在安全防火墙和Cisco IOS上实施DVTI

目录

简介

本文档介绍如何在自适应安全设备上使用EIGRP实施动态虚拟隧道接口中心辐射型解决方案。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解ASA上的虚拟隧道接口
- 集线器/辐条/ISP之间的基本底层连接
- 对EIGRP的基本了解

- 自适应安全设备9.19(1)版或更高版本

使用的组件

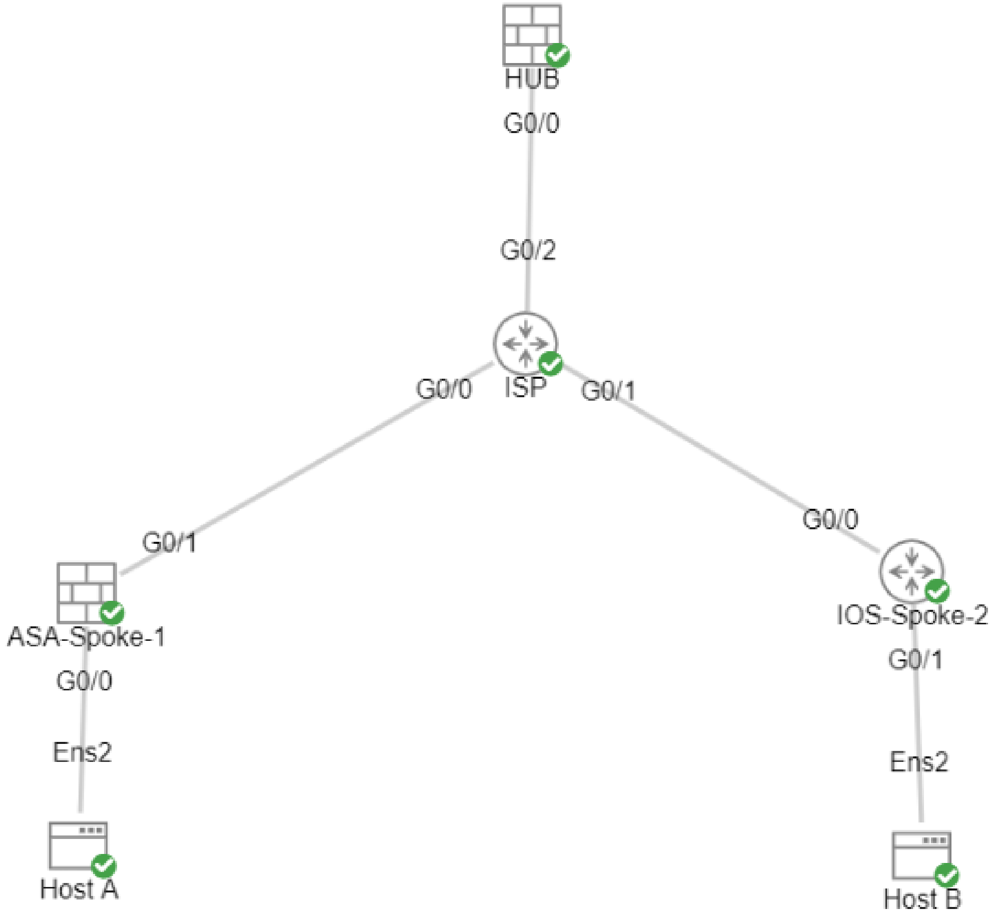
本文档中的信息基于以下软件和硬件版本：

- 两台ASAv设备，均为版本9.19(1)。用于分支1和中心
- 两个Cisco IOS® v设备版本15.9(3)M4。一个用于ISP设备，一个用于分支2。
- 两个Ubuntu主机到用于隧道的通用流量

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



配置

在集线器ASA上配置WAN接口和IKEv2加密参数

进入集线器的配置模式。

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

在集线器ASA上配置IKEv2参数

创建定义IKE连接的阶段1参数的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 b
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
```

创建IKEv2 IPsec建议以定义用于保护流量的第2阶段参数。

```
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
```

创建包含IPsec建议的IPsec配置文件。

```
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-
```

创建环回和虚拟模板接口

```
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
```

创建隧道组并通过IKEv2交换通告隧道接口IP

创建隧道组以指定隧道类型和身份验证方法。

```
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
```

在集线器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上的接口

配置 WAN 接口.

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

配置LAN接口

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

配置一个环回接口。

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

在分支ASA上配置IKEv2加密参数

创建与集线器上的参数匹配的IKEv2策略。

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

创建与集线器上的参数匹配的IKEv2 IPsec提议。

```
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
```

创建包含IPsec建议的IPsec配置文件。

```
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上配置静态虚拟隧道接口

配置指向集线器的静态虚拟隧道接口。 分支设备配置到集线器的常规静态虚拟隧道接口，只有集线器需要虚拟模板。

```
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
```

创建隧道组并通过IKEv2交换通告隧道接口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

创建EIGRP自治系统并应用要通告的所需网络。

```
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接口

```
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IKEv2参数和AAA

创建IKEv2建议以匹配ASA上的第1阶段参数。

```
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
```

创建IKEv2策略以附加提议。

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

创建IKEv2授权策略。

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

在设备上启用AAA。

```
aaa new-model
```

创建AAA授权网络。

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

创建包含IKE SA不可协商参数的存储库的IKEv2配置文件，例如本地或远程身份和身份验证方法。

```
crypto ikev2 profile NAME
match identity remote address  198.51.100.1    (Used to match the address of the Hub VTI source Interfa
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 d
                                                which is unsupported on the ASA.)
aaa authorization group psk list NAME NAME     (Specifies an AAA method list and username for group. Th
```

创建转换集以定义用于保护隧道流量的加密和散列参数。

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

创建用于容纳转换集和IKEv2配置文件的加密IPsec配置文件。

```
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静态虚拟隧道接口

配置指向集线器的静态虚拟隧道接口。

```
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 applie
                                           and transform set parameters to the tunnel Interface.)
```

在分支路由器上配置EIGRP路由

创建EIGRP自治系统并应用要通告的所需网络。

```
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
```

验证

使用本部分可确认配置能否正常运行。

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虚拟模板和虚拟访问：

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

```
show interface virtual-access #
```

Cisco IOS路由：

```
show run | sec eigrp
```

```
show ip eigrp topology
```

```
show ip eigrp neighbors
```

```
show ip route
```

```
show ip route eigrp
```

Cisco IOS加密：

```
show run | sec cry
```

```
show crypto ikev2 sa
```

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

Cisco IOS隧道接口：

```
show run interface tunnel#
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

ASA调试：

```
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调试：

```
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
```

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。