在安全防火牆和Cisco IOS上實施DVTI

目錄

簡介

本文檔介紹如何在自適應安全裝置上使用EIGRP實施動態虛擬隧道介面中心輻射解決方案。

必要條件

需求

思科建議您瞭解以下主題：

- 對ASA上的虛擬通道介面的基本瞭解
- 集線器/輻條/ISP之間的基本底層連線
- 對EIGRP有基礎認識

- 自適應安全裝置9.19(1)版或更高版本

採用元件

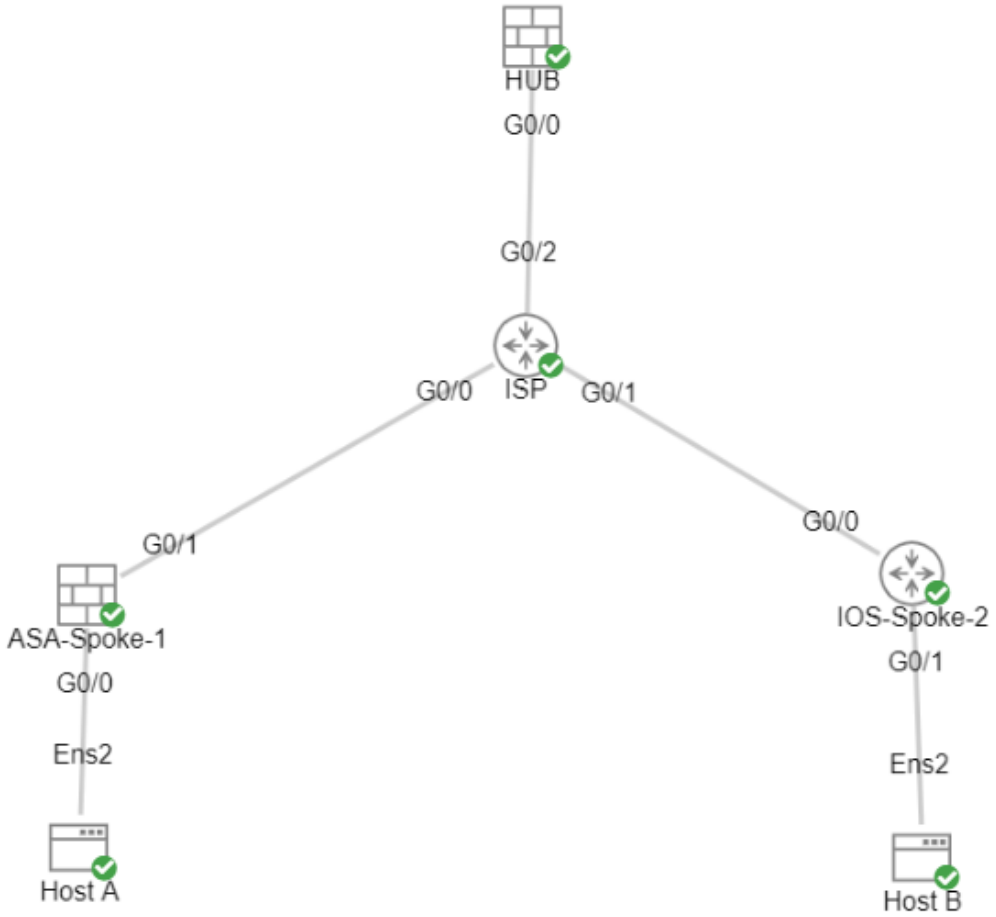
本文中的資訊係根據以下軟體和硬體版本：

- 兩台ASAv裝置，均為9.19(1)版。用於分支1和中心
- 兩個Cisco IOS® v裝置版本15.9(3)M4。一個用於ISP裝置，一個用於分支2。
- 兩台Ubuntu主機連線到用於通道的通用流量

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



組態

在中心ASA上配置WAN介面和IKEv2加密引數

進入集線器上的配置模式。

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

在中心ASA上配置IKEv2引數

建立定義IKE連線的階段1引數的IKEv2策略。

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

建立IKEv2 IPsec建議以定義用於保護流量的第2階段引數。

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

建立包含IPsec建議的IPsec配置檔案。

```
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-
```

建立環回和虛擬模板介面

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

```
interface Virtual-Template 1 type tunnel
ip unnumbered LOOP1                            (Borrows the IP address specified in Loopback1 for a
nameif DVTI
tunnel source Interface OUTSIDE                (Specifies the Interface that the tunnel terminates
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
```

建立隧道組並通過IKEv2 Exchange通告隧道介面IP

建立隧道組以指定隧道型別和身份驗證方法。

```
tunnel-group DefaultL2LGroup ipsec-attributes            ('DefaultL2LGroup' is a default tunnel-group
virtual-template 1                                       (This command ties the Virtual-Template previ
ikev2 remote-authentication pre-shared-key cisco123      (This specifies the remote authentication as
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 e
```

在中心ASA上配置EIGRP路由

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

配置分支ASA上的介面

配置WAN介面。

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

配置LAN介面。

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

配置環回介面。

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

在分支ASA上配置IKEv2加密引數

建立與集線器上的引數匹配的IKEv2策略。

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

建立與集線器上的引數匹配的IKEv2 IPsec提議。

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

建立包含IPsec建議的IPsec配置檔案。

```
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-propo
```

在分支ASA上配置靜態虛擬隧道介面

配置指向集線器的靜態虛擬通道介面。 分支裝置配置到集線器的常規靜態虛擬通道介面，只有集線器需要虛擬模板。

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

建立隧道組並通過IKEv2 Exchange通告隧道介面IP

```
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
```

在分支ASA上配置EIGRP路由

建立EIGRP自治系統並應用要通告的所需網路。

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

配置分支路由器上的介面

```
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
```

在分支路由器上配置IKEv2引數和AAA

建立IKEv2方案以匹配ASA上的第1階段引數。

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

建立IKEv2策略以附加提議。

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

建立IKEv2授權策略。

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

在裝置上啟用AAA。

```
aaa new-model
```

建立AAA授權網路。

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

建立IKEv2配置檔案，該配置檔案包含IKE SA不可協商的引數的儲存庫，例如本地或遠端身份和身份驗證方法。

```
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 p
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
```

建立轉換集，以定義用於保護隧道流量的加密和雜湊引數。

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

建立用於容納轉換集和IKEv2配置檔案的加密IPsec配置檔案。

```
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.)
```

在分支路由器上配置靜態虛擬隧道介面

配置指向集線器的靜態虛擬通道介面。

```
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.)
```

在分支路由器上配置EIGRP路由

建立EIGRP自治系統並應用要通告的所需網路。

```
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 E
network 10.12.0.0 0.0.0.255      (Advertises the Host-B network to the hub. This allows the hub to noti
```

驗證

使用本節內容，確認您的組態是否正常運作。

ASA路由：

```
show run router

show eigrp topology

show eigrp neighbors

show route [eigrp]
```

ASA加密：

```
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虛擬模板和虛擬訪問：

```
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 Crypto:

```
show run | sec cry

show crypto ikev2 sa

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

Cisco IOS通道介面：

```
show run interface tunnel#
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

ASA調試：

```
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調試：

```
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
```

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。