Implementazione di DVTI su Secure Firewall e Cisco IOS

Sommario

Introduzione

Questo documento descrive come implementare una soluzione Hub and Spoke Dynamic Virtual Tunnel Interface con EIGRP su Adaptive Security Appliance.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base delle interfacce tunnel virtuali sull'appliance ASA
- Connettività di base tra Hub/Spoke/ISP
- Conoscenze di base dell'EIGRP

- Adaptive Security Appliance versione 9.19(1) o successiva

Componenti usati

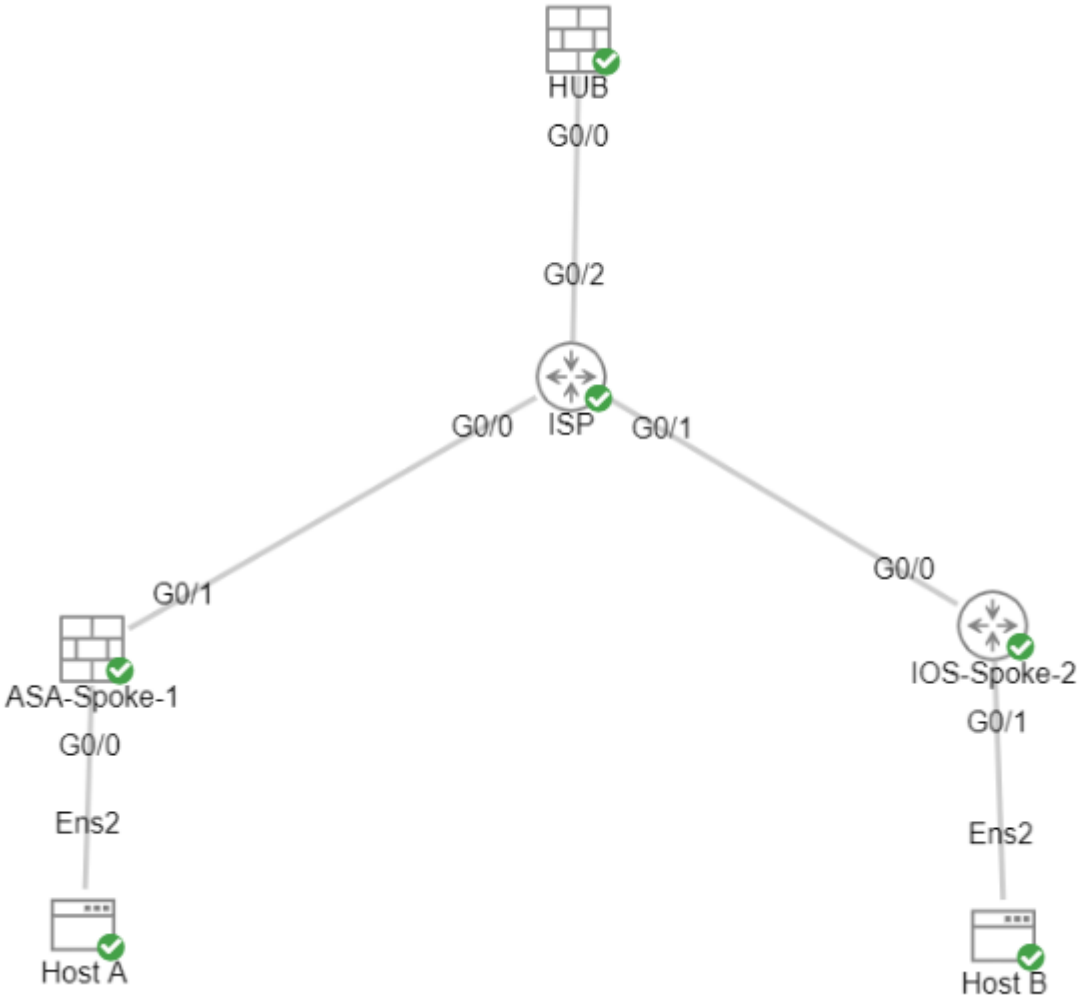
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Due dispositivi ASAv, entrambe le versioni 9.19(1). Utilizzato per il raggio 1 e l'hub
- Due dispositivi Cisco IOS® v versione 15.9(3)M4. Uno per il dispositivo ISP, uno utilizzato per Spoke 2.
- Due host Ubuntu al traffico generico destinato ai tunnel

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazioni

Configurare i parametri dell'interfaccia WAN e della crittografia IKEv2 sull'appliance ASA hub

Accedere alla modalità di configurazione nell'hub.

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

Configurare i parametri IKEv2 sull'appliance ASA hub

Creare un criterio IKEv2 che definisca i parametri della fase 1 della connessione 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
```

Creare una proposta IPSec IKEv2 per definire i parametri della fase 2 utilizzati per proteggere il traffico.

```
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
```

Creare un profilo IPSec contenente la 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
```

Creazione di un'interfaccia di loopback e di modello virtuale

```
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
```

Creazione di un gruppo di tunnel e annuncio degli IP delle interfacce tunnel tramite Exchange IKEv2

Creare un gruppo di tunnel per specificare il tipo di tunnel e il metodo di autenticazione.

```
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
```

Configurazione del routing EIGRP sull'appliance ASA hub

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

Configurazione delle interfacce sull'appliance ASA Spoke

Configurare l'interfaccia WAN.

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

Configurare l'interfaccia LAN.

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

Configurare un'interfaccia di loopback.

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

Configurazione dei parametri di crittografia IKEv2 sull'appliance ASA Spoke

Creare un criterio IKEv2 corrispondente ai parametri dell'hub.

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

Creare una proposta IPSec IKEv2 corrispondente ai parametri dell'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
```

Creare un profilo IPSec contenente la 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
```

Configurazione dell'interfaccia tunnel virtuale statica sull'appliance ASA Spoke

Configurare un'interfaccia tunnel virtuale statica che punti all'hub. I dispositivi spoke configurano interfacce tunnel virtuali statiche regolari per l'hub, solo l'hub richiede un modello virtuale.

```
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
```

Creazione di un gruppo di tunnel e annuncio degli IP delle interfacce tunnel tramite Exchange IKEv2

```
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
```

Configurazione del routing EIGRP sull'appliance ASA Spoke

Creare un sistema autonomo EIGRP e applicare le reti desiderate da pubblicizzare.

```
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
```

Configurazione delle interfacce sul router 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
```

Configurazione dei parametri IKEv2 e AAA sul router spoke

Creare una proposta IKEv2 corrispondente ai parametri della fase 1 sull'appliance 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
```

Creare un criterio IKEv2 per allegare le proposte.

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

Creare un criterio di autorizzazione IKEv2.

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

```
route set Interface
```

Abilitare il server AAA sul dispositivo.

```
aaa new-model
```

Creare una rete di autorizzazioni AAA.

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

Creare un profilo IKEv2 contenente un repository dei parametri non negoziabili dell'associazione di protezione IKE, ad esempio le identità locali o remote e i metodi di autenticazione.

```
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
```

Creare un set di trasformazioni per definire i parametri di crittografia e hashing utilizzati per proteggere il traffico del tunneling.

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

Creare un profilo IPsec di crittografia per ospitare il set di trasformazioni e il profilo 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.)
```

Configurazione dell'interfaccia del tunnel virtuale statico sul router spoke

Configurare un'interfaccia tunnel virtuale statica che punti all'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.)
```

Configurazione del routing EIGRP sul router Spoke

Creare un sistema autonomo EIGRP e applicare le reti desiderate da pubblicizzare.

```
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
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Routing ASA:

```
show run router

show eigrp topology

show eigrp neighbors

show route [eigrp]
```

Crittografia 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 and Virtual-Access:

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

show interface virtual-access #
```

Routing Cisco IOS:

```
show run | sec eigrp

show ip eigrp topology

show ip eigrp neighbors

show ip route

show ip route eigrp
```

Crittografia Cisco IOS:

```
show run | sec cry

show crypto ikev2 sa

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

Interfaccia tunnel Cisco IOS:

```
show run interface tunnel#
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Debug dell'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
```

Debug 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
```

Informazioni correlate

- Supporto tecnico e download Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).