Laboratory_22: Configuring site-to-site IPSEC VPN on ASA using IKEv2.

Objectives

- Configure a site-to-site VPN using IKEv2.

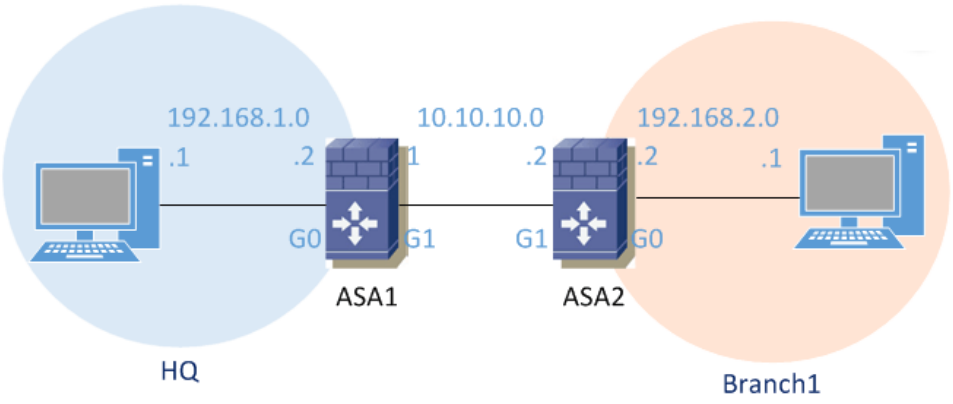
Background / Scenario

The scenario of configuring site-to-site VPN between two Cisco Adaptive Security Appliances is often used by companies that have more than one geographical location sharing the same resources, documents, servers, etc. The Cisco ASA is often used as VPN terminator, supporting a variety of VPN types and protocols.

IKEv2 is the new standard for configuring IPSEC VPNs. Although the legacy IKEv1 is widely used in real world networks, it's good to know how to configure IKEv2 as well since this is usually required in high-security VPN networks (for compliance purposes).

Behind each security appliance there is a private LAN network. After configuring the VPN tunnel, the private LAN networks in HQ and Branch1 (two geographically dispersed locations) will be able to communicate over the internet and share resources.

Topology



Part 1: Basic firewall configuration

Step 1: Configuring IP addressing on ASA1 and ASA2.

ASA1:

```
ASA1(config)# interface GigabitEthernet0
ASA1(config-if)# nameif inside
INFO: Security level for “inside” set to 100 by default.
ASA1(config-if)# ip address 192.168.1.2 255.255.255.0
ASA1(config-if)# no shutdown
ASA1(config-if)# interface GigabitEthernet1
ASA1(config-if)# nameif outside
INFO: Security level for “outside” set to 0 by default.
ASA1(config-if)# ip address 10.10.10.1 255.255.255.0
ASA1(config-if)# no shutdown
```

```
ASA1# show interfaces ip brief
```

Interface	IP-Address	OK? Method Status	Protocol
GigabitEthernet0	192.168.1.2	YES manual up	up
GigabitEthernet1	10.10.10.1	YES manual up	up

ASA2:

```
ASA2(config)# interface GigabitEthernet0
ASA2(config-if)# nameif inside
INFO: Security level for “inside” set to 100 by default.
ASA2(config-if)# ip address 192.168.2.2 255.255.255.0
ASA2(config-if)# no shutdown
```

```
ASA2(config-if)# interface GigabitEthernet1
ASA2(config-if)# nameif outside
INFO: Security level for “outside” set to 0 by default.
ASA2(config-if)# ip address 10.10.10.2 255.255.255.0
ASA2(config-if)# no shutdown
```

```
ASA2# show interfaces ip brief
```

Interface	IP-Address	OK? Method Status	Protocol
GigabitEthernet0	192.168.2.2	YES manual up	up
GigabitEthernet1	10.10.10.2	YES manual up	up

Part 2: Configure the ISAKMP policies with IKEv2

Step 1: In this scenario, we used 3DES encryption with Diffie-Hellman group 2, hash function SHA-1 and an encryption key lifetime of 43200 seconds (12 hours).

ASA1:

```
ASA1(config)# crypto ikev2 policy 1
ASA1(config-ikev2-policy)# group 2
ASA1(config-ikev2-policy)# encryption 3des
ASA1(config-ikev2-policy)# prf sha
ASA1(config-ikev2-policy)# lifetime seconds 43200
```

Finally, after the parameters have been set, we will enable IKEv2 on the outside interface

```
ASA1(config-ikev2-policy)# crypto ikev2 enable outside
```

ASA2:

```
ASA2(config)# crypto ikev2 policy 1
ASA2(config-ikev2-policy)# group 2
ASA2(config-ikev2-policy)# encryption 3des
ASA2(config-ikev2-policy)# prf sha
ASA2(config-ikev2-policy)# lifetime seconds 43200
ASA2(config-ikev2-policy)# crypto ikev2 enable outside
```

Step 2: configure IKEv2 proposal.

As opposed to IKEv1, where we configured a transform set that combines the encryption and authentication method, with IKEv2 we can configure multiple encryption and authentication types, and multiple integrity algorithms for a single policy.

ASA1:

```
ASA1(config)#crypto ipsec ikev2 ipsec-proposal P1
ASA1(config-ipsec-proposal)#protocol esp encryption 3des aes des
ASA1(config-ipsec-proposal)#protocol esp integrity sha-1
```

ASA2:

```
ASA2(config)# crypto ipsec ikev2 ipsec-proposal P1
ASA2(config-ipsec-proposal)# protocol esp encryption 3des aes des
ASA2(config-ipsec-proposal)# protocol esp integrity sha-1
```

Step 3: Identify the VPN interesting traffic with an access list.

ASA1:

```
ASA1(config)# access-list ACL1 extended permit ip 192.168.1.0
255.255.255.0 192.168.2.0 255.255.255.0
```

ASA2:

```
ASA2(config)# access-list ACL2 extended permit ip 192.168.2.0
255.255.255.0 192.168.1.0 255.255.255.0
```

Step 4: Define a tunnel group.

There are two default tunnel groups in the ASA: DefaultRAGroup is the default IPsec remote-access tunnel group and DefaultL2Lgroup is the default IPsec LAN-to-LAN tunnel group.

To establish a LAN-to-LAN connection, two attributes must be set:

- Connection type – IPsec LAN-to-LAN.
- Authentication method for the IP – in this scenario we will use preshared key for IKEv2.
- The name of the tunnel is the IP address of the peer. IKEv2 preshared key is configured as 32fjsk0392fg.

ASA1:

```
ASA1(config)# tunnel-group 10.10.10.2 type ipsec-l2l
ASA1(config)# tunnel-group 10.10.10.2 ipsec-attributes
ASA1(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key
32fjsk0392fg
ASA1(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key
32fjsk0392fg
```

ASA2:

```
ASA2(config)# tunnel-group 10.10.10.1 type ipsec-l2l
ASA2(config)# tunnel-group 10.10.10.1 ipsec-attributes
ASA2(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key
32fjsk0392fg
ASA2(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key
32fjsk0392fg
```

Step 5: Create a crypto map linking the access list

ASA1

```
ASA1(config)# crypto map cmap 1 match address ACL1
ASA1(config)# crypto map cmap 1 set peer 10.10.10.2
```

```
ASA1(config)# crypto map cmap 1 set ikev2 ipsec-proposal P1
ASA1(config)# crypto map cmap interface outside
```

ASA2

```
ASA2(config)# crypto map cmap 1 match address ACL2
ASA2(config)# crypto map cmap 1 set peer 10.10.10.1
ASA2(config)# crypto map cmap 1 set ikev2 ipsec-proposal P1
ASA2(config)# crypto map cmap interface outside
```

Part 3: Configure the ISAKMP policies with IKEv2

IPSEC VPN traffic does not work with NAT. You must not perform NAT on VPN packets. Therefore, in addition to configuring Internet access, we must also configure NAT exclusion for VPN traffic:

Step 1: Configure NAT Overload (PAT) for Internet Access

ASA1

```
object network HQ
subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic interface
object network Branch1
subnet 192.168.2.0 255.255.255.0
```

ASA2

```
object network Branch1
subnet 192.168.2.0 255.255.255.0
nat (inside,outside) dynamic interface
object network HQ
subnet 192.168.1.0 255.255.255.0
```

Step 2: Configure NAT Exclusion for VPN Traffic

ASA1

nat (inside,outside) source static HQ HQ destination static Branch1 Branch1 no-proxy-arp route-lookup

ASA2

nat (inside,outside) source static Branch1 Branch1 destination static HQ HQ no-proxy-arp route-looku