Migration von Legacy EzVPN zu Enhanced EzVPN - Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine Easy VPN-Konfiguration (EzVPN) konfiguriert wird, bei der Spoke 1 für die Verbindung mit dem Hub erweitertes EzVPN verwendet, während Spoke 2 für die Verbindung mit demselben Hub das Legacy-EzVPN verwendet. Der Hub ist für erweitertes EzVPN konfiguriert. Der Unterschied zwischen erweitertem EzVPN und Legacy-EzVPN besteht in der Verwendung dynamischer Virtual Tunnel Interfaces (dVTIs) in der ersten und in der Crypto Map in der zweiten. Cisco dVTI ist eine Methode, die von Kunden mit Cisco EzVPN sowohl für die Server- als auch für die Remote-Konfiguration verwendet werden kann. Die Tunnel bieten eine separate On-Demand-Schnittstelle für den virtuellen Zugriff für jede EzVPN-Verbindung. Die Konfiguration der virtuellen Zugriffsschnittstellen wird aus einer virtuellen Vorlagenkonfiguration geklont, die die IPsec-Konfiguration und alle Cisco IOS® Software-Funktionen umfasst, die auf der virtuellen Vorlagenschnittstelle konfiguriert sind, z. B. QoS, NetFlow oder Zugriffskontrolllisten (ACLs).

Mit IPsec dVTIs und Cisco EzVPN können Benutzer hochsichere Verbindungen für Remote-Access-VPNs bereitstellen, die mit Cisco AVVID (Architektur für Sprache, Video und integrierte Daten) kombiniert werden können, um konvergente Sprach-, Video- und Datenverbindungen über IP-Netzwerke bereitzustellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit EzVPN vertraut sind.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco IOS Version 15.4(2)T.

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.

Hintergrundinformationen

Das Cisco EzVPN mit dVTI-Konfiguration stellt eine routingfähige Schnittstelle bereit, um Datenverkehr selektiv an verschiedene Ziele zu senden, z. B. an einen EzVPN-Konzentrator, einen anderen Site-to-Site-Peer oder das Internet. Für die IPsec-dVTI-Konfiguration ist keine statische Zuordnung von IPsec-Sitzungen zu einer physischen Schnittstelle erforderlich. Dies ermöglicht die Flexibilität, verschlüsselten Datenverkehr über jede physische Schnittstelle zu senden und zu empfangen, z. B. bei mehreren Pfaden. Der Datenverkehr wird verschlüsselt, wenn er von oder an die Tunnelschnittstelle weitergeleitet wird.

Der Datenverkehr wird mithilfe der IP-Routing-Tabelle an die Tunnelschnittstelle oder von dieser

weitergeleitet. Routen werden während der Konfiguration des IKE-Modus dynamisch gelernt und in die Routing-Tabelle eingefügt, die auf den dVTI zeigt. Dynamisches IP-Routing kann verwendet werden, um Routen über das VPN zu propagieren. Die Verwendung von IP-Routing zur Weiterleitung des Datenverkehrs an die Verschlüsselung vereinfacht die IPsec-VPN-Konfiguration im Vergleich zur Verwendung von ACLs mit der Crypto Map in der nativen IPsec-Konfiguration.

In Versionen vor der Cisco IOS-Version 12.4(2)T mussten während der Tunnel-Up-/Tunnel-Down-Umstellung Attribute analysiert und angewendet werden, die während der Moduskonfiguration weitergeleitet wurden. Wenn solche Attribute zur Anwendung von Konfigurationen auf die Schnittstelle führten, musste die vorhandene Konfiguration überschrieben werden. Mit der dVTI-Support-Funktion kann die Tunnelup-Konfiguration auf separate Schnittstellen angewendet werden, was die Unterstützung separater Funktionen bei der Tunnelauslastung vereinfacht. Funktionen, die auf den Datenverkehr (vor der Verschlüsselung) angewendet werden, der in den Tunnel gelangt, können von den Funktionen getrennt werden, die auf Datenverkehr angewendet werden, der nicht durch den Tunnel geleitet wird (z. B. Split-Tunnel-Datenverkehr und Datenverkehr, der das Gerät verlässt, wenn der Tunnel nicht aktiv ist).

Wenn die EzVPN-Aushandlung erfolgreich war, wird der Leitungsprotokollstatus der virtuellen Zugriffsschnittstelle geändert. Wenn der EzVPN-Tunnel ausfällt, weil die Sicherheitszuordnung abläuft oder gelöscht wird, wird der Status des Verbindungsprotokolls der virtuellen Zugriffsschnittstelle deaktiviert.

Die Routing-Tabellen fungieren in einer virtuellen EzVPN-Schnittstellenkonfiguration als Datenverkehrsselektoren - d. h. die Routen ersetzen die Zugriffsliste auf der Crypto Map (Crypto Map). In einer virtuellen Schnittstellenkonfiguration handelt EzVPN eine einzelne IPsec-Sicherheitszuordnung aus, wenn der EzVPN-Server mit einem IPsec-dVTI konfiguriert wurde. Diese einzelne Sicherheitszuordnung wird unabhängig vom konfigurierten EzVPN-Modus erstellt.

Nachdem die Sicherheitszuordnung eingerichtet wurde, werden dem direkten Datenverkehr zum Unternehmensnetzwerk Routen hinzugefügt, die auf die virtuelle Zugriffsschnittstelle zeigen. EzVPN fügt dem VPN-Konzentrator auch eine Route hinzu, sodass gekapselte IPsec-Pakete an das Unternehmensnetzwerk weitergeleitet werden. Bei einem Non-Split-Modus wird eine Standardroute hinzugefügt, die auf die virtuelle Zugriffsschnittstelle zeigt. Wenn der EzVPN-Server den Split-Tunnel "überträgt", wird das Split-Tunnel-Subnetz zum Ziel, zu dem die Routen hinzugefügt werden, die auf den virtuellen Zugriff verweisen. Wenn der Peer (VPN-Konzentrator) nicht direkt verbunden ist, fügt EzVPN dem Peer eine Route hinzu.

> **Hinweis**: Auf den meisten Routern, auf denen die Cisco EzVPN Client-Software ausgeführt wird, ist eine Standardroute konfiguriert. Die konfigurierte Standardroute muss einen Metrik-Wert größer als 1 haben, da EzVPN eine Standardroute mit dem Metrik-Wert 1 hinzufügt. Die Route verweist auf die virtuelle Zugriffsschnittstelle, sodass der gesamte Datenverkehr an das Unternehmensnetzwerk weitergeleitet wird, wenn der Konzentrator das Split-Tunnel-Attribut nicht "drückt".

QoS kann eingesetzt werden, um die Leistung verschiedener Anwendungen im Netzwerk zu verbessern. In dieser Konfiguration wird Traffic Shaping zwischen den beiden Standorten verwendet, um die gesamte Datenverkehrsmenge zu begrenzen, die zwischen den Standorten übertragen werden soll. Darüber hinaus kann die QoS-Konfiguration eine beliebige Kombination von QoS-Funktionen der Cisco IOS-Software unterstützen, um alle Sprach-, Video- oder Datenanwendungen zu unterstützen.

Hinweis: Die QoS-Konfiguration in diesem Leitfaden dient nur zu Demonstrationszwecken. Es wird erwartet, dass die VTI-Skalierbarkeitsergebnisse ähnlich der GRE (Point-to-Point) Generic Routing Encapsulation) über IPsec sind. Fragen Sie bei Fragen zur Skalierung und Leistung Ihren Ansprechpartner bei Cisco. Weitere Informationen finden Sie unter Konfigurieren einer virtuellen Tunnelschnittstelle mit IP-Sicherheit.

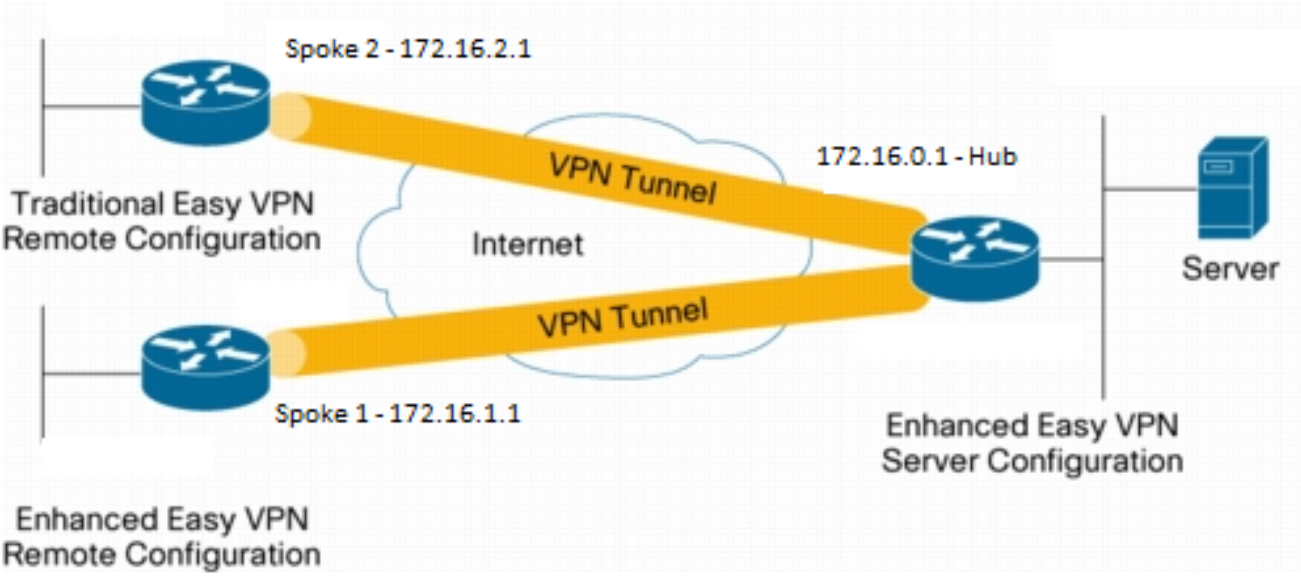
Vorteile

- **Vereinfachtes Management**
  Kunden können mithilfe der virtuellen Cisco IOS-Vorlage nach Bedarf neue virtuelle Zugriffsschnittstellen für IPsec klonen, was die Komplexität der VPN-Konfiguration vereinfacht und zu Kostensenkungen führt. Darüber hinaus können bestehende Verwaltungsanwendungen jetzt separate Schnittstellen für verschiedene Standorte zu Überwachungszwecken überwachen.
- **Stellt eine routbare Schnittstelle bereit**
  Cisco IPsec VTIs können alle Arten von IP-Routing-Protokollen unterstützen. Kunden können diese Funktionen nutzen, um größere Büroumgebungen wie Zweigstellen miteinander zu verbinden.
- **Verbesserte Skalierung**
  IPsec-VTIs verwenden einzelne Sicherheitszuordnungen pro Standort, die unterschiedliche Arten von Datenverkehr abdecken und so eine bessere Skalierung ermöglichen.
- **Flexible Definition von Funktionen**
  Ein IPsec-VTI ist eine Kapselung innerhalb einer eigenen Schnittstelle. Dies bietet Flexibilität bei der Definition von Funktionen für Klartext-Datenverkehr auf IPsec-VTIs und definiert Funktionen für verschlüsselten Datenverkehr auf physischen Schnittstellen.

Konfigurieren

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm



Konfigurationsübersicht

Hub-Konfiguration

```
hostname Hub
!
no aaa new-model
!
no ip domain lookup
!
username test-user privilege 15 password 0 cisco123
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group En-Ezvpn
 key test-En-Ezvpn
crypto isakmp profile En-EzVpn-Isakmp-Profile
   match identity group En-Ezvpn
   isakmp authorization list default
   client configuration address respond
   virtual-template 1
!
!
crypto ipsec transform-set VPN-TS esp-aes esp-sha-hmac
 mode tunnel
!
crypto ipsec profile En-EzVpn-Ipsec-Profile
 set transform-set VPN-TS
 set isakmp-profile En-EzVpn-Isakmp-Profile
!
```

```
!
interface Loopback0
 description Router-ID
 ip address 10.0.0.1 255.255.255.255
!
interface Loopback1
 description inside-network
 ip address 192.168.0.1 255.255.255.255
!
interface Ethernet0/0
 description WAN-Link
 ip address 172.16.0.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile En-EzVpn-Ipsec-Profile
!
router eigrp 1
 network 10.0.0.1 0.0.0.0
 network 192.168.0.1 0.0.0.0
 network 192.168.1.1 0.0.0.0
!
ip route 0.0.0.0 0.0.0.0 172.16.0.100
!
end
```

Spoke 1-Konfiguration (Enhanced EzVPN)

```
hostname Spoke1
!
no aaa new-model
!
interface Loopback0
 description Router-ID
 ip address 10.0.1.1 255.255.255.255
 crypto ipsec client ezvpn En-EzVpn inside
!
interface Loopback1
 description Inside-network
 ip address 192.168.1.1 255.255.255.255
!
interface Ethernet0/0
 description WAN-Link
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn En-EzVpn
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel mode ipsec ipv4
!
router eigrp 1
 network 10.0.1.1 0.0.0.0
 network 192.168.1.1 0.0.0.0
!
ip route 0.0.0.0 0.0.0.0 172.16.1.100
!
```

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto ipsec client ezvpn En-EzVpn
 connect auto
 group En-Ezvpn key test-En-Ezvpn
 mode network-extension
 peer 172.16.0.1
 virtual-interface 1
!
end
```

> **Vorsicht**: Die virtuelle Vorlage muss definiert werden, bevor die Client-Konfiguration eingegeben wird. Ohne eine vorhandene virtuelle Vorlage mit derselben Nummer akzeptiert der Router den Befehl **virtual-interface 1**.

Spoke 2 (ältere EzVPN-Konfiguration)

```
hostname Spoke2
!
no aaa new-model
!
no ip domain lookup
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto ipsec client ezvpn Leg-Ezvpn
 connect auto
 group En-Ezvpn key test-En-Ezvpn
 mode network-extension
 peer 172.16.0.1
 xauth userid mode interactive
!
!
interface Loopback0
 ip address 10.0.2.1 255.255.255.255
 crypto ipsec client ezvpn Leg-Ezvpn inside
!
interface Loopback1
 ip address 192.168.2.1 255.255.255.255
!
interface Ethernet0/0
 ip address 172.16.2.1 255.255.255.0
 crypto ipsec client ezvpn Leg-Ezvpn
!
ip route 0.0.0.0 0.0.0.0 172.16.2.100
!
end
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Hub-to-Spoke 1-Tunnel

Phase 1

```
Hub#show crypto isakmp sa det
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.

1006  172.16.0.1      172.16.2.1             ACTIVE aes  sha    psk  2  23:54:53 C
      Engine-id:Conn-id =  SW:6

1005  172.16.0.1      172.16.1.1             ACTIVE aes  sha    psk  2  23:02:14 C
      Engine-id:Conn-id =  SW:5

IPv6 Crypto ISAKMP SA
```

Phase 2

Die Proxys hier sind für Any/any, was impliziert, dass jeder Datenverkehr, der den virtuellen Zugriff 1 verlässt, verschlüsselt und an 172.16.1.1 gesendet wird.

```
Hub#show crypto ipsec sa peer 172.16.1.1 detail

interface: Virtual-Access1
   Crypto map tag: Virtual-Access1-head-0, local addr 172.16.0.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 172.16.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 776, #pkts encrypt: 776, #pkts digest: 776
   #pkts decaps: 771, #pkts decrypt: 771, #pkts verify: 771
   #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 tagged (send): 0, #pkts untagged (rcv): 0
   #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
   #pkts internal err (send): 0, #pkts internal err (recv) 0
```

```
    local crypto endpt.: 172.16.0.1, remote crypto endpt.: 172.16.1.1
    plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0x9159A91E(2438572318)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xB82853D4(3089650644)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 13, flow_id: SW:13, sibling_flags 80000040, crypto map:
Virtual-Access1-head-0
       sa timing: remaining key lifetime (k/sec): (4342983/3529)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x9159A91E(2438572318)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 14, flow_id: SW:14, sibling_flags 80000040, crypto map:
Virtual-Access1-head-0
       sa timing: remaining key lifetime (k/sec): (4342983/3529)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

EIGRP

```
Hub#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   172.16.1.1              Vi1                      13 00:59:28   31  1398  0  3
```

Hinweis: Spoke 2 bildet keinen Eintrag, da es nicht möglich ist, einen EIGRP-Peer (Enhanced Interior Gateway Routing Protocol) ohne eine routbare Schnittstelle zu bilden. Dies ist einer der Vorteile der Verwendung von dVTIs in den Spoke.

Spoke 1

Phase 1

```
Spoke1#show cry is sa det
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.

1005  172.16.1.1      172.16.0.1             ACTIVE aes  sha    psk  2  22:57:07 C
      Engine-id:Conn-id =  SW:5

IPv6 Crypto ISAKMP SA
```

Phase 2

```
Spoke1#show crypto ipsec sa detail

interface: Virtual-Access1
   Crypto map tag: Virtual-Access1-head-0, local addr 172.16.1.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 172.16.0.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 821, #pkts encrypt: 821, #pkts digest: 821
   #pkts decaps: 826, #pkts decrypt: 826, #pkts verify: 826
   #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 tagged (send): 0, #pkts untagged (rcv): 0
   #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
   #pkts internal err (send): 0, #pkts internal err (recv) 0

    local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.0.1
    plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0xB82853D4(3089650644)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x9159A91E(2438572318)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 11, flow_id: SW:11, sibling_flags 80004040, crypto map:
Virtual-Access1-head-0
       sa timing: remaining key lifetime (k/sec): (4354968/3290)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xB82853D4(3089650644)
```

```
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 12, flow_id: SW:12, sibling_flags 80004040, crypto map:
Virtual-Access1-head-0
       sa timing: remaining key lifetime (k/sec): (4354968/3290)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

EZVPN

```
Spoke1#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : En-EzVpn
Inside interface list: Loopback0
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Save Password: Disallowed
Current EzVPN Peer: 172.16.0.1
```

Routing - EIGRP

In Spoke 2 werden die Proxys so konfiguriert, dass jeder Datenverkehr, der die virtuelle Zugriffsschnittstelle verlässt, verschlüsselt wird. Solange eine Route vorhanden ist, die auf diese Schnittstelle für ein Netzwerk verweist, wird der Datenverkehr verschlüsselt:

```
Spoke1#ping 192.168.0.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/6 ms

Spoke1#ping 192.168.0.1 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms

Spoke1# sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override

Gateway of last resort is 172.16.1.100 to network 0.0.0.0
```

```
S*    0.0.0.0/0 [1/0] via 172.16.1.100
                [1/0] via 0.0.0.0, Virtual-Access1
     10.0.0.0/32 is subnetted, 2 subnets
D        10.0.0.1 [90/27008000] via 10.0.0.1, 01:16:15, Virtual-Access1
C        10.0.1.1 is directly connected, Loopback0
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S        172.16.0.1/32 [1/0] via 172.16.1.100
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0
     192.168.0.0/32 is subnetted, 1 subnets
D        192.168.0.1 [90/27008000] via 10.0.0.1, 01:16:15, Virtual-Access1
      192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.1 is directly connected, Loopbback1
Spoke1#
```

Hub-to-Spoke 2-Tunnel

Phase 1

```
Hub#show crypto isakmp sa det
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.

1006  172.16.0.1      172.16.2.1             ACTIVE aes  sha    psk  2  23:54:53 C
      Engine-id:Conn-id =  SW:6

1005  172.16.0.1      172.16.1.1             ACTIVE aes  sha    psk  2  23:02:14 C
      Engine-id:Conn-id =  SW:5

IPv6 Crypto ISAKMP SA
```

Phase 2

In diesem Beispiel wird keine Split-Tunnel-ACL unter der Clientkonfiguration auf dem Hub verwendet. Daher sind die Proxys, die in den Spokes gebildet werden, für jedes EzVPN "innerhalb"-Netzwerk im Spoke-Netzwerk zu jedem Netzwerk. Grundsätzlich wird am Hub sämtlicher Datenverkehr, der für eines der "internen" Netzwerke in den Spokes bestimmt ist, verschlüsselt und an 172.16.2.1 gesendet.

```
Hub#show crypto ipsec sa  peer 172.16.2.1 detail

interface: Virtual-Access2
   Crypto map tag: Virtual-Access2-head-0, local addr 172.16.0.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.0.2.1/255.255.255.255/0/0)
   current_peer 172.16.2.1 port 500
    PERMIT, flags={origin_is_acl,}
```

```
   #pkts encaps: 15, #pkts encrypt: 15, #pkts digest: 15
   #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
   #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 tagged (send): 0, #pkts untagged (rcv): 0
   #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
   #pkts internal err (send): 0, #pkts internal err (recv) 0

    local crypto endpt.: 172.16.0.1, remote crypto endpt.: 172.16.2.1
    plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0x166CAC10(376220688)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x8525868A(2233829002)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 11, flow_id: SW:11, sibling_flags 80000040, crypto map:
Virtual-Access2-head-0
       sa timing: remaining key lifetime (k/sec): (4217845/1850)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x166CAC10(376220688)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 12, flow_id: SW:12, sibling_flags 80000040, crypto map:
Virtual-Access2-head-0
       sa timing: remaining key lifetime (k/sec): (4217845/1850)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

Spoke 2

Phase 1

```
Spoke2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.0.1      172.16.2.1      QM_IDLE           1001 ACTIVE
```

```
IPv6 Crypto ISAKMP SA
```

Phase 2

```
Spoke2#show crypto ipsec sa detail

interface: Ethernet0/0
   Crypto map tag: Ethernet0/0-head-0, local addr 172.16.2.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.0.2.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 172.16.0.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
   #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #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 tagged (send): 0, #pkts untagged (rcv): 0
   #pkts not tagged (send): 0, #pkts not untagged (rcv): 0
   #pkts internal err (send): 0, #pkts internal err (recv) 0

    local crypto endpt.: 172.16.2.1, remote crypto endpt.: 172.16.0.1
    plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0x8525868A(2233829002)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x166CAC10(376220688)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map:
Ethernet0/0-head-0
       sa timing: remaining key lifetime (k/sec): (4336232/2830)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x8525868A(2233829002)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map:
Ethernet0/0-head-0
       sa timing: remaining key lifetime (k/sec): (4336232/2830)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:
```

```
    outbound pcp sas:
```

EZVPN

```
Spoke2#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 8

Tunnel name : Leg-Ezvpn
Inside interface list: Loopback0
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Save Password: Disallowed
Current EzVPN Peer: 172.16.0.1
```

Routing - Statisch

Im Gegensatz zu Spoke 1 muss Spoke 2 über statische Routen verfügen oder RRI (Reverse Route Injection) verwenden, um Routen zu injizieren, um ihm mitzuteilen, welcher Datenverkehr verschlüsselt werden soll und was nicht. In diesem Beispiel wird nur Datenverkehr, der von Loopback 0 stammt, gemäß Proxys und Routing verschlüsselt.

```
Spoke2#ping 192.168.0.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
.....
Success rate is 0 percent (0/5)

Spoke2#ping 192.168.0.1 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/7 ms

Spoke2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.2.100 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.100
      10.0.0.0/32 is subnetted, 1 subnets
C        10.0.2.1 is directly connected, Loopback0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Ethernet0/0
L        172.16.2.1/32 is directly connected, Ethernet0/0
      192.168.2.0/32 is subnetted, 1 subnets
C        192.168.2.1 is directly connected, Loopback1
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

> **Tipp**: In EzVPN kommen die Tunnel sehr oft nach Konfigurationsänderungen nicht mehr auf. In diesem Fall werden die Tunnel durch Löschen von Phase 1 und Phase 2 nicht hochgefahren. Geben Sie in den meisten Fällen den Befehl **clear crypto ipsec client ezvpn <group-name>** in das Spoke ein, um den Tunnel aufzurufen.

> **Hinweis**: Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug**-Befehlen finden Sie unter Wichtige Informationen.

Hub-Befehle

- **debug crypto ipsec** - Zeigt die IPsec-Verhandlungen von Phase 2 an.
- **debug crypto isakmp -** Zeigt die ISAKMP-Verhandlungen von Phase 1 an.

Spoke-Befehle

- **debug crypto ipsec -** Zeigt die IPsec-Verhandlungen von Phase 2 an.
- **debug crypto isakmp -** Zeigt die ISAKMP-Verhandlungen von Phase 1 an.
- **debug crypto ipsec client ezvpn -** Zeigt das EzVPN-Debuggen an.

Zugehörige Informationen

- IPsec-Support-Seite
- Cisco Easy VPN Remote
- Easy VPN-Server
- IPsec Virtual Tunnel-Schnittstelle
- Konfigurieren der IPsec-Netzwerksicherheit
- Konfigurieren des Internet Key Exchange Security Protocol
- Technischer Support und Dokumentation - Cisco Systems