Dynamischer standortübergreifender IKEv2-VPN-Tunnel zwischen ASA und einem IOS-Router - Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie ein Site-to-Site Internet Key Exchange Version 2 (IKEv2) VPN-Tunnel zwischen einer Adaptive Security Appliance (ASA) und einem Cisco Router, dessen Router über eine dynamische IP-Adresse verfügt und die ASA über eine statische IP-Adresse auf den öffentlich zugänglichen Schnittstellen verfügt, konfiguriert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS® Version 15.1(1)T oder spätere Version
- Cisco ASA Version 8.4(1) oder spätere Version

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

In diesem Dokument werden folgende Szenarien erläutert:

- Szenario 1: Eine ASA wird mit einer statischen IP-Adresse konfiguriert, die eine benannte Tunnelgruppe verwendet, und der Router ist mit einer dynamischen IP-Adresse konfiguriert.

- Szenario 2: Eine ASA wird mit einer dynamischen IP-Adresse konfiguriert, und der Router ist mit einer dynamischen IP-Adresse konfiguriert.

- Szenario 3: Dieses Szenario wird hier nicht behandelt. In diesem Szenario wird die ASA mit einer statischen IP-Adresse konfiguriert, verwendet jedoch die Tunnelgruppe DefaultL2LG. Die Konfiguration hierfür ähnelt der Konfiguration, die im Artikel Konfigurationsbeispiel für den dynamischen Site-to-Site-IKEv2-VPN-Tunnel zwischen zwei ASAs beschrieben wird.

Der größte Konfigurationsunterschied zwischen Szenario 1 und 3 besteht in der vom Remote-Router verwendeten ISAKMP-ID (Internet Security Association and Key Management Protocol). Wenn die DefaultL2LGroup auf der statischen ASA verwendet wird, muss die ISAKMP-ID des Peers auf dem Router die Adresse der ASA sein. Wenn jedoch eine benannte Tunnelgruppe verwendet wird, muss die ISAKMP-ID des Peers auf dem Router mit dem auf der ASA konfigurierten Tunnelgruppennamen identisch sein. Dies wird mithilfe des folgenden Befehls auf dem Router erreicht:

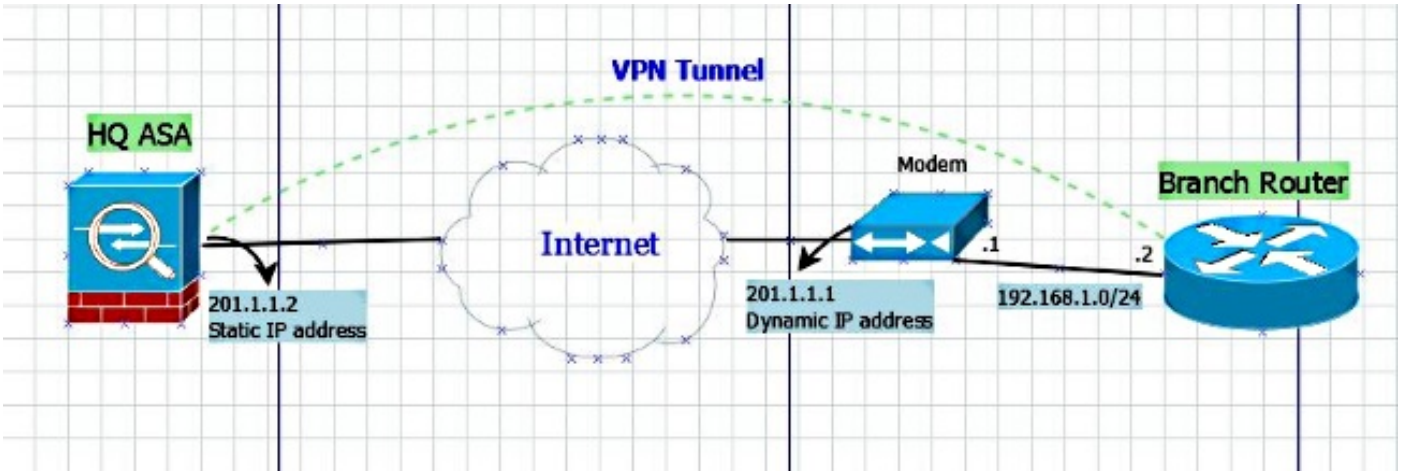
```
identity local key-id
```

Der Vorteil bei der Verwendung benannter Tunnelgruppen auf der statischen ASA besteht darin, dass bei Verwendung der DefaultL2LGroup die Konfiguration auf den dynamischen Remote-ASAs/Routern, die die vorinstallierten Schlüssel enthält, identisch sein muss und nicht viel Detailgenauigkeit bei der Einrichtung von Richtlinien ermöglicht.

Konfigurieren

Szenario 1

Netzwerkdiagramm



Konfiguration

In diesem Abschnitt wird die Konfiguration auf der ASA und dem Router anhand der Konfiguration der benannten Tunnelgruppe beschrieben.

Statische ASA-Konfiguration

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 201.1.1.2 255.255.255.0
!
crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
 protocol esp encryption aes
 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
crypto map vpn 1 ipsec-isakmp dynamic dmap
crypto map vpn interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

group-policy Site-to-Site internal
group-policy Site-to-Site attributes
 vpn-tunnel-protocol ikev2
tunnel-group S2S-IKEv2 type ipsec-l2l
tunnel-group S2S-IKEv2 general-attributes
 default-group-policy Site-to-Site
tunnel-group S2S-IKEv2 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco321
 ikev2 local-authentication pre-shared-key cisco123
```

Dynamische Routerkonfiguration

Der Dynamic Router wird fast genauso konfiguriert wie normalerweise, wenn der Router ein dynamischer Standort für den IKEv2 L2L-Tunnel ist, wobei ein Befehl hinzugefügt wird, wie hier gezeigt:

```
ip access-list extended vpn
 permit ip host 10.10.10.1 host 201.1.1.2

crypto ikev2 proposal L2L-Prop
 encryption 3des
 integrity sha1
 group 2 5
!
crypto ikev2 policy L2L-Pol
 proposal L2L-Prop
!
crypto ikev2 keyring L2L-Keyring
 peer vpn
 address 201.1.1.2
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
!
crypto ikev2 profile L2L-Prof
 match identity remote address 201.1.1.2 255.255.255.255
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map vpn 10 ipsec-isakmp
 set peer 201.1.1.2
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
!
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
```

Auf jedem dynamischen Peer ist die Schlüssel-ID also unterschiedlich, und auf der statischen ASA muss eine entsprechende Tunnelgruppe mit dem richtigen Namen erstellt werden. Dies erhöht auch die Granularität der Richtlinien, die auf einer ASA implementiert werden.

Szenario 2

> **Hinweis**: Diese Konfiguration ist nur möglich, wenn mindestens eine Seite ein Router ist. Wenn beide Seiten ASAs sind, funktioniert diese Konfiguration derzeit nicht. In Version 8.4 kann die ASA den FQDN (Fully Qualified Domain Name) nicht mit dem Befehl **set peer** (**Peer-Set**) verwenden, jedoch wurde eine CSCus37350-Erweiterung für zukünftige Versionen angefordert.

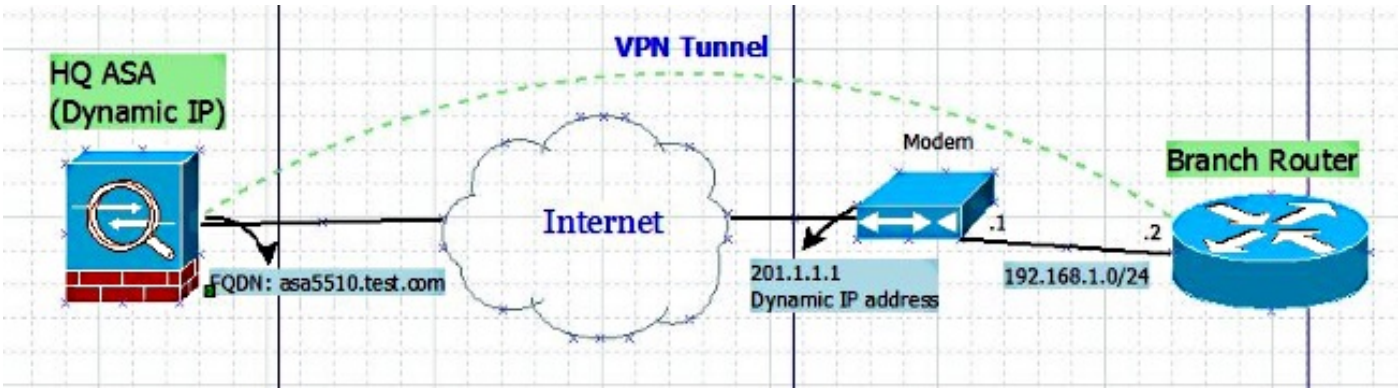
Wenn die IP-Adresse der Remote-ASA ebenfalls dynamisch ist, jedoch für die VPN-Schnittstelle ein vollqualifizierter Domänenname zugewiesen ist, definieren Sie stattdessen die IP-Adresse der Remote-ASA jetzt den FQDN der Remote-ASA mit dem folgenden Befehl auf dem Router:

```
C1941(config)#do show run | sec crypto map

crypto map vpn 10 ipsec-isakmp
 set peer <FQDN> dynamic
```

> **Tipp**: Das **dynamische** Schlüsselwort ist optional. Wenn Sie den Hostnamen eines Remote-IPsec-Peers über den Befehl **setpeer** angeben, können Sie auch das dynamische Schlüsselwort eingeben, das die DNS-Auflösung (Domain Name Server) des Hostnamens verzögert, bis der IPsec-Tunnel eingerichtet wurde.
>
> Durch die verzögerte Auflösung kann die Cisco IOS-Software erkennen, ob sich die IP-Adresse des Remote-IPsec-Peers geändert hat. So kann die Software den Peer unter der neuen IP-Adresse kontaktieren. Wenn das dynamische Schlüsselwort nicht ausgegeben wird, wird der Hostname sofort nach der Angabe aufgelöst. Die Cisco IOS-Software kann also keine Änderung der IP-Adresse erkennen und versucht daher, eine Verbindung zu der zuvor aufgelösten IP-Adresse herzustellen.

Netzwerkdiagramm



Konfiguration

Dynamische ASA-Konfiguration

Die Konfiguration auf der ASA entspricht der statischen ASA-Konfiguration mit nur einer Ausnahme, nämlich dass die IP-Adresse auf der physischen Schnittstelle nicht statisch definiert ist.

Routerkonfiguration

```
crypto ikev2 keyring L2L-Keyring
 peer vpn
 hostname asa5510.test.com
```

```
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
 !
crypto ikev2 profile L2L-Prof
 match identity remote fqdn domain test.com
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

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

crypto map vpn 10 ipsec-isakmp
 set peer asa5510.test.com dynamic
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
```

Überprüfen

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

Statische ASA

- Dies ist das Ergebnis des Befehls **show crypto IKEv2 sa det**:

```
IKEv2 SAs:

Session-id:23, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
120434199        201.1.1.2/4500        201.1.1.1/4500      READY    RESPONDER
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/915 sec
     Session-id: 23
     Status Description: Negotiation done
     Local spi: 97272A4B4DED4A5C       Remote spi: 67E01CB8E8619AF1
     Local id: 201.1.1.2
      Remote id: S2S-IKEv2
     Local req mess id: 43             Remote req mess id: 2
     Local next mess id: 43            Remote next mess id: 2
     Local req queued: 43              Remote req queued: 2
     Local window: 1                   Remote window: 5
     DPD configured for 10 seconds, retry 2
     NAT-T is detected  outside
Child sa: local selector  201.1.1.2/0 - 201.1.1.2/65535
          remote selector 10.10.10.1/0 - 10.10.10.1/65535
          ESP spi in/out: 0x853c02/0x41aa84f4
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

- Dies ist das Ergebnis des Befehls **show crypto ipsec sa**:

```
interface: outside
   Crypto map tag: dmap, seq num: 1, local addr: 201.1.1.2

     local ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
     remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
     current_peer: 201.1.1.1


     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 4, #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.: 201.1.1.2/4500, remote crypto endpt.: 201.1.1.1/4500
     path mtu 1500, ipsec overhead 82(52), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: 41AA84F4
     current inbound spi : 00853C02

   inbound esp sas:
     spi: 0x00853C02 (8731650)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, }
        slot: 0, conn_id: 94208, crypto-map: dmap
        sa timing: remaining key lifetime (kB/sec): (4101119/27843)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x0000001F
   outbound esp sas:
     spi: 0x41AA84F4 (1101694196)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, }
        slot: 0, conn_id: 94208, crypto-map: dmap
        sa timing: remaining key lifetime (kB/sec): (4055039/27843)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

Dynamischer Router

- Dies ist das Ergebnis des Befehls **show crypto IKEv2 a detail**:

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/1013 sec
     CE id: 1023, Session-id: 23
     Status Description: Negotiation done
```

```
     Local spi: 67E01CB8E8619AF1       Remote spi: 97272A4B4DED4A5C
      Local id: S2S-IKEv2
     Remote id: 201.1.1.2
     Local req msg id:  2              Remote req msg id:  48
     Local next msg id: 2              Remote next msg id: 48
     Local req queued:  2              Remote req queued:  48
     Local window:      5              Remote window:      1
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is detected inside
     Cisco Trust Security SGT is disabled
     Initiator of SA : Yes

 IPv6 Crypto IKEv2  SA
```

- Dies ist das Ergebnis des Befehls **show crypto ipsec sa**:

```
interface: GigabitEthernet0/0
   Crypto map tag: vpn, local addr 192.168.1.2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
  current_peer 201.1.1.2 port 4500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 192.168.1.2, remote crypto endpt.: 201.1.1.2
    plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0x853C02(8731650)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x41AA84F4(1101694196)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       conn id: 2006, flow_id: Onboard VPN:6, sibling_flags 80000040, crypto map: vpn
       sa timing: remaining key lifetime (k/sec): (4263591/2510)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x853C02(8731650)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       conn id: 2005, flow_id: Onboard VPN:5, sibling_flags 80000040, crypto map: vpn
       sa timing: remaining key lifetime (k/sec): (4263591/2510)
       IV size: 16 bytes
       replay detection support: Y
```

```
        Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

Dynamischer Router (mit Remote Dynamic ASA)

- Dies ist das Ergebnis des Befehls **show crypto IKEv2 a detail**:

```
C1941#show cry ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1516 sec
      CE id: 1034, Session-id: 24
      Status Description: Negotiation done
      Local spi: 98322AED6163EE83       Remote spi: 092A1E5620F6AA9C
       Local id: S2S-IKEv2
       Remote id: asa5510.test.com
      Local req msg id:  2              Remote req msg id:  73
      Local next msg id: 2              Remote next msg id: 73
      Local req queued:  2              Remote req queued:  73
      Local window:      5              Remote window:      1
      DPD configured for 0 seconds, retry 0
      Fragmentation not configured.
      Extended Authentication not configured.
      NAT-T is detected inside
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes

 IPv6 Crypto IKEv2  SA
```

> **Hinweis**: Die Remote-ID und die lokale ID in dieser Ausgabe ist die **benannte Tunnelgruppe, die** Sie auf der ASA definiert haben, um zu überprüfen, ob Sie zur richtigen Tunnelgruppe gehören. Dies kann auch überprüft werden, wenn Sie IKEv2 an beiden Enden debuggen.

Fehlerbehebung

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

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.

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

Verwenden Sie auf dem Cisco IOS-Router:

```
deb crypto ikev2 error
deb crypto ikev2 packet
deb crypto ikev2 internal
```

Auf der ASA:

```
deb crypto ikev2 protocol
deb crypto ikev2 platform
```