Implemente o DVTI no Secure Firewall e no Cisco IOS

Contents

Introdução

Este documento descreve como implementar uma solução de hub e spoke Dynamic Virtual Tunnel Interface com EIGRP no Adaptive Security Appliance.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica das interfaces de túnel virtual no ASA
- Conectividade básica da base entre Hub/Spokes/ISP
- Entendimento básico do EIGRP

- Adaptive Security Appliance versão 9.19(1) ou posterior

Componentes Utilizados

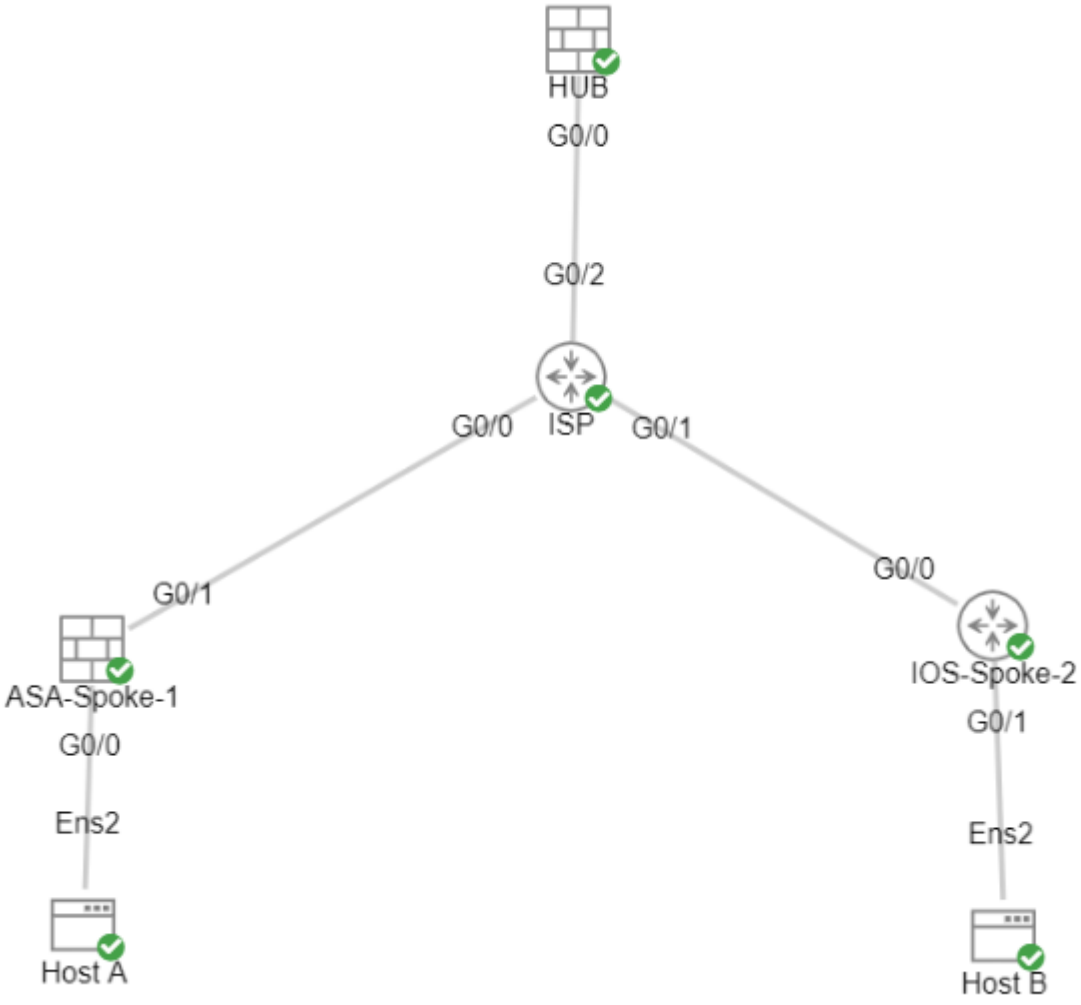
As informações neste documento são baseadas nestas versões de software e hardware:

- Dois dispositivos ASAv, ambos versão 9.19(1). Utilizado para Spoke 1 e o Hub
- Dois dispositivos Cisco IOS® v versão 15.9(3)M4. Um para o dispositivo ISP, um utilizado para Spoke 2.
- Dois hosts Ubuntu para tráfego genérico destinado aos túneis

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Configurações

Configurar a interface WAN e os parâmetros de criptografia IKEv2 no ASA de hub

Entre no modo de configuração no hub.

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

Configurar os parâmetros IKEv2 no ASA de hub

Crie uma política IKEv2 que defina os parâmetros da Fase 1 da conexão 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
```

Crie uma proposta IKEv2 IPsec para definir os parâmetros da Fase 2 usados para proteger o tráfego.

```
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
```

Crie um perfil IPsec que contenha a proposta IPsec.

```
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
```

Criar uma interface de modelo virtual e de loopback

```
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
```

Crie um grupo de túneis e anuncie os IPs da interface de túnel através do IKEv2 Exchange

Crie um tunnel-group para especificar o tipo de túnel e o método de autenticação.

```
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
```

Configurar o Roteamento EIGRP no ASA do Hub

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

Configurar as interfaces no ASA spoke

Configurar a interface WAN.

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

Configurar a interface LAN.

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

Configure uma interface de loopback.

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

Configurar os parâmetros de criptografia IKEv2 no ASA spoke

Crie uma política IKEv2 que corresponda aos parâmetros no hub.

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

Crie uma proposta IKEv2 IPsec que corresponda aos parâmetros no hub.

```
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
```

Crie um perfil IPsec que contenha a proposta IPsec.

```
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
```

Configure a interface de túnel virtual estático no ASA spoke

Configure uma Interface de Túnel Virtual estática apontando para o hub. Os dispositivos spoke configuram interfaces estáticas regulares de túnel virtual para o hub, somente o hub requer um modelo virtual.

```
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
```

Crie um grupo de túneis e anuncie os IPs da interface de túnel através do IKEv2 Exchange

```
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
```

Configurar o Roteamento EIGRP no ASA Spoke

Crie um sistema autônomo EIGRP e aplique as redes desejadas a serem anunciadas.

```
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
```

Configure as interfaces no roteador spoke

```
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 os parâmetros IKEv2 e AAA no roteador spoke

Crie uma proposta IKEv2 para corresponder aos parâmetros da Fase 1 no 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 any va
                                  and is not a matching parameter with plain AES.)
integrity sha256
group 21
```

Crie uma política IKEv2 para anexar as propostas.

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

Crie uma política de autorização IKEv2.

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

```
route set Interface
```

Ative o AAA no dispositivo.

```
aaa new-model
```

Crie uma rede de autorização AAA.

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

Crie um Perfil IKEv2 que contenha um repositório de parâmetros não negociáveis do SA IKE, como identidades locais ou remotas e métodos de autenticação.

```
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
```

Crie um conjunto de transformação para definir os parâmetros de criptografia e hash usados para proteger o tráfego em túnel.

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

Crie um perfil IPsec de criptografia para hospedar o conjunto de transformação e o 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.)
```

Configure a interface de túnel virtual estático no roteador spoke

Configure uma Interface de Túnel Virtual estática apontando para o 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. This applies
                                           and transform set parameters to the tunnel Interface.)
```

Configurar o roteamento EIGRP no roteador spoke

Crie um sistema autônomo EIGRP e aplique as redes desejadas a serem anunciadas.

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Roteamento ASA:

```
show run router

show eigrp topology

show eigrp neighbors

show route [eigrp]
```

Criptografia 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
```

Modelo virtual ASA e acessos virtuais:

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

show interface virtual-access #
```

Roteamento do Cisco IOS:

```
show run | sec eigrp

show ip eigrp topology

show ip eigrp neighbors

show ip route

show ip route eigrp
```

Criptografia do Cisco IOS:

```
show run | sec cry

show crypto ikev2 sa

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

Interface de túnel do Cisco IOS:

```
show run interface tunnel#
```

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Depurações do 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
```

Depurações do 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
```

Informações Relacionadas

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.