Implement DVTI on Secure Firewall and Cisco IOS

Contents

Introduction

This document describes how to implement a Dynamic Virtual Tunnel Interface hub and spoke solution with EIGRP on Adaptive Security Appliance.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of Virtual Tunnel Interfaces on ASA
- Basic underlay connectivity between Hub/Spokes/ISP
- Basic understanding of EIGRP

- Adaptive Security Appliance version 9.19(1) or higher

Components Used

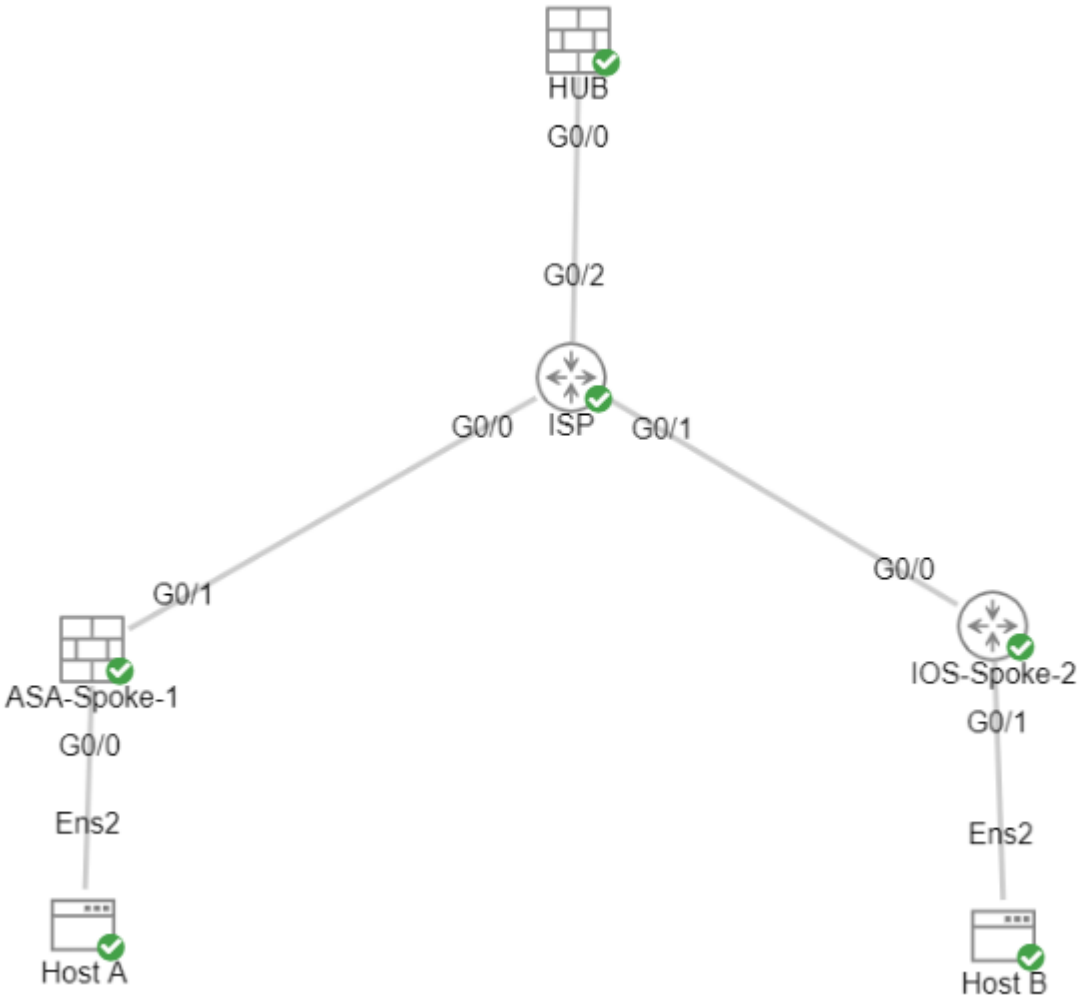
The information in this document is based on these software and hardware versions:

- Two ASAv devices, both version 9.19(1). Utilized for Spoke 1 and the Hub
- Two Cisco IOS® v devices version 15.9(3)M4. One for ISP device, one utilized for Spoke 2.
- Two Ubuntu hosts to generic traffic meant for the 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. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configurations

Configure the WAN Interface and IKEv2 crypto parameters on the Hub ASA

Enter configuration mode on the hub.

```
interface g0/0
```

```
ip address 198.51.100.1 255.255.255.0
nameif OUTSIDE
```

Configure the IKEv2 Parameters on the Hub ASA

Create an IKEv2 policy that defines the Phase 1 parameters of the IKE connection.

```
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
```

Create an IKEv2 IPsec-proposal to define the Phase 2 parameters used to protect the traffic.

```
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
```

Create an IPsec profile that contains the IPsec-proposal.

```
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
```

Create a Loopback and Virtual-Template Interface

```
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 d
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
```

Create a Tunnel-group and Advertise the Tunnel Interface IPs via IKEv2 Exchange

Create a tunnel-group to specify type of tunnel and method of authentication.

```
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
```

Configue EIGRP Routing on the Hub ASA

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

Configure the Interfaces on the Spoke ASA

Configure the WAN Interface.

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

Configure the LAN Interface.

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

Configure a Loopback Interface.

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

Configure the IKEv2 Crypto Parameters on the Spoke ASA

Create an IKEv2 policy that matches the parameters on the hub.

```
crypto ikev2 policy 1
```

```
encryption aes-256
integrity sha256
group 21
prf sha256
lifetime 86400
```

Create an IKEv2 IPsec-proposal that matches the parameters on the 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
```

Create an IPsec profile that contains the IPsec-proposal.

```
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 the Static Virtual Tunnel Interface on the Spoke ASA

Configure a static Virtual Tunnel Interface pointing to the hub. The spoke devices configure regular static Virtual Tunnel Interfaces to the hub, only the hub requires a Virtual-Template.

```
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
```

Create a Tunnel-Group and Advertise the Tunnel Interface IPs 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
```

Configure EIGRP Routing on the Spoke ASA

Create an EIGRP autonomous system and apply the desired networks to be advertised.

```
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 the Interfaces on the Spoke Router

```
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 the IKEv2 Parameters and AAA on the Spoke Router

Create an IKEv2 proposal to match the Phase 1 parameters on the 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
```

Create an IKEv2 policy to attach the proposal(s).

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

Create an IKEv2 authorization policy.

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

Enable AAA on the device.

```
aaa new-model
```

Create an AAA authorization network.

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

Create an IKEv2 Profile that contains a repository of the nonnegotiable parameters of the IKE SA, such as local or remote identities and authentication methods.

```
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
```

Create a transform set to define the encryption and hashing parameters used to protect the tunneled traffic.

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

Create a crypto IPsec profile to house the transform-set and IKEv2 profile.

```
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 the Static Virtual Tunnel Interface on the Spoke Router

Configure a static Virtual Tunnel Interface pointing to the 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.)
```

Configue EIGRP Routing on the Spoke Router

Create an EIGRP autonomous system and apply the desired networks to be advertised.

```
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
```

Verify

Use this section in order to confirm that your configuration works properly.

ASA Routing:

```
show run router

show eigrp topology

show eigrp neighbors

show route [eigrp]
```

ASA Crypto:

```
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-Accesses:

```
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 Tunnel Interface:

```
show run interface tunnel#
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

ASA Debugs:

```
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 Debugs:

```
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
```

Related Information

- Cisco Technical Support & Downloads