Mise en oeuvre de DVTI sur Secure Firewall et Cisco IOS

Table des matières

Introduction

Ce document décrit comment implémenter une solution hub and spoke d'interface de tunnel virtuel dynamique avec EIGRP sur un dispositif de sécurité adaptatif.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base des interfaces de tunnel virtuel sur ASA
- Connectivité sous-jacente de base entre concentrateur/satellites/FAI
- Compréhension de base du protocole EIGRP

- Adaptive Security Appliance version 9.19(1) ou ultérieure

Composants utilisés

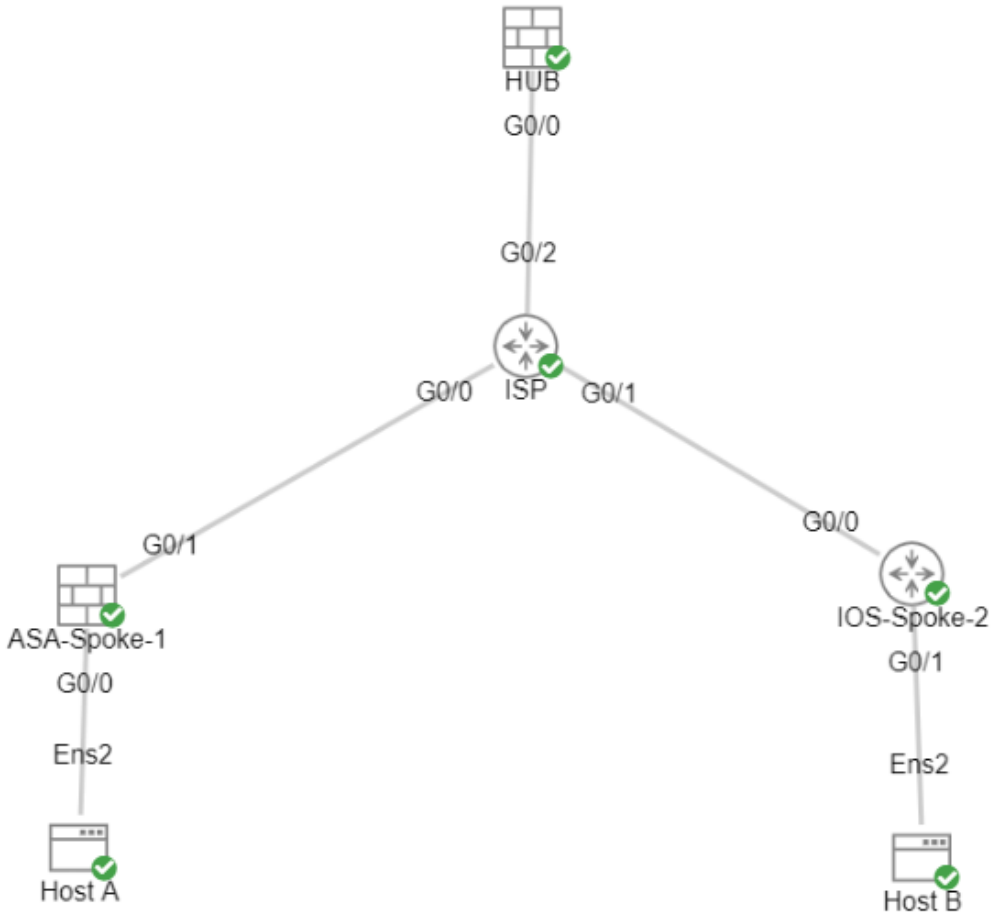
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Deux périphériques ASAv, tous deux version 9.19(1). Utilisé pour le satellite 1 et le concentrateur
- Deux périphériques Cisco IOS® v version 15.9(3)M4. Un pour le périphérique ISP, un utilisé pour Spoke 2.
- Deux hôtes Ubuntu pour le trafic générique destiné aux tunnels

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Diagramme du réseau



Configurations

Configurez l'interface WAN et les paramètres de chiffrement IKEv2 sur le concentrateur ASA

Passez en mode de configuration sur le concentrateur.

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

Configuration des paramètres IKEv2 sur le concentrateur ASA

Créez une stratégie IKEv2 qui définit les paramètres de phase 1 de la connexion IKE.

```
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
```

Créez une proposition IKEv2 IPsec pour définir les paramètres de Phase 2 utilisés pour protéger le trafic.

```
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
```

Créez un profil IPsec contenant la proposition 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-
```

Créer une interface de bouclage et de modèle virtuel

```
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
```

Création d'un groupe de tunnels et annonce des adresses IP d'interface de tunnel via IKEv2 Exchange

Créez un groupe de tunnels pour spécifier le type de tunnel et la méthode d'authentification.

```
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
```

Configuration du routage EIGRP sur le concentrateur ASA

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

Configuration des interfaces sur l'ASA satellite

Configurer l'interface WAN

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

Configurez l'interface LAN.

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

Configurer une interface de bouclage

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

Configuration des paramètres de chiffrement IKEv2 sur l'ASA satellite

Créez une stratégie IKEv2 correspondant aux paramètres du concentrateur.

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

Créez une proposition IKEv2 IPsec qui correspond aux paramètres du concentrateur.

```
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
```

Créez un profil IPsec contenant la proposition 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-propo
```

Configuration de l'interface de tunnel virtuel statique sur l'ASA satellite

Configurez une interface de tunnel virtuel statique pointant vers le concentrateur. Les périphériques en étoile configurent des interfaces de tunnel virtuel statiques régulières sur le concentrateur, seul le concentrateur nécessite un modèle virtuel.

```
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
```

Création d'un groupe de tunnels et annonce des adresses IP d'interface de tunnel via 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
```

Configuration du routage EIGRP sur l'ASA satellite

Créez un système autonome EIGRP et appliquez les réseaux souhaités à annoncer.

```
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
```

Configuration des interfaces sur le routeur satellite

```
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
```

Configurez les paramètres IKEv2 et AAA sur le routeur Spoke

Créez une proposition IKEv2 correspondant aux paramètres de la phase 1 sur l'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 v
                                  and is not a matching parameter with plain AES.)
integrity sha256
group 21
```

Créez une stratégie IKEv2 pour joindre la ou les propositions.

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

Créez une stratégie d'autorisation IKEv2.

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

Activez AAA sur le périphérique.

```
aaa new-model
```

Créez un réseau d'autorisation AAA.

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

Créez un profil IKEv2 contenant un référentiel des paramètres non négociables de l'association de sécurité IKE, tels que les identités locales ou distantes et les méthodes d'authentification.

```
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
```

Créez un jeu de transformation pour définir les paramètres de chiffrement et de hachage utilisés pour protéger le trafic tunnelisé.

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

Créez un profil IPsec de chiffrement pour héberger le transform-set et le profil 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.)
```

Configuration de l'interface de tunnel virtuel statique sur le routeur satellite

Configurez une interface de tunnel virtuel statique pointant vers le concentrateur.

```
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.)
```

Configuration du routage EIGRP sur le routeur satellite

Créez un système autonome EIGRP et appliquez les réseaux souhaités à annoncer.

```
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
```

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Routage ASA :

```
show run router

show eigrp topology

show eigrp neighbors

show route [eigrp]
```

Crypto 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
```

Modèle virtuel ASA et accès virtuels :

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

show interface virtual-access #
```

Routage Cisco IOS :

```
show run | sec eigrp

show ip eigrp topology

show ip eigrp neighbors

show ip route

show ip route eigrp
```

Crypto Cisco IOS :

```
show run | sec cry

show crypto ikev2 sa

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

Interface de tunnel Cisco IOS :

```
show run interface tunnel#
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Débogage de l'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
```

Débogages 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
```

Informations connexes

- Assistance technique et téléchargements Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.