Implementierung von DVTI auf einer sicheren Firewall und Cisco IOS

Inhalt

Einleitung

In diesem Dokument wird die Implementierung einer Hub-and-Spoke-Lösung mit Dynamic Virtual Tunnel Interface und EIGRP auf der Adaptive Security Appliance beschrieben.

Voraussetzungen

Anforderungen

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

- Grundlegendes Verständnis von virtuellen Tunnelschnittstellen auf ASA
- Grundlegende Underlay-Verbindungen zwischen Hub/Spokes/ISP
- Grundlegendes Verständnis des EIGRP

- Adaptive Security Appliance Version 9.19(1) oder höher

Verwendete Komponenten

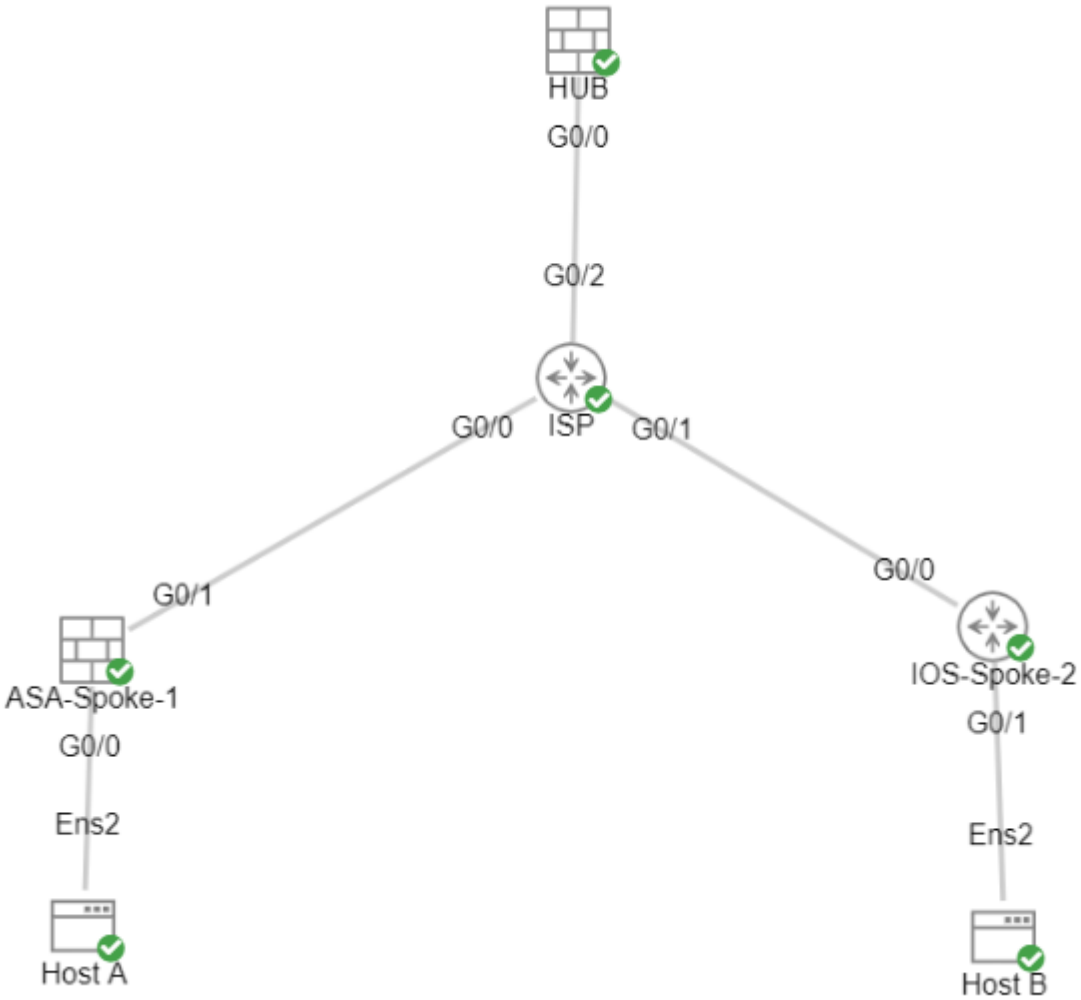
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Zwei ASAv-Geräte, beide Version 9.19(1). Für Spoke 1 und Hub verwendet
- Zwei Cisco IOS® v-Geräte Version 15.9(3)M4. Eines für ISP-Gerät, eines für Spoke 2.
- Zwei Ubuntu-Hosts für generischen Datenverkehr für die Tunnel

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 kennen.

Konfigurieren

Netzwerkdiagramm



Konfigurationen

Konfigurieren der WAN-Schnittstelle und der IKEv2-Verschlüsselungsparameter auf der Hub-ASA

Wechseln Sie auf dem Hub in den Konfigurationsmodus.

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

Konfigurieren der IKEv2-Parameter auf der Hub-ASA

Erstellen Sie eine IKEv2-Richtlinie, die die Phase-1-Parameter der IKE-Verbindung definiert.

```
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
```

Erstellen Sie einen IKEv2-IPsec-Vorschlag, um die Parameter für Phase 2 zum Schutz des Datenverkehrs zu definieren.

```
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
```

Erstellen Sie ein IPsec-Profil, das den IPsec-Vorschlag enthält.

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

Erstellen einer Loopback- und Virtual-Template-Schnittstelle

```
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
```

Erstellen Sie eine Tunnelgruppe, und geben Sie die Tunnel-Schnittstellen-IPs über IKEv2 Exchange an.

Erstellen Sie eine Tunnelgruppe, um den Tunneltyp und die Authentifizierungsmethode anzugeben.

```
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
```

Konfigurieren von EIGRP-Routing auf der 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
```

Konfigurieren der Schnittstellen auf der Spoke-ASA

Konfigurieren der WAN-Schnittstelle

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

Konfigurieren der LAN-Schnittstelle

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

Konfigurieren einer Loopback-Schnittstelle

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

Konfigurieren der IKEv2-Verschlüsselungsparameter auf der Spoke-ASA

Erstellen Sie eine IKEv2-Richtlinie, die mit den Parametern auf dem Hub übereinstimmt.

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 21
prf sha256
lifetime 86400
```

Erstellen Sie einen IKEv2-IPsec-Vorschlag, der mit den Parametern auf dem Hub übereinstimmt.

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

Erstellen Sie ein IPsec-Profil, das den IPsec-Vorschlag enthält.

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

Konfigurieren der statischen virtuellen Tunnelschnittstelle auf der Spoke-ASA

Konfigurieren Sie eine statische virtuelle Tunnelschnittstelle, die auf den Hub verweist. Die Spoke-Geräte konfigurieren reguläre statische virtuelle Tunnelschnittstellen zum Hub, nur für den Hub ist eine virtuelle Vorlage erforderlich.

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

Erstellen Sie eine Tunnelgruppe, und geben Sie die Tunnel-Schnittstellen-IPs über IKEv2 Exchange an.

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

Konfigurieren von EIGRP-Routing auf der Spoke-ASA

Erstellen Sie ein autonomes EIGRP-System und wenden Sie die gewünschten Netzwerke an, die beworben werden sollen.

```
router eigrp 100
network 10.45.0.0 255.255.255.0        (Advertises the Host-A network to the hub. This allows the hub to
network 172.16.50.1 255.255.255.255    (Advertises and utilizes the tunnel IP address to form an EIGRP n
```

Konfigurieren der Schnittstellen auf dem Spoke-Router

```
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
```

Konfigurieren der IKEv2-Parameter und AAA auf dem Spoke-Router

Erstellen Sie ein IKEv2-Angebot, das mit den Phase-1-Parametern auf der ASA übereinstimmt.

```
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 any va
                                  and is not a matching parameter with plain AES.)
integrity sha256
group 21
```

Erstellen Sie eine IKEv2-Richtlinie, um die Angebote hinzuzufügen.

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

Erstellen einer IKEv2-Autorisierungsrichtlinie

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

Aktivieren Sie AAA auf dem Gerät.

```
aaa new-model
```

Erstellen Sie ein AAA-Autorisierungsnetzwerk.

```
aaa authorization network NAME local    (Creates a name and method for aaa authorization that is referen
```

Erstellen Sie ein IKEv2-Profil, das ein Repository der nicht übertragbaren Parameter der IKE SA enthält, z. B. lokale oder entfernte Identitäten und Authentifizierungsmethoden.

```
crypto ikev2 profile NAME
match identity remote address  198.51.100.1    (Used to match the address of the Hub VTI source Interfac
identity local address  192.0.2.1              (Defines the local IKE-ID of the router for this IKEv2 pr
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 by de
                                                which is unsupported on the ASA.)
aaa authorization group psk list NAME NAME     (Specifies an AAA method list and username for group. The
```

Erstellen Sie einen Transformationssatz, um die Verschlüsselungs- und Hashing-Parameter zu definieren, die zum Schutz des getunnelten Datenverkehrs verwendet werden.

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

Erstellen Sie ein Krypto-IPsec-Profil, das den Transformationssatz und das IKEv2-Profil enthält.

```
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.)
```

Konfigurieren der statischen virtuellen Tunnelschnittstelle auf dem Spoke-Router

Konfigurieren Sie eine statische virtuelle Tunnelschnittstelle, die auf den Hub verweist.

```
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. This applies
                                           and transform set parameters to the tunnel Interface.)
```

Konfigurieren von EIGRP-Routing auf dem Spoke-Router

Erstellen Sie ein autonomes EIGRP-System und wenden Sie die gewünschten Netzwerke an, die beworben werden sollen.

```
router eigrp 100
network 172.16.50.2 0.0.0.0     (Routers advertise EIGRP networks with the wildcard mask.
                                 This advertises the tunnel IP address to allow the device to form an EI
network 10.12.0.0 0.0.0.255      (Advertises the Host-B network to the hub. This allows the hub to notif
```

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

ASA-Routing:

```
show run router

show eigrp topology

show eigrp neighbors

show route [eigrp]
```

ASA-Verschlüsselung:

```
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 Virtual-Template und Virtual-Access:

```
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-Verschlüsselung:

```
show run | sec cry

show crypto ikev2 sa

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

Cisco IOS-Tunnelschnittstelle:

```
show run interface tunnel#
```

Fehlerbehebung

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

ASA-Fehlersuche:

```
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-Debugger:

```
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
```

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

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.