Konfigurieren eines Site-to-Site IPSec-IKEv1-Tunnels zwischen einem ASA- und einem Cisco IOS-Router

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie ein standortübergreifender (LAN-to-LAN) IKEv1-Tunnel über die CLI zwischen einer Cisco ASA und einem Router, auf dem die Cisco IOS®-Software ausgeführt wird, konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco IOS
- Cisco Adaptive Security Appliance (ASA)
- Allgemeine IPSec-Konzepte

Verwendete Komponenten

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

- Cisco ASA der 5512-X-Serie mit Software-Version 9.4(1)
- Cisco Integrated Services Router (ISR) der 1941-Serie mit Cisco IOS-Software Version 15.4(3)M2

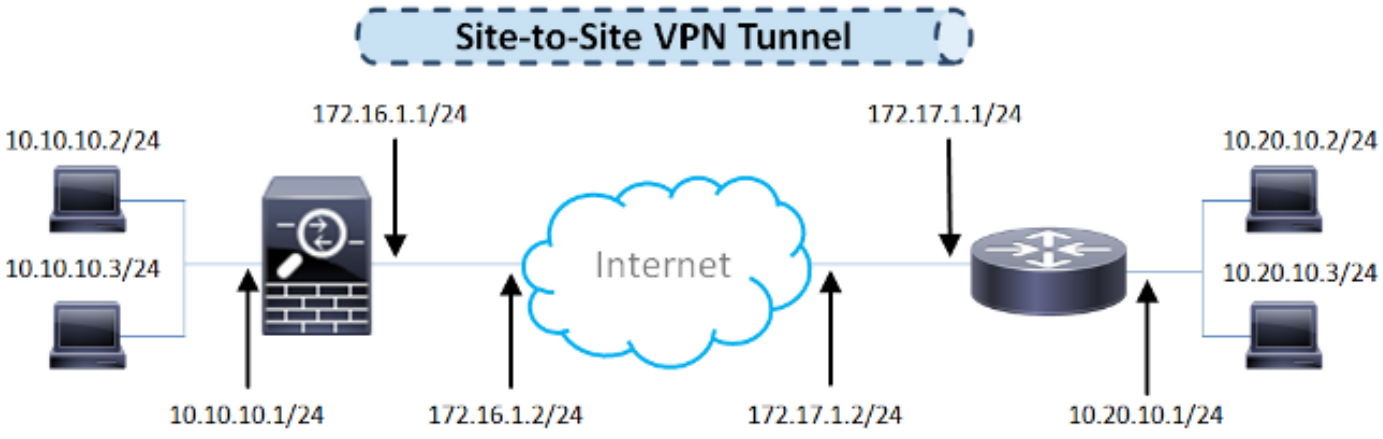
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie die CLI-Konfigurationen der ASA- und Cisco IOS-Router abschließen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



ASA-Konfiguration

ASA-Schnittstellen konfigurieren

Wenn die ASA-Schnittstellen nicht konfiguriert sind, stellen Sie sicher, dass Sie mindestens die IP-Adressen, die Schnittstellennamen und die Sicherheitsstufen konfigurieren:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

> **Hinweis**: Stellen Sie sicher, dass sowohl das interne als auch das externe Netzwerk, insbesondere der Remote-Peer, mit dem ein Site-to-Site-VPN-Tunnel eingerichtet wird, verbunden sind. Sie können einen Ping verwenden, um die grundlegenden Netzwerkverbindungen zu überprüfen.

IKEv1-Richtlinie konfigurieren und IKEv1 auf der externen Schnittstelle aktivieren

Um die ISAKMP-Richtlinien (Internet Security Association and Key Management Protocol) für die IKEv1-Verbindungen (Internet Key Exchange Version 1) von IPSec zu konfigurieren, geben Sie Folgendes ein: `crypto ikev1 policy` command:

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

> **Hinweis:** Eine IKEv1-Richtlinienübereinstimmung liegt vor, wenn beide Richtlinien der beiden Peers dieselben Parameterwerte für Authentifizierung, Verschlüsselung, Hash und Diffie-Hellman enthalten. Für IKEv1 muss die Remote-Peer-Richtlinie auch eine Lebensdauer angeben, die kleiner oder gleich der Lebensdauer in der vom Initiator gesendeten Richtlinie ist. Wenn die Lebensdauern nicht identisch sind, verwendet die ASA die kürzere Lebensdauer.

> **Hinweis:** Wenn Sie für einen bestimmten Richtlinienparameter keinen Wert angeben, wird der Standardwert angewendet.

Sie müssen IKEv1 auf der Schnittstelle aktivieren, die den VPN-Tunnel beendet. In der Regel ist dies die externe (oder öffentliche) Schnittstelle. Um IKEv1 zu aktivieren, geben Sie `crypto ikev1 enable` Befehl im globalen Konfigurationsmodus:

```
crypto ikev1 enable outside
```

Tunnelgruppe konfigurieren (LAN-to-LAN-Verbindungsprofil)

Für einen LAN-zu-LAN-Tunnel lautet der Verbindungsprofiltyp ipsec-l2l . Um den vorinstallierten IKEv1-Schlüssel zu konfigurieren, geben Sie den tunnel-group ipsec-attributes Konfigurationsmodus:

```
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
```

ACL für den relevanten VPN-Datenverkehr konfigurieren

Die ASA verwendet Zugriffskontrolllisten (Access Control Lists, ACLs), um den mit IPSec-Verschlüsselung zu schützenden Datenverkehr von dem Datenverkehr zu unterscheiden, der nicht geschützt werden muss. Es schützt die ausgehenden Pakete, die durch eine Application Control Engine (ACE) zugelassen werden, und stellt sicher, dass die eingehenden Pakete geschützt sind, die durch eine ACE zugelassen werden.

```
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0

access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
```

> **Hinweis:** Eine ACL für VPN-Datenverkehr verwendet die Quell- und Ziel-IP-Adressen nach Network Address Translation (NAT).

> **Hinweis:** Eine ACL für VPN-Datenverkehr muss auf beiden VPN-Peers gespiegelt werden.

> **Hinweis:** Wenn dem geschützten Datenverkehr ein neues Subnetz hinzugefügt werden muss, fügen Sie der entsprechenden Objektgruppe einfach ein Subnetz bzw. einen Host hinzu, und führen Sie eine Spiegelungsänderung auf dem Remote-VPN-Peer durch.

NAT-Ausnahme konfigurieren

> **Hinweis**: Die in diesem Abschnitt beschriebene Konfiguration ist optional.

In der Regel darf für den VPN-Datenverkehr keine NAT durchgeführt werden. Sie müssen eine Identitäts-NAT-Regel erstellen, um diesen Datenverkehr auszuschließen. Die Identitäts-NAT-Regel übersetzt einfach eine Adresse in dieselbe Adresse.

```
nat (inside,outside) source static local-network local-network destination static
remote-network remote-network no-proxy-arp route-lookup
```

IKEv1-Transformationssatz konfigurieren

Ein IKEv1-Transformationssatz ist eine Kombination aus Sicherheitsprotokollen und Algorithmen, die definieren, wie die ASA Daten schützt. Während der Verhandlung der IPSec-Sicherheitszuordnungen müssen die Peers einen Transformationssatz oder -vorschlag identifizieren, der für beide Peers gleich ist. Die ASA wendet dann den übereinstimmenden Transformationssatz oder -vorschlag an, um eine Sicherheitszuordnung zu erstellen, die Datenflüsse in der Zugriffsliste für diese Crypto Map schützt.

Um den IKEv1-Transformationssatz zu konfigurieren, geben Sie den `crypto ipsec ikev1 transform-set` command:

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```

Crypto Map konfigurieren und auf eine Schnittstelle anwenden

Eine Crypto Map definiert eine IPSec-Richtlinie, die in der IPSec-Sicherheitszuordnung ausgehandelt werden soll, und umfasst:

- Eine Zugriffsliste, um die Pakete zu identifizieren, die die IPSec-Verbindung zulässt und schützt
- Peer-Identifizierung
- Eine lokale Adresse für den IPSec-Datenverkehr
- Die IKEv1-Transformationssätze

Hier ein Beispiel:

```
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
```

Sie können dann die Crypto Map auf die Schnittstelle anwenden:

```
crypto map outside_map interface outside
```

ASA-Endkonfiguration

Nachfolgend finden Sie die endgültige Konfiguration der ASA:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0
!
access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
!
nat (inside,outside) source static local-network local-network destination
static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
crypto map outside_map interface outside
```

CLI-Konfiguration des Cisco IOS Routers

Schnittstellen konfigurieren

Wenn die Cisco IOS Router-Schnittstellen noch nicht konfiguriert sind, müssen mindestens die LAN- und WAN-Schnittstellen konfiguriert werden. Hier ein Beispiel:

```
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
no shutdown
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
no shutdown
```

Stellen Sie sicher, dass sowohl zu internen als auch zu externen Netzwerken eine Verbindung besteht, insbesondere zum Remote-Peer, der für die Einrichtung eines Site-to-Site-VPN-Tunnels verwendet wird. Sie können einen Ping verwenden, um die grundlegenden Netzwerkverbindungen zu überprüfen.

ISAKMP-Richtlinie (IKEv1) konfigurieren

Um die ISAKMP-Richtlinien für die IKEv1-Verbindungen zu konfigurieren, geben Sie crypto isakmp policy im globalen Konfigurationsmodus. Hier ein Beispiel:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
```

Hinweis: Sie können auf jedem Peer, der an IPSec teilnimmt, mehrere IKE-Richtlinien konfigurieren. Wenn die IKE-Aushandlung beginnt, versucht sie, eine gemeinsame Richtlinie zu finden, die auf beiden Peers konfiguriert ist, und beginnt mit den Richtlinien mit der höchsten Priorität, die auf dem Remote-Peer angegeben sind.

Crypto-ISAKMP-Schlüssel konfigurieren

Um einen vorinstallierten Authentifizierungsschlüssel zu konfigurieren, geben Sie den crypto isakmp key Befehl im globalen Konfigurationsmodus:

```
crypto isakmp key cisco123 address 172.16.1.1
```

ACL für relevanten VPN-Datenverkehr konfigurieren

Verwenden Sie die erweiterte oder benannte Zugriffsliste, um den Datenverkehr anzugeben, der durch Verschlüsselung geschützt werden muss. Hier ein Beispiel:

```
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

Hinweis: Eine ACL für VPN-Datenverkehr verwendet die Quell- und Ziel-IP-Adressen nach NAT.

Hinweis: Eine ACL für VPN-Datenverkehr muss auf beiden VPN-Peers gespiegelt werden.

NAT-Ausnahme konfigurieren

Hinweis: Die in diesem Abschnitt beschriebene Konfiguration ist optional.

In der Regel darf für den VPN-Datenverkehr keine NAT durchgeführt werden. Wenn die NAT-Überlastung verwendet wird, muss eine Routing-Map verwendet werden, um den relevanten VPN-Datenverkehr von der Übersetzung auszunehmen. Beachten Sie, dass der relevante VPN-Datenverkehr in der Zugriffsliste, die in der Routenübersicht verwendet wird, abgelehnt werden muss.

```
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 111

ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
```

Transformationssatz konfigurieren

Um einen IPSec-Transformationssatz (eine akzeptable Kombination von Sicherheitsprotokollen und Algorithmen) zu definieren, geben Sie die crypto ipsec transform-set im globalen Konfigurationsmodus. Hier ein Beispiel:

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
```

Crypto Map konfigurieren und auf eine Schnittstelle anwenden

Geben Sie den Befehl crypto map global configuration ein, um einen Crypto Map-Eintrag zu erstellen oder zu ändern und den Konfigurationsmodus für Crypto Map zu aktivieren. Damit der Crypto Map-Eintrag vollständig ist, müssen einige Aspekte definiert werden:

- Die IPsec-Peers, an die der geschützte Datenverkehr weitergeleitet werden kann, müssen definiert werden. Dies sind die Peers, mit denen eine SA eingerichtet werden kann. Um einen IPSec-Peer in einem Crypto Map-Eintrag anzugeben, geben Sie den set peer aus.
- Die für die Verwendung mit dem geschützten Datenverkehr akzeptablen Transformationssätze müssen definiert werden. Um die Transformationssätze festzulegen, die mit dem Crypto Map-Eintrag verwendet werden können, geben Sie den set transform-set aus.
- Der zu schützende Datenverkehr muss definiert werden. Um eine erweiterte Zugriffsliste für einen Crypto Map-Eintrag anzugeben, geben Sie den match address aus.

Hier ein Beispiel:

```
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
```

Der letzte Schritt ist die Anwendung der zuvor definierten Crypto Map-Gruppe auf eine Schnittstelle. Um dies anzuwenden, geben Sie den crypto map Schnittstellenkonfigurationsbefehl:

```
interface GigabitEthernet0/0
crypto map outside_map
```

Cisco IOS - Abschlusskonfiguration

Nachfolgend finden Sie die endgültige CLI-Konfiguration des Cisco IOS-Routers:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
!
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 crypto map outside_map
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
!
route-map nonat permit 10
 match ip address 111
!
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any
```

Überprüfung

Bevor Sie überprüfen, ob der Tunnel betriebsbereit ist und der Datenverkehr weitergeleitet wird, müssen Sie sicherstellen, dass der relevante Datenverkehr entweder an die ASA oder an den Cisco IOS-Router gesendet wird.

> **Hinweis:** Auf der ASA kann das Paket-Tracer-Tool, das dem relevanten Datenverkehr entspricht, verwendet werden, um den IPSec-Tunnel (z. B. packet-tracer input inside tcp 10.10.10.10

12345 10.20.10.10 80 detailed B.).

Überprüfung Phase 1

Geben Sie den Befehl show crypto isakmp sa ein, um zu überprüfen, ob IKEv1 Phase 1 auf der ASA läuft. Für die erwartete Ausgabe wird der MM_ACTIVE status:

```
ciscoasa# show crypto isakmp sa

IKEv1 SAs:

  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.17.1.1
   Type    : L2L             Role    : responder
   Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#
```

Um zu überprüfen, ob IKEv1 Phase 1 auf dem Cisco IOS aktiviert ist, geben Sie den show crypto isakmp sa aus. Für die erwartete Ausgabe wird der ACTIVE status:

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      172.17.1.1      QM_IDLE           1005 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

Überprüfung Phase 2

Um zu überprüfen, ob IKEv1 Phase 2 auf der ASA aktiv ist, geben Sie den show crypto ipsec sa aus. Als Ausgabe wird sowohl der eingehende als auch der ausgehende Security Parameter Index (SPI) erwartet. Wenn der Datenverkehr den Tunnel durchläuft, müssen die Zähler für Encaps/Entcaps inkrementiert werden.

> **Hinweis:** Für jeden ACL-Eintrag wird eine separate SA für ein- und ausgehenden Datenverkehr erstellt, was zu einer langen Dauer führen kann. show crypto ipsec sa Befehlsausgabe (abhängig von der Anzahl der ACE-Einträge in der Krypto-ACL).

Hier ein Beispiel:

```
ciscoasa# show crypto ipsec sa peer 172.17.1.1
peer address: 172.17.1.1
   Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
 10.20.10.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
     current_peer: 172.17.1.1


#pkts encaps: 1005, #pkts encrypt: 1005, #pkts digest: 1005
     #pkts decaps: 1014, #pkts decrypt: 1014, #pkts verify: 1014
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 1005, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.17.1.1/0
     path mtu 1500, ipsec overhead 74(44), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: 8A9FE619
     current inbound spi : D8639BD0

inbound esp sas:
     spi: 0xD8639BD0 (3630406608)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914900/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
     spi: 0x8A9FE619 (2325734937)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914901/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001

ciscoasa#
```

Um zu überprüfen, ob IKEv1 Phase 2 auf dem Cisco IOS aktiviert ist, geben Sie den show crypto ipsec sa aus. Als Ausgabe wird sowohl der eingehende als auch der ausgehende SPI erwartet. Wenn der Datenverkehr den Tunnel durchläuft, müssen die Zähler für Encaps/Entcaps inkrementiert werden.

Hier ein Beispiel:

```
Router#show crypto ipsec sa peer 172.16.1.1
```

```
interface: GigabitEthernet0/0
   Crypto map tag: outside_map, local addr 172.17.1.1

  protected vrf: (none)
local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  current_peer 172.16.1.1 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 2024, #pkts encrypt: 2024, #pkts digest: 2024
   #pkts decaps: 2015, #pkts decrypt: 2015, #pkts verify: 2015
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 26, #recv errors 0

    local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0xD8639BD0(3630406608)
    PFS (Y/N): N, DH group: none

inbound esp sas:
     spi: 0x8A9FE619(2325734937)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449870/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

outbound esp sas:
     spi: 0xD8639BD0(3630406608)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449868/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
Router#
```

Überprüfung Phase 1 und 2

In diesem Abschnitt werden die Befehle beschrieben, die Sie auf der ASA oder dem Cisco IOS verwenden können, um die Details für Phase 1 und 2 zu überprüfen.

Geben Sie show vpn-sessiondb auf der ASA zur Überprüfung:

```
ciscoasa# show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1

Session Type: LAN-to-LAN Detailed

Connection   : 172.17.1.1
Index        : 2                     IP Addr      : 172.17.1.1
Protocol     : IKEv1 IPsec
Encryption   : IKEv1: (1)AES128  IPsec: (1)AES128
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 100500                Bytes Rx     : 101400
Login Time   : 18:06:02 UTC Wed Jul 22 2015
Duration     : 0h:05m:07s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
 Tunnel ID    : 2.1
 UDP Src Port : 500                   UDP Dst Port : 500
 IKE Neg Mode : Main                  Auth Mode    : preSharedKeys
 Encryption   : AES128                Hashing      : SHA1
 Rekey Int (T): 86400 Seconds         Rekey Left(T): 86093 Seconds
 D/H Group    : 2
 Filter Name  :

IPsec:
 Tunnel ID    : 2.2
 Local Addr   : 10.10.10.0/255.255.255.0/0/0
 Remote Addr  : 10.20.10.0/255.255.255.0/0/0
 Encryption   : AES128                Hashing      : SHA1
 Encapsulation: Tunnel
 Rekey Int (T): 3600 Seconds          Rekey Left(T): 3293 Seconds
 Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607901 K-Bytes
 Idle Time Out: 30 Minutes            Idle TO Left : 26 Minutes
 Bytes Tx     : 100500                Bytes Rx     : 101400
 Pkts Tx      : 1005                  Pkts Rx      : 1014

NAC:
 Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
 SQ Int (T)   : 0 Seconds             EoU Age(T)   : 309 Seconds
 Hold Left (T): 0 Seconds             Posture Token:
 Redirect URL :

ciscoasa#
```

Geben Sie show crypto session zur Überprüfung auf Cisco IOS:

```
Router#show crypto session remote 172.16.1.1 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: GigabitEthernet0/0
Uptime: 00:03:36
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: 172.16.1.1
     Desc: (none)
 IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active
         Capabilities:(none) connid:1005 lifetime:23:56:23
```

```
 IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 2015 drop 0 life (KB/Sec) 4449870/3383
       Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383

Router#
```

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Fehlerbehebung in Ihrer Konfiguration.

> **Hinweis:** Lesen Sie vor der Verwendung die Cisco Dokumente Important Information on Debug Commands and IP Security Troubleshooting - Understanding and Using debug Commands debug -Befehlen.

IPSec LAN-to-LAN-Prüftool

Um automatisch zu überprüfen, ob die IPSec-Konfiguration zwischen LAN und ASA und Cisco IOS gültig ist, können Sie das Tool IPSec-LAN-to-LANChecker verwenden. Das Werkzeug ist so konzipiert, dass es eine show tech Oder show running-config von einem ASA- oder Cisco IOS-Router aus. Es untersucht die Konfiguration und versucht zu erkennen, ob ein auf einer Crypto Map basierender LAN-zu-LAN-IPSec-Tunnel konfiguriert ist. Ist dies der Fall, führt es eine Mehrpunktprüfung der Konfiguration durch und hebt alle Konfigurationsfehler und Einstellungen für den Tunnel hervor, die ausgehandelt würden.

ASA-Fehlersuche

Um die IPSec IKEv1-Tunnelaushandlung auf einer ASA-Firewall zu beheben, können Sie Folgendes verwenden: debug Befehle:

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

> **Hinweis:** Wenn die Anzahl der VPN-Tunnel auf der ASA erheblich ist, debug crypto condition peer A.B.C.D -Befehls vor dem Aktivieren der Debugs verwendet werden, damit die Debugausgaben nur den angegebenen Peer enthalten.

Cisco IOS Router-Fehlerbehebung

Um die IPSec IKEv1-Tunnelaushandlung auf einem Cisco IOS-Router zu beheben, können Sie die folgenden Debug-Befehle verwenden:

```
debug crypto ipsec
debug crypto isakmp
```

Hinweis: Wenn die Anzahl der VPN-Tunnel auf dem Cisco IOS erheblich ist, `debug crypto condition peer ipv4 A.B.C.D` müssen vor dem Aktivieren der Debugs verwendet werden, damit die Debugausgaben nur den angegebenen Peer einschließen.

Tipp: Im Cisco Dokument Most Common L2L and Remote Access IPSec VPN Troubleshooting Solutions (Häufigste Lösungen für L2L- und Remote-Zugriffs-IPSec-VPN) finden Sie weitere Informationen zur Fehlerbehebung bei Site-to-Site-VPNs.

Referenzen

- Wichtige Informationen zu Debug-Befehlen
- Problembehebung für IP-Sicherheit – Verständnis und Verwendung von Debug-Befehlen
- Gängigste Lösungen für die Behebung von Problemen mit L2L- und Remote Access IPSec VPN
- IPSec LAN-to-LAN-Prüfer
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

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