Implemente DVTI en Secure Firewall y Cisco IOS

Contenido

Introducción

Este documento describe cómo implementar una solución radial de interfaz de túnel virtual dinámico con EIGRP en Adaptive Security Appliance.

Prerequisites

Requirements

- Comprensión básica de las interfaces de túnel virtual en ASA
- Conectividad subyacente básica entre concentradores/radios/ISP
- Conocimientos básicos de EIGRP

- Adaptive Security Appliance versión 9.19(1) o superior

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

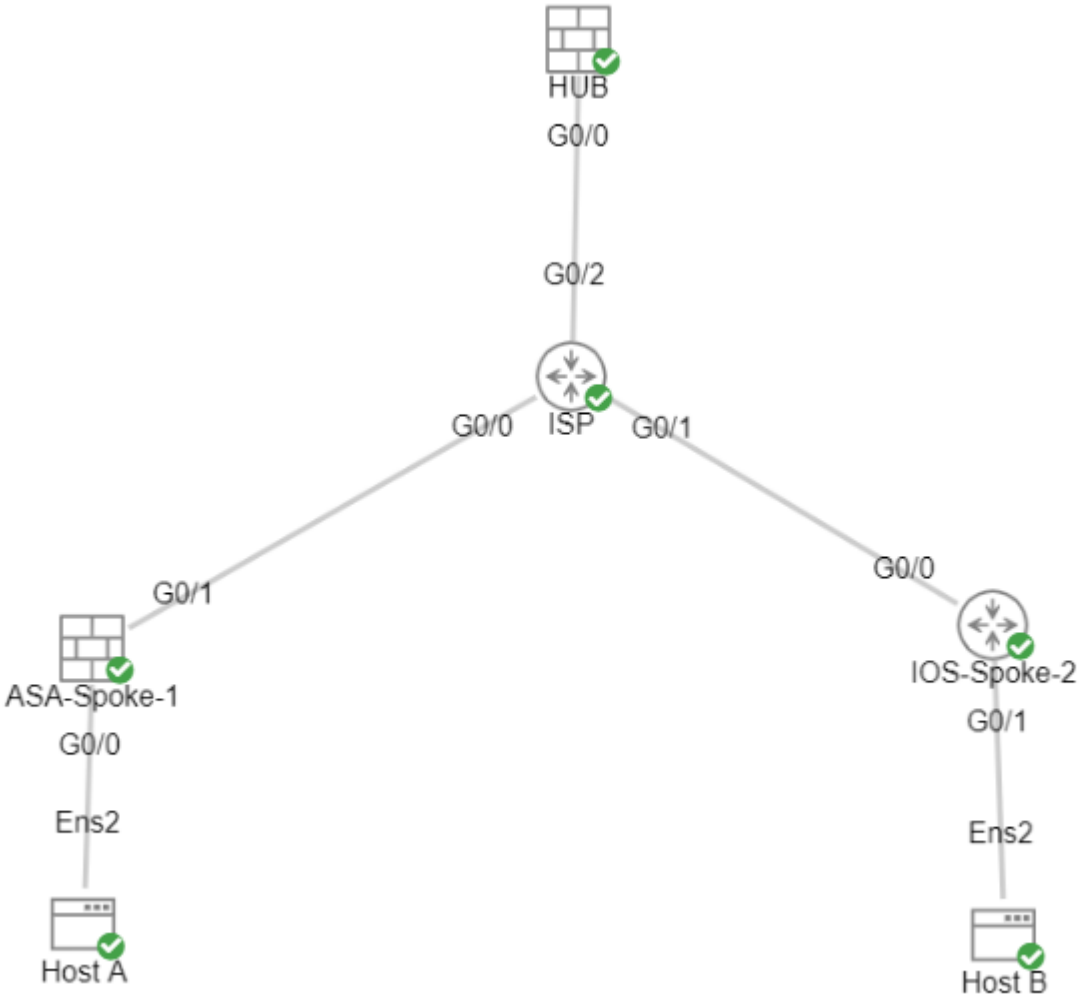
- Dos dispositivos ASAv, ambos versión 9.19(1). Utilizado para el spoke 1 y el hub
- Dos dispositivos Cisco IOS® v versión 15.9(3)M4. Uno para el dispositivo ISP, otro para Spoke 2.

- Dos hosts Ubuntu para el tráfico genérico destinado a los túneles

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



Configuraciones

Configure la interfaz WAN y los parámetros de cifrado IKEv2 en el ASA del hub

Entre en el modo de configuración del hub.

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

Configuración de los parámetros IKEv2 en el ASA del hub

Cree una política IKEv2 que defina los parámetros de fase 1 de la conexión IKE.

```
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
```

Cree una propuesta IKEv2 IPsec para definir los parámetros de fase 2 utilizados para proteger el tráfico.

```
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
```

Cree un perfil IPsec que contenga la propuesta de IPsec.

```
    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
```

Creación de una Interfaz de Loopback y Plantilla Virtual

```
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
```

Cree un grupo de túnel y anuncie las IP de la interfaz de túnel a través de IKEv2 Exchange

Cree un grupo de túnel para especificar el tipo de túnel y el método de autenticación.

```
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
```

Configuración del routing EIGRP en el ASA del hub

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

Configuración de las Interfaces en el Spoke ASA

Configuración de la interfaz WAN.

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

Configuración de la interfaz LAN.

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

Configuración de una interfaz de loopback.

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

Configuración de los Parámetros Crypto IKEv2 en el Spoke ASA

Cree una política IKEv2 que coincida con los parámetros del hub.

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

```
lifetime 86400
```

Cree una propuesta de IPsec IKEv2 que coincida con los parámetros del 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
```

Cree un perfil IPsec que contenga la propuesta de IPsec.

```
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
```

Configuración de la Interfaz de Túnel Virtual Estática en el Spoke ASA

Configure una interfaz de túnel virtual estática que apunte al hub. Los dispositivos spoke configuran interfaces de túnel virtual estáticas regulares al hub; sólo el hub requiere una plantilla virtual.

```
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
```

Cree un Grupo de Túnel y Anuncie las IPs de la Interfaz de Túnel a través de 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
```

Configuración del Ruteo EIGRP en el Spoke ASA

Cree un sistema autónomo EIGRP y aplique las redes deseadas que se anunciarán.

```
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 addi
```

Configuración de las interfaces en el router de radio

```
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
```

Configure los parámetros IKEv2 y AAA en el router de radio

Cree una propuesta IKEv2 para que coincida con los parámetros de la fase 1 en el ASA.

```
    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
```

Cree una política IKEv2 para adjuntar las propuestas.

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

Cree una política de autorización IKEv2.

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

Active AAA en el dispositivo.

```
aaa new-model
```

Cree una red de autorización AAA.

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

Cree un perfil IKEv2 que contenga un repositorio de los parámetros no negociables de la SA IKE, como identidades locales o remotas y métodos de autenticación.

```
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
```

Cree un conjunto de transformación para definir los parámetros de cifrado y de hash utilizados para proteger el tráfico tunelado.

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

Cree un perfil IPSec de cifrado para alojar el conjunto de transformación y el perfil IKEv2.

```
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)
```

Configuración de la Interfaz de Túnel Virtual Estática en el Router Spoke

Configure una interfaz de túnel virtual estática que apunte al hub.

```
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
```

Configuración del Ruteo EIGRP en el Router Spoke

Cree un sistema autónomo EIGRP y aplique las redes deseadas que se anunciarán.

```
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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Routing de ASA:

```
show run router

show eigrp topology

show eigrp neighbors

show route [eigrp]
```

Cifrado ASA:

```
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 y Virtual-Accesses:

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

show interface virtual-access #
```

Routing de Cisco IOS:

```
show run | sec eigrp
show ip eigrp topology
show ip eigrp neighbors
show ip route
show ip route eigrp
```

Cisco IOS Crypto:

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

Interfaz de túnel de Cisco IOS:

```
show run interface tunnel#
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Depuraciones de ASA:

```
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
```

Depuraciones de Cisco IOS:

```
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
```

Información Relacionada

- **Asistencia técnica y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).