ISAKMP: Setzen Sie den neuen Knoten -830593317 auf QM_IDLE.
ISAKMP: (1002) Verarbeitung der HASH-Nutzlast. Nachrichten-ID = 3464373979
ISAKMP: (1002) Verarbeitung der SA-Nutzlast. Nachrichten-ID = 3464373979
ISAKMP:(1002):Überprüfen von IPSec-Vorschlag 1
ISAKMP: umwandeln 1, ESP_3DES
ISAKMP: Attribute in Transformation:
ISAKMP: Encaps sind 2 (Transport)
ISAKMP: SA-Lebensdauer (in Sekunden)
ISAKMP: SA-Lebensdauer (Basic) von 3600
ISAKMP: SA-Lebensdauer in Kilobyte
ISAKMP: SA-Lebensdauer (VPI) von 0x0 0x46 0x50 0x0
ISAKMP: Authentifizierer ist HMAC-SHA

sich um eine Shell eines SA, das noch nicht zum Übergeben von Datenverkehr verwendet werden kann.	**ISAKMP:(1002):Atts sind zulässig.** IPSEC(validate_vorschlag_request): Vorschlag Teil 1 IPSEC(validate_vorschlag_request): Vorschlagsteil 1, **(Schlüssel eng. msg.) EINGEHEND lokal= 172.16.10.1:0, remote= 172.16.1.1:0,** **local_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),** **remote_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),** **protocol= ESP, transformation= NONE (Transport),** **lebensdur= 0s und 0kb,** **spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0**
Dies sind nur allgemeine IPSec-Service-Nachrichten, die sagen, dass es ordnungsgemäß funktioniert.	IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Verbindungssuche zurückgegeben 0 IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start bereits abgehört **IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Öffnen eines Sockels mit dem Profil DMVPN-IPSEC** IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Verbindungssuche zurückgegeben 0 IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Sofortiges Auslösen des Tunnels IPSEC-IFC MGRE/Tu0: Tunnel0-Tunnelschnittstelle zur freigegebenen Liste hinzufügen IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): tunnel_protection_start_ausstehend_timer 8C93888 IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Good-Listen-Anforderung
Der Pseudo-crypto-Map-Eintrag wird für das IP-Protokoll 47 (GRE) von 172.16.10.1 (öffentliche Hub-Adresse) bis 172.16.1.1 (öffentliche Spoke-Adresse) erstellt. Ein IPSec SA/SPI wird sowohl für ein- als auch für ausgehenden Datenverkehr mit Werten aus dem akzeptierten Angebot erstellt.	Einfügung der Karte in mapdb AVL fehlgeschlagen, Map + Ass Paar existiert bereits auf der mapdb CRYPTO_SS(TUNNEL SEC): Passive offene Socket-Informationen: local 172.16.10.1 172.16.10.1/255.255.255.255/0, remote 172.16.1.1 172.16.1.1/255.255.255.255/0, prot 47, ifc Tu0 Crypto mapdb: Proxy-Übereinstimmung **src-Adresse: 172,16,10,1** **dst-Adresse: 172,16,1,1** **Protokoll: 47** src-Port: 0 dst-Port: 0 ISAKMP: (1002) NONCE-Payload wird verarbeitet. Nachrichten-ID = 3464373979 ISAKMP: (1002) Nutzlast der Verarbeitungs-ID. Nachrichten-ID = 3464373979 ISAKMP: (1002) Nutzlast der Verarbeitungs-ID. Nachrichten-ID = 3464373979 ISAKMP:(1002):QM-Responder erhält spi ISAKMP:(1002):Knoten 3464373979, Eingabe = IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP:(1002):Alter Status = IKE_QM_READY New State = IKE_QM_SPI_STARVE** **ISAKMP: (1002) Erstellen von IPSec SAs** **eingehende SA von 172.16.1.1 bis 172.16.10.1**

(f/i) 0/ 0
(Proxy 172.16.1.1 bis 172.16.10.1)
hat spi 0xDD2AC2B3 und conn_id 0
Lebensdauer von 3.600 Sekunden
Lebensdauer von 4608000 Kilobyte
Ausgehende SA von 172.16.10.1 bis 172.16.1.1
(f/i) 0/0
(Proxy 172.16.10.1 bis 172.16.1.1)
hat spi 0x82C3E0C4 und conn_id 0
Lebensdauer von 3.600 Sekunden
Lebensdauer von 4608000 Kilobyte

Die zweite QM-Nachricht, die vom Hub gesendet wird. Durch den IPSec-Dienst generierte Nachricht, die bestätigt, dass der Tunnelschutz auf Tunnel0 aktiviert ist.

ISAKMP: (1002) Senden des Pakets an 172.16.1.1 my_port 500 peer_port 500 (R) QM_IDLE
ISAKMP:(1002):Senden eines IKE-IPv4-Pakets.
ISAKMP:(1002):Knoten 3464373979, Eingabe = IKE_MESG_INTERNAL, IKE_GOT_SPI

Es wird eine weitere Meldung zur SA-Erstellung angezeigt, in der die Ziel-IPs, SPIs, Attribute für Transformationssätze und die Lebensdauer in Kilobyte und Sekunden verbleiben.

ISAKMP:(1002):Alter Zustand = IKE_QM_SPI_STARVE Neuer Status = IKE_QM_R_QM2
CRYPTO_SS(TUNNEL SEC): Vollständige Bindung der Anwendung an den Socket
IPSEC(key_engine): Warteschlangenereignis mit 1 KMI-Meldung(en)
Crypto mapdb: Proxy-Übereinstimmung
src-Adresse: 172,16,10,1
dst-Adresse: 172,16,1,1
Protokoll: 47
src-Port: 0
dst-Port: 0
IPSEC(crypto_ipsec_sa_find_ident_head): Wiederverbindung mit denselben Proxys und Peer 172.16.1.1
IPSEC(policy_db_add_ident): src 172.16.10.1, dest 172.16.1.1, dest_port 0

IPSEC(create_sa): als erstellt,
(sa) sa_dest= 172.16.10.1, sa_proto= 50,
sa_spi= 0xDD2AC2B3(3710567091),
sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 3
sa_life(k/sec)= (4536779/3600)
IPSEC(create_sa): als erstellt,
(sa) sa_dest= 172.16.1.1, sa_proto= 50,
sa_spi= 0x82C3E0C4(2193875140),
sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 4
sa_life(k/sec)= (4536779/3600)
IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): Tunnel0 ident 8B6A0E8 mit tun_decap_oce 6A648F0 aktualisieren
IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Verbindungssuche zurückgegeben 8C9388
IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Gute Socket-fähige Nachricht
IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1):

Verbindungssuche zurückgegeben 8C9388
IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): tunnel_protection_socket_up
IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Signalisierung NHRP
IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): MTU-Nachricht MTU 1458
IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Verbindungssuche zurückgegeben 8C9388
ISAKMP (1002): empfangenes Paket von 172.16.10.1 dport 500 sport 500 Global (I) QM_IDLE
ISAKMP: (1002) Verarbeitung der HASH-Nutzlast. Nachrichten-ID = 3464373979
ISAKMP: (1002) Verarbeitung der SA-Nutzlast. Nachrichten-ID = 3464373979
ISAKMP:(1002):Überprüfen von IPSec-Vorschlag 1
ISAKMP: umwandeln 1, ESP_3DES
ISAKMP: Attribute in Transformation:
ISAKMP: Encaps sind 2 (Transport)
ISAKMP: SA-Lebensdauer (in Sekunden)
ISAKMP: SA-Lebensdauer (Basic) von 3600
ISAKMP: SA-Lebensdauer in Kilobyte
ISAKMP: SA-Lebensdauer (VPI) von 0x0 0x46 0x50 0x0
ISAKMP: Authentifizierer ist HMAC-SHA
ISAKMP:(1002):Atts sind zulässig.
IPSEC(validate_vorschlag_request): Vorschlag Teil 1
IPSEC(validate_vorschlag_request): Vorschlagsteil 1,
(Schlüssel eng. msg.) EINGEHEND lokal= 172.16.1.1:0, remote= 172.16.10.1:0,
local_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),
remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),
protocol= ESP, transformation= NONE (Transport),
lebensdur= 0s und 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
Crypto mapdb: Proxy-Übereinstimmung
src-Adresse: 172,16,1,1
dst-Adresse: 172,16,10,1
Protokoll: 47
src-Port: 0
dst-Port: 0
ISAKMP: (1002) NONCE-Payload wird verarbeitet. Nachrichten-ID = 3464373979
ISAKMP: (1002) Nutzlast der Verarbeitungs-ID. Nachrichten-ID = 3464373979
ISAKMP: (1002) Nutzlast der Verarbeitungs-ID. Nachrichten-ID = 3464373979
ISAKMP: (1002) Erstellen von IPSec SAs
eingehende SA von 172.16.10.1 bis 172.16.1.1 (f/i) 0/ 0
(Proxy 172.16.10.1 bis 172.16.1.1)

Das Spoke
QM-Paket,
enthält. Die
vom Hub e
empfangen
Folgendes
(Transportr
Tunnelmod
Lebensdau
und 460800
Hex), HMA
Authentifizi
Verschlüss
sich um die
die in der lo
festgelegt w
akzeptiert u
SA erstellt.
SPI-Werte
Index) zuge
sich um ein
noch nicht
Datenverke
kann.
Der Pseudo
für das IP-P
172.16.10.1
Adresse) b
öffentliche

Ein IPSec S
ein- als auc
Datenverke
akzeptierte

hat spi 0x82C3E0C4 und conn_id 0
Lebensdauer von 3.600 Sekunden
Lebensdauer von 4608000 Kilobyte
Ausgehende SA von 172.16.1.1 bis 172.16.10.1 (f/i) 0/0
(Proxy 172.16.1.1 bis 172.16.10.1)
hat spi 0xDD2AC2B3 und conn_id 0
Lebensdauer von 3.600 Sekunden
Lebensdauer von 4608000 Kilobyte
ISAKMP: (1002) Senden des Pakets an 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1002):Senden eines IKE-IPv4-Pakets.
ISAKMP:(1002):Löschen des Knotens -830593317: Fehlerursache "Kein Fehler"
ISAKMP:(1002):Knoten 3464373979, Eingabe = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1002):Alter Zustand = IKE_QM_I_QM1 Neuer Status = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): Warteschlangenereignis mit 1 KMI-Meldung(en)
Crypto mapdb: Proxy-Übereinstimmung
src-Adresse: 172,16,1,1
dst-Adresse: 172,16,10,1
Protokoll: 47
src-Port: 0
dst-Port: 0
IPSEC(crypto_ipsec_sa_find_ident_head): Wiederverbindung mit denselben Proxys und Peer 172.16.10.1
IPSEC(policy_db_add_ident): src 172.16.1.1, dest 172.16.10.1, dest_port 0

IPSEC(create_sa): als erstellt,
(sa) sa_dest= 172.16.1.1, sa_proto= 50,
sa_spi= 0x82C3E0C4(2193875140),
sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 3
sa_life(k/sec)= (4499172/3600)
IPSEC(create_sa): als erstellt,
(sa) sa_dest= 172.16.10.1, sa_proto= 50,
sa_spi= 0xDD2AC2B3(3710567091),
sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 4
sa_life(k/sec)= (4499172/3600)
IPSEC(update_current_outbound_sa): Aktivieren Sie SA Peer 172.16.10.1 Current Outbound sa to SPI DD2AC2B3.
IPSEC(update_current_outbound_sa): Aktualisiert Peer 172.16.10.1 Ausgehend als an SPI DD2AC2B3
IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): Tunnel0 ident 94F2740 mit tun_decap_oce 794ED30 aktualisieren
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Verbindungssuche zurückgegeben 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):

Das Spoke
letzte QM-N
den QM-Au
Gegensatz
jeder Peer
(MM1 bis M
IPSec ein v
drei anstatt
Der Initiato
"Spoke", wi
IKE_QM_I_
wechselt vo
direkt zu Q
QM_PHAS
Responder
QM_SPI_S
QM_PHAS
Es wird ein
Erstellung a
IPs, SPIs, A
Transforma
Lebensdau
Sekunden

tunnel_protection_socket_up
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Signalisierung NHRP
NHRP: NHS 10.1.1.254 Tunnel0 vrf 0 Cluster 0 Priorität 0 Von ' ' wird auf 'E' übertragen

IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Verbindungssuche zurückgegeben 961D220
NHRP: Versuch, Paket über DEST 10.1.1.254 zu senden

Diese letzten QM-Meldungen bestätigen, dass der Quick Mode abgeschlossen ist und IPSec auf beiden Seiten des Tunnels aktiv ist. Im Gegensatz zu ISAKMP, bei dem jeder Peer jeden Zustand durchläuft (MM1 bis MM6/P1_COMPLETE), ist IPSec ein wenig anders, da es nur drei anstatt sechs Nachrichten gibt. Der Responder (in diesem Fall unser Hub, wie durch "R" in der Meldung IKE_QM_**R**_QM1 gekennzeichnet) geht QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE. Der Initiator (Spoke) wechselt von QM_READY, dann direkt zu QM_I_QM1 zu QM_PHASE2_COMPLETE.

ISAKMP (1002): empfangenes Paket von 172.16.1.1 dport 500 sport 500 Global (R) QM_IDLE
ISAKMP:(1002):Löschen des Knotens -830593317: Fehler FALSE-Grund "QM done (await)"
ISAKMP:(1002):Knoten 3464373979, Eingabe = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1002):Alter Zustand = IKE_QM_R_QM2 Neuer Status = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): Warteschlangenereignis mit 1 KMI-Meldung(en)
IPSEC(key_engine_enable_outbound): Benachrichtigung von ISAKMP aktivieren
IPSEC(key_engine_enable_outbound): SA mit spi 2193875140/50 aktivieren
IPSEC(update_current_outbound_sa): Aktivieren Sie SA Peer 172.16.1.1 Current Outbound sa to SPI 82C3E0C4.
IPSEC(update_current_outbound_sa): Aktueller ausgehender Peer 172.16.1.1 als an SPI 82C3E0C4
NHRP: Registrierungsanfrage über Tunnel0 vrf 0 senden, Paketgröße: 108
src: 10.1.1.1, dst: 10.1.1.254
F) Fan: IPv4(1), Typ: IP(800), Hop: 255, Version: 1
shtl: 4 (NSAP), SSL: 0 (NSAP)
Pktsz: 108 Abs.: 52
M) Flaggen: "Unique nat", erforderlich: 65540
src NBMA: 172,16,1,1
SRC-Protokoll: 10.1.1.1, dst-Protokoll: 10.1.1.254
(C-1)-Code: Kein Fehler(0)
Präfix: 32 mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0 (NSAP), proto_len: 0, vorf: 0
Adressverlängerung(3):
NHS-Datensatzerweiterung für Weiterleitung(4):
NHS-Datensatzerweiterung für Umkehrverkehr(5):
Authentifizierungserweiterung(7):
Typ:Cleartext(1), data:NHRPAUTH
NAT-Adresserweiterung(9):
(C-1)-Code: Kein Fehler(0)
Präfix: 32 mtu: 17912, hd_time: 0
addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, vorf.: 0
Kunden-NBMA: 172,16,10,1

Dies sind d
Registrieru
Hub gesen
NHS (dem
normal, me
zu sehen, d
versuchen,
anzumelde
"Registrieru
src,dst: Qu
Adressen (
sind die Qu
Router ges
src NBMA:
Adresse de
gesendet h
NHS anzur
src-Protoko
Spokes, da
registrieren
dst-Protoko
NHS/Hubs
Authentifizi
data&colon

Clientprotokoll: 10.1.1.254

NHRP-RATE: Senden des anfänglichen Registrierungsantrags für 10.1.1.254, Anfrage 65540
%LINK-3-UPDOWN: Interface Tunnel0 (Schnittstellentunnel0, Status geändert, hochgefahren)
NHRP: if_up: Tunnel0 proto 0
NHRP: Tunnel0: Cache-Update für Ziel 10.1.1.254/32 Next-Hop 10.1.1.254
172,16,10,1
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Verbindungssuche zurückgegeben 961D220
NHRP: Versuch, Paket über DEST 10.1.1.254 zu senden
IPSEC-IFC GRE/Tu0: Tunnel kommt
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Verbindungssuche zurückgegeben 961D220
IPSEC-IFC GRE/Tu0: crypto_ss_listen_start bereits abgehört
IPSEC-IFC GRE/Tu0: crypto_ss_listen_start bereits abgehört
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Öffnen eines Sockels mit dem Profil DMVPN-IPSEC
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Verbindungssuche zurückgegeben 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Der Sockel ist bereits geöffnet. Ignorieren.
%LINEPROTO-5-UPDOWN: Leitungsprotokoll auf Interface Tunnel0 (Schnittstellentunnel0), Status auf up

Dies sind die NHRP-Registrierungsanfragen, die vom Spoke-Team beim NHS (dem Hub) eingegangen sind. Es ist normal, mehrere dieser Meldungen zu sehen, da die Spokes weiterhin versuchen, sich beim NHS anzumelden, bis sie eine "Registrierungsantwort" erhalten.
src NBMA: die NBMA (Internet-Adresse des Spokes), der das Paket gesendet hat und versucht, sich beim NHS anzumelden
src-Protokoll: Tunneladresse des Spokes, das versucht, sich zu registrieren
dst-Protokoll: Tunneladresse des NHS/Hubs
Authentifizierungserweiterung, data: NHRP-

NHRP: Empfang der Registrierungsanfrage über Tunnel0 VRF 0, Paketgröße: 108
F) Fan: IPv4(1), Typ: IP(800), Hop: 255, Version: 1
shtl: 4 (NSAP), SSL: 0 (NSAP)
Pktsz: 108 Abs.: 52
M) Flaggen: "Unique nat", erforderlich: 65540
src NBMA: 172,16,1,1
SRC-Protokoll: 10.1.1.1, dst-Protokoll: 10.1.1.254
(C-1)-Code: Kein Fehler(0)
Präfix: 32 mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0 (NSAP), proto_len: 0, vorf: 0
Adressverlängerung(3):
NHS-Datensatzerweiterung für Weiterleitung(4):
NHS-Datensatzerweiterung für Umkehrverkehr(5):
Authentifizierungserweiterung(7):
Typ:Cleartext(1), data:NHRPAUTH
NAT-Adresserweiterung(9):
(C-1)-Code: Kein Fehler(0)
Präfix: 32 mtu: 17912, hd_time: 0

Authentifizi
Kunden-NB
NHS/Hubs
Clientproto
NHS/Hubs
Weitere NH
wonach de
Registrieru
an den NH
auch eine E
Cache-Eint
10.1.1.254/
bei NBMA
ist. Die vers
dass der Tu
hier zu seh

Dies sind a
Dienstmeld
sie ordnung
Hier ist end
Tunnelprot

Authentifizierungszeichenfolge **Kunden-NBMA**: NBMA-Adresse des NHS/Hubs **Clientprotokoll**: Tunneladresse des NHS/Hubs	addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, vorf.: 0 **Kunden-NBMA: 172,16,10,1** **Clientprotokoll: 10.1.1.254**
NHRP-Debugpakete zum Hinzufügen des Zielnetzwerks 10.1.1.1/32 verfügbar über den nächsten Hop von 10.1.1.1 bei NHRP von 172.16.1.1. 172.16.1.1 wird außerdem der Liste der Adressen hinzugefügt, an die der Hub Multicast-Datenverkehr weiterleitet. Diese Meldungen bestätigen, dass die Registrierung erfolgreich war, wie auch eine Entschließung für die Spokes Tunnel-Adresse.	NHRP: netid_in = 1, to_us = 1 **NHRP: Tunnel0: Cache-Add für Ziel 10.1.1.1/32 Next-Hop 10.1.1.1** **172,16,1,1** **NHRP: Hinzufügen von Tunnel-Endpunkten (VPN: 10.1.1.1, NBMA: 172.16.1.1)** **NHRP: Erfolgreich angeschlossener NHRP-Unterblock für Tunnel-Endpunkte (VPN: 10.1.1.1, NBMA: 172.16.1.1)** NHRP: Unterblock-Knoten für Cache eingefügt: Ziel-Einfügeter Unterblock-Knoten für Cache: Ziel 10.1.1.1/32nhop 10.1.1.1 NHRP: Konvertierter interner dynamischer Cache-Eintrag für 10.1.1.1/32 Interface Tunnel0 in externer Cache **NHRP: Tu0: Erstellen von dynamischer Multicast-Zuordnung NBMA: 172,16,1,1** **NHRP: Dynamische Multicast-Zuordnung für NBMA hinzugefügt: 172,16,1,1** NHRP: Aktualisieren unseres Cache mit NBMA: 172.16.10.1, NBMA_ALT: 172,16,10,1 NHRP: Neue obligatorische Länge: 32 NHRP: Versuch, Paket über DEST 10.1.1.1 zu senden **NHRP: NHRP konnte 10.1.1.1 auf NBMA 172.16.1.1 erfolgreich auflösen.** **NHRP: Kapselung erfolgreich abgeschlossen. Tunnel-IP-Adresse 172.16.1.1**
Dies ist die NHRP-Registrierungsantwort, die der Hub als Antwort auf die zuvor erhaltene NHRP-Registrierungsanfrage an das Spoke gesendet hat. Wie die anderen Registrierungspakete sendet auch der Hub mehrere dieser Pakete als Antwort auf mehrere Anfragen. **src,dst**: Tunnelquelle (Hub) und Ziel (Spoke)-IP-Adressen Dies sind die Quelle und das Ziel des vom Router gesendeten GRE-Pakets **src NBMA**: NBMA (Internet-Adresse des Spokes) **src-Protokoll**: Tunneladresse des Spokes, das versucht, sich zu registrieren **dst-Protokoll**: Tunneladresse des NHS/Hubs **Kunden-NBMA**: NBMA-Adresse des NHS/Hubs	**NHRP: Senden der Registrierungsantwort über Tunnel0 VRF 0, Paketgröße: 128** **src: 10.1.1.254, dst: 10.1.1.1** F) Fan: IPv4(1), Typ: IP(800), Hop: 255, Version: 1 shtl: 4 (NSAP), SSL: 0 (NSAP) Pktsz: 128 Extoff: 52 M) Flaggen: "Unique nat", erforderlich: 65540 **src NBMA: 172,16,1,1** **SRC-Protokoll: 10.1.1.1, dst-Protokoll: 10.1.1.254** (C-1)-Code: Kein Fehler(0) Präfix: 32 mtu: 17912, hd_time: 7200 addr_len: 0(NSAP), subaddr_len: 0 (NSAP), proto_len: 0, vorf: 0 Adressverlängerung(3): C) Code: Kein Fehler(0) Präfix: 32 mtu: 17912, hd_time: 7200 addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, vorf.: 0 **Kunden-NBMA: 172,16,10,1** **Clientprotokoll: 10.1.1.254** NHS-Datensatzerweiterung für Weiterleitung(4):

Clientprotokoll: Tunneladresse des NHS/Hubs
Authentifizierungserweiterung, data: NHRP-Authentifizierungszeichenfolge

NHS-Datensatzerweiterung für Umkehrverkehr(5):
Authentifizierungserweiterung(7):
Typ:Cleartext(1), data:NHRPAUTH
NAT-Adresserweiterung(9):
(C-1)-Code: Kein Fehler(0)
Präfix: 32 mtu: 17912, hd_time: 0
addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, vorf.: 0
Kunden-NBMA: 172,16,10,1
Clientprotokoll: 10.1.1.254
NHRP: Empfang der Registrierungsantwort über Tunnel0 VRF 0, Paketgröße: 128
F) Fan: IPv4(1), Typ: IP(800), Hop: 255, Version: 1
shtl: 4 (NSAP), SSL: 0 (NSAP)
Pktsz: 128 Extoff: 52
M) Flaggen: "Unique nat", erforderlich: 65541
src NBMA: 172,16,1,1
SRC-Protokoll: 10.1.1.1, dst-Protokoll: 10.1.1.254
(C-1)-Code: Kein Fehler(0)
Präfix: 32 mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0 (NSAP), proto_len: 0, vorf: 0
Adressverlängerung(3):
C) Code: Kein Fehler(0)
Präfix: 32 mtu: 17912, hd_time: 7200
addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, vorf.: 0
Kunden-NBMA: 172,16,10,1
Clientprotokoll: 10.1.1.254
NHS-Datensatzerweiterung für Weiterleitung(4):
NHS-Datensatzerweiterung für Umkehrverkehr(5):
Authentifizierungserweiterung(7):
Typ:Cleartext(1), data:NHRPAUTH
NAT-Adresserweiterung(9):
(C-1)-Code: Kein Fehler(0)
Präfix: 32 mtu: 17912, hd_time: 0
addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, vorf.: 0
Kunden-NBMA: 172,16,10,1
Clientprotokoll: 10.1.1.254

Dies ist die
Registrieru
als Antwort
NHRP-Reg
Spoke gese
Registrieru
der Hub me
Antwort auf
src NBMA:
des Spokes
src-Protoko
Spokes, da
registrieren
dst-Protoko
NHS/Hubs
Kunden-NB
NHS/Hubs
Clientproto
NHS/Hubs
Authentifizi
data&colon
Authentifizi

Generellere IPSec-Dienstmeldungen, die sagen, dass sie ordnungsgemäß funktioniert.

NHRP: netid_in = 0, to_us = 1
IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start bereits abgehört
IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Öffnen eines Sockels mit dem Profil DMVPN-IPSEC
IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Verbindungssuche zurückgegeben 8C9388
IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Der Sockel ist bereits geöffnet. Ignorieren.
IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): tunnel_protection_stop_ausstehend_timer 8C93888
NHRP: NHS-UP: 10.1.1.254

NHRP-Serv
angeben, d

		10.1.1.254
Die Systemmeldung, die angibt, dass die EIGRP-Adjacency aktiv ist, und der Nachbarn mit der Adresse 10.1.1.1 spricht.	%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.1 (Tunnel0) ist aktiviert: neue Adjacency	
	%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.254 (Tunnel0) ist aktiviert: neue Adjacency	Die System die EIGRP- Nachbarhu
Systemmeldung, die eine erfolgreiche NHRP-Auflösung bestätigt.	NHRP: NHRP konnte 10.1.1.1 auf NBMA 172.16.1.1 erfolgreich auflösen.	

Überprüfen der Funktionalität und Fehlerbehebung

Dieser Abschnitt enthält einige der nützlichsten **show**-Befehle, die zur Fehlerbehebung für Hub and Spoke verwendet werden. Um spezifischere Debuggen zu aktivieren, verwenden Sie die folgenden Debugkonditionen:

- debug dmvpn condition peer nbma *NBMA_ADDRESS*
- debug dmvpn condition peer tunnel *TUNNEL_ADDRESS*
- debug crypto condition peer ipv4 *NBMA_ADDRESS*

Krypto-Sockets anzeigen

```
Spoke1#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.1.1/172.16.10.1
Local Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0"

Hub#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.10.1/172.16.1.1
Local Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0"
```

Anzeige von Kryptositzungsdetails

```
Spoke1#show crypto session detail
```

```
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:01:01
Session status: UP-ACTIVE
Peer: 172.16.10.1 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 172.16.10.1
Desc: (none)
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:58
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 25 drop 0 life (KB/Sec) 4596087/3538
Outbound: #pkts enc'ed 25 drop 3 life (KB/Sec) 4596087/3538

Hub#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:01:47
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none)
ivrf: (none)
Phase1_id: 172.16.1.1
Desc: (none)
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:12
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 35 drop 0 life (KB/Sec) 4576682/3492
Outbound: #pkts enc'ed 35 drop 0 life (KB/Sec) 4576682/3492
```

show crypto isakmp sa detail

```
Spoke1#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1001 172.16.1.1 172.16.10.1 ACTIVE 3des sha psk 1 23:59:10
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA

Hub#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption IPv4 Crypto ISAKMP SA
```

```
C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1001 172.16.10.1 172.16.1.1 ACTIVE 3des sha psk 1 23:58:20
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA
```

show crypto ipsec sa detail

```
Spoke1#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.1.1
protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
current_peer 172.16.10.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 3, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.10.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xA259D71(170237297)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport,}
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
outbound ah sas:
outbound pcp sas:

Hub#show crypto ipsec sa detail
```

```
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
current_peer 172.16.1.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 34, #pkts encrypt: 34, #pkts digest: 34
#pkts decaps: 34, #pkts decrypt: 34, #pkts verify: 34
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x8D538D11(2371063057)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas: spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:
outbound pcp sas:
```

show ip nhrp

```
Spoke1#show ip nhrp
10.1.1.254/32 via 10.1.1.254
Tunnel0 created 00:00:55, never expire
Type: static, Flags:
NBMA address: 172.16.10.1
```

```
Hub#show ip nhrp
10.1.1.1/32 via 10.1.1.1
Tunnel0 created 00:01:26, expire 01:58:33
Type: dynamic, Flags: unique registered
NBMA address: 172.16.1.1
```

show ip nhs

```
Spoke1#show ip nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.1.1.254 RE priority = 0 cluster = 0

Hub#show ip nhrp nhs (As the hub is the only NHS for this DMVPN cloud,
it does not have any servers configured)
```

show dmvpn [Detail]

```
"show dmvpn detail" returns the output of show ip nhrp nhs, show dmvpn,
and show crypto session detail

Spoke1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# 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: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.10.1 10.1.1.254 UP 00:00:39 S

Spoke1#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# 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 Tunnel0 is up/up, Addr. is 10.1.1.1, VRF ""
Tunnel Src./Dest. addr: 172.16.1.1/172.16.10.1, Tunnel VRF ""
Protocol/Transport: "GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled

IPv4 NHS:
10.1.1.254 RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
----- --------------- --------------- ----- -------- ----- -----------------
1 172.16.10.1 10.1.1.254 UP 00:00:41 S 10.1.1.254/32


Crypto Session Details:
--------------------------------------------------------------------------------
Interface: Tunnel0
```

```
Session: [0x08D513D0]
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:59:18
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.10.1
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 21 drop 0 life (KB/Sec) 4596088/3558
Outbound: #pkts enc'ed 21 drop 3 life (KB/Sec) 4596088/3558
Outbound SPI : 0x A259D71, transform : esp-3des esp-sha-hmac
Socket State: Open

Pending DMVPN Sessions:

Hub#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# 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: Tunnel0, IPv4 NHRP Details Type:Hub, NHRP Peers:1,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.1.1.1 UP 00:01:30 D

Hub#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket # 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 Tunnel0 is up/up, Addr. is 10.1.1.254, VRF "" Tunnel Src./Dest. addr:
172.16.10.1/MGRE, Tunnel VRF "" Protocol/Transport: "multi-GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled Type:Hub, Total NBMA Peers (v4/v6): 1
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network ----- --------------- --
------------- ----- -------- ----- ----------------- 1 172.16.1.1 10.1.1.1 UP 00:01:32 D
10.1.1.1/32

Crypto Session Details:
-------------------------------------------------------------------------------- Interface:
Tunnel0
Session: [0x08A27858]
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:26
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.1.1
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound SPI : 0x8D538D11, transform : esp-3des esp-sha-hmac
Socket State: Open

Pending DMVPN Sessions:
```

Zugehörige Informationen

- IPsec-Fehlerbehebung: Verwenden von Debugbefehlen
- Verschlüsselungstechnologie der nächsten Generation
- RFC 3706: IKE Dead Peer Detection
- RFC 3947: IKE NAT-Traversal

- Technischer Support und Dokumentation - Cisco Systems