Voer DVTI op beveiligde firewall en Cisco IOS uit

Inhoud

Inleiding

Dit document beschrijft hoe u een Dynamic Virtual Tunnel Interface hub en spraakoplossing met EIGRP kunt implementeren op adaptieve security applicatie.

Voorwaarden

Vereisten

- Basiskennis van virtuele tunnelinterfaces op ASA
- Basis onderliggende connectiviteit tussen hub/spaken/ISP
- Basiskennis van EIGRP

- Adaptieve security applicatie versie 9.19(1) of hoger

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

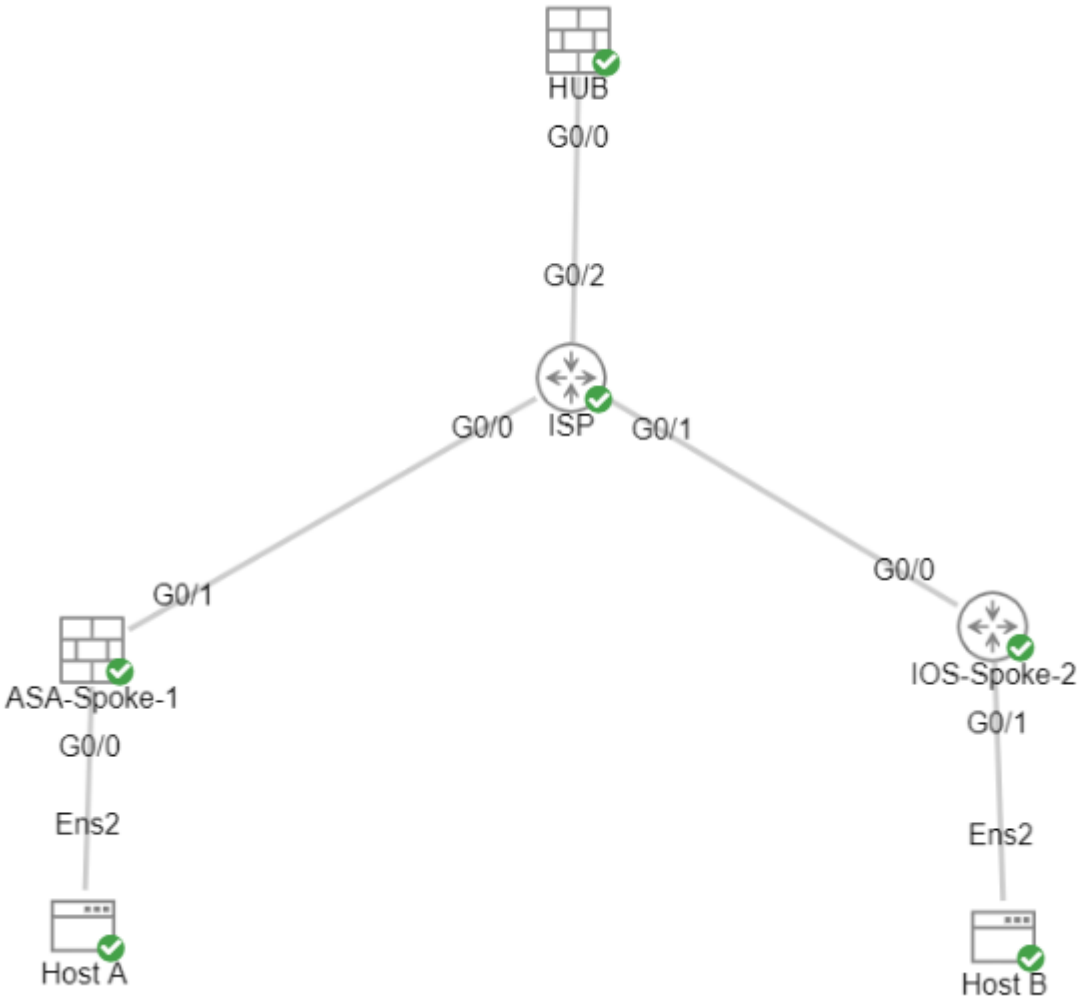
- Twee ASAv-apparaten, beide versie 9.19(1). Gebruikt voor Spoke 1 en de Hub
- Twee Cisco IOS® v-apparaten, versie 15.9(3)M4. Eén voor ISP-apparaat, één gebruikt voor Spoke 2.

- Twee Ubuntu-hosts voor generiek verkeer bedoeld voor de tunnels

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdiagram



Configuraties

De WAN-interfaceparameters en de IKEv2-cryptoparameters op de Hub ASA configureren

Voer de configuratiemodus in op de hub.

```
interface g0/0
ip address 198.51.100.1 255.255.255.0
nameif OUTSIDE
```

De IKEv2-parameters op de hub ASA configureren

Maak een IKEv2 beleid dat de fase 1 parameters van de IKE verbinding definieert.

```
crypto ikev2 policy 1      (The number is locally significant on the device, this determine the order in
encryption aes-256         (Defines the encryption parameter used to encrypt the initial communication b
integrity sha256           (Defines the integrity used to secure the initial communication between the d
group 21                   (Defines the Diffie-Hellman group used to protect the key exchange between de
prf sha256                 (Pseudo Random Function, an optional value to define, automatically chooses t
lifetime seconds 86400     (Controls the phase 1 rekey, specified in seconds. Optional value, as the def
```

Maak een IKEv2 IPsec-voorstel om de parameters van fase 2 te definiëren die worden gebruikt om het verkeer te beschermen.

```
crypto ipsec ikev2 ipsec-proposal NAME               (Name is locally signicant and is used as a refere
protocol esp encryption aes-256                      (specifies that Encapsulating Security Payload and
protocol esp integrity sha-256                       (specifies that Encapsulating Security Payload and
```

Maak een IPsec-profiel dat het IPsec-voorstel bevat.

```
    crypto ipsec profile NAME                   (This name is referenced on the Virtual-Template Interf
    set ikev2 ipsec-proposal NAME               (This is the name previously used when creating the ips
```

Een Loopback- en Virtual-Template-interface maken

```
interface loopback 1
ip address 172.16.50.254 255.255.255.255       (This IP address is used for all of the Virtual-Access I
nameif LOOP1
```

```
interface Virtual-Template 1 type tunnel
ip unnumbered LOOP1                               (Borrows the IP address specified in Loopback1 for al
nameif DVTI
tunnel source Interface OUTSIDE                   (Specifies the Interface that the tunnel terminates o
tunnel mode ipsec ipv4                            (Specifies that the mode uses ipsec, and uses ipv4)
tunnel protection ipsec profile NAME              (Reference the name of the previously created ipsec p
```

Een tunnelgroep maken en de tunnelinterface IPâ€™s adverteren via IKEv2 Exchange

Maak een tunnelgroep om het type tunnel en de verificatiemethode te specificeren.

```
tunnel-group DefaultL2LGroup ipsec-attributes             ('DefaultL2LGroup' is a default tunnel-group u
virtual-template 1                                        (This command ties the Virtual-Template previo
ikev2 remote-authentication pre-shared-key cisco123       (This specifies the remote authentication as a
ikev2 local-authentication pre-shared-key cisco123        (This specifies the local authentication as a
ikev2 route set Interface                                 (Advertises the VTI Interface IP over IKEv2 ex
```

Configureer EIGRP-routing op de hub ASA

```
router eigrp 100
network 172.16.50.254 255.255.255.255         (Advertise the IP address of the Loopback used for the Vir
```

De interfaces op de Spoke ASA configureren

Configureer de WAN-interface.

```
interface g0/1
ip address 203.0.113.1 255.255.255.0
nameif OUTSIDE-SPOKE-1
```

Configureer de LAN-interface.

```
interface g0/0
ip address 10.45.0.4 255.255.255.0
nameif INSIDE-SPOKE-1
```

Configureer een Loopback-interface.

```
interface loopback1
ip address 172.16.50.1 255.255.255.255
nameif Loop1
```

Configureer de IKEv2 Crypto Parameters op de Spoke ASA

Maak een IKEv2-beleid dat overeenkomt met de parameters op de hub.

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 21
prf sha256
```

```
lifetime 86400
```

Maak een IKEv2 IPsec-voorstel dat overeenkomt met de parameters op de hub.

```
crypto ipsec ikev2 ipsec-proposal NAME          (Name is locally signicant, this does not need to m
protocol esp encryption aes-256
protocol esp integrity sha-256
```

Maak een IPsec-profiel dat het IPsec-voorstel bevat.

```
crypto ipsec profile NAME              (This name is locally significant and is referenced in the S
set ikev2 ipsec-proposal NAME          (This is the name previously used when creating the ipsec-pr
```

De statische virtuele tunnelinterface op de spraak-ASA configureren

Configureer een statische virtuele tunnelinterface die naar de hub wijst. De spraakapparaten configureren reguliere statische virtuele tunnelinterfaces naar de hub, alleen de hub vereist een virtuele sjabloon.

```
interface tunnel1
ip unnumbered loopback1
nameif ASA-SPOKE-SVTI
tunnel destination  198.51.100.254          (Tunnel destination references the Hub ASA tunnel source
tunnel mode ipsec ipv4
tunnel protection ipsec profile NAME
```

Een tunnelgroep maken en de tunnelinterface IPâ€™s adverteren via IKEv2 Exchange

```
tunnel-group 198.51.100.1 type ipsec-l2l                  (This specifies the connection type as ip
tunnel-group 198.51.100.1 ipsec-attributes                (Ipsec attributes allows you to make char
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
ikev2 route set Interface
```

Configureer EIGRP-routing op de spraak-ASA

Creeer een autonoom systeem EIGRP en pas de gewenste te adverteren netwerken toe.

```
router eigrp 100
network 10.45.0.0 255.255.255.0                         (Advertises the Host-A network to the hub.
network 172.16.50.1 255.255.255.255                     (Advertises and utilizes the tunnel IP addr
```

De interfaces op de spraakrouter configureren

```
interface g0/0
ip address 192.0.2.1 255.255.255.0
no shut
```

```
interface g0/1
ip address 10.12.0.2
no shut
```

```
interface loopback1
ip address 172.16.50.2 255.255.255.255
```

Configureer de IKEv2-parameters en de AAA op de spraakrouter

Maak een IKEv2-voorstel om de parameters van fase 1 op de ASA aan te passen.

```
    crypto ikev2 proposal NAME       (These parameters must match the ASA IKEv2 Policy)
    encryption aes-cbc-256           (aes-cbc-256 is the same as the ASA aes-256. However, AES-GCM of ar
    integrity sha256
    group 21
```

Creëer een IKEv2-beleid om de voorstellen toe te voegen.

```
    crypto ikev2 policy NAME
    proposal NAME               (This is the name of the IKEv2 proposal created in the step ikev2)
```

Maak een IKEv2-autorisatiebeleid.

```
    crypto ikev2 authorization policy NAME      (IKEv2 authorization policy serves as a container of IKE
    route set Interface
```

Schakel AAA in op het apparaat.

```
    aaa new-model
```

Maak een AAA-autorisatienetwerk.

```
aaa authorization network NAME local                (Creates a name and method for aaa authorizatior
```

Maak een IKEv2-profiel dat een repository bevat van de niet-verhandelbare parameters van IKE SA, zoals lokale of externe identiteiten en verificatiemethoden.

```
crypto ikev2 profile NAME
match identity remote address  198.51.100.1    (Used to match the address of the Hub VTI source Inte
identity local address  192.0.2.1              (Defines the local IKE-ID of the router for this IKEv
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
no config-exchange request                      (Applies to Cisco IOS, Cisco IOS-XE devices do this b
aaa authorization group psk list NAME NAME      (Specifies an AAA method list and username for group
```

Maak een transformatie die is ingesteld om de versleutelings- en hashingparameters te definiëren die worden gebruikt om het tunnelverkeer te beschermen.

```
crypto ipsec transform-set NAME esp aes 256 esp-sha256-hmac
```

Maak een crypto IPsec-profiel voor de transformatie en IKEv2-profiel.

```
crypto ipsec profile NAME                 (Define the name of the ipsec-profile)
set transform-set NAME                    (Reference the name of the created transform set)
set ikev2-profile NAME                    (Reference the name of the created IKEv2 profile)
```

De statische virtuele tunnelinterface op de spraakrouter configureren

Configureer een statische virtuele tunnelinterface die naar de hub wijst.

```
interface tunnel1
ip unnumbered loopback1
tunnel source g0/0
tunnel mode ipsec ipv4
tunnel destination 198.51.100.1
tunnel protection ipsec profile NAME            (Reference the name of the created ipsec profile. T
```

Configureer EIGRP-routing op de spraakrouter

Creeer een autonoom systeem EIGRP en pas de gewenste te adverteren netwerken toe.

```
router eigrp 100
network 172.16.50.2 0.0.0.0             (Routers advertise EIGRP networks with the wildcard mask. Th
network 10.12.0.0 0.0.0.255             (Advertises the Host-B network to the hub. This allows the H
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

ASA-routing:

```
show run router

show eigrp topology

show eigrp neighbors

show route [eigrp]
```

ASA Crypto:

```
show run crypto ikev2

show run crypto ipsec

show run tunnel-group [NAME]

show crypto ikev2 sa

show crypto ipsec sa peer X.X.X.X
```

ASA virtuele sjablonen en virtuele toegang:

```
show run interface virtual-template # type tunnel

show interface virtual-access #
```

Cisco IOS-routing:

```
show run | sec eigrp

show ip eigrp topology

show ip eigrp neighbors
```

```
show ip route
show ip route eigrp
```

Cisco IOS-encryptie:

```
show run | sec cry
show crypto ikev2 sa
show crypto ipsec sa peer X.X.X.X
```

Cisco IOS-tunnelinterface:

```
show run interface tunnel#
```

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

ASA debugs:

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug ip eigrp #
debug ip eigrp neighbor X.X.X.X
```

Cisco IOS-debuggen:

```
debug crypto ikev2
debug crypto ikev2 error
debug crypto ikev2 packet
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

```
debug ip eigrp #

debug ip eigrp neighbor X.X.X.X
```

Gerelateerde informatie

- **Cisco technische ondersteuning en downloads**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.