Cisco IPSEC

IKEv2 VTI Site to Site VPN lab

Contents

I. Lab nodes 3

II. Lab objective 3

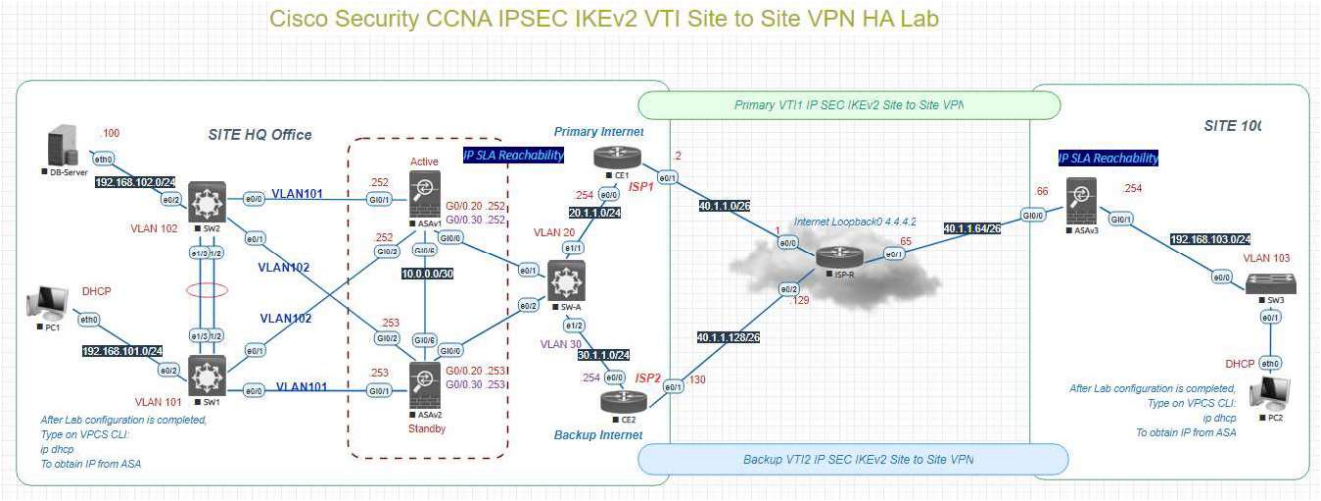
III. Solution 3

1. Configure ASAv1 and ASAv3 Interfaces and default route 3
2. Creating ASAv objects 5
3. Configure DHCP Pools for inside network 5
5. Permit intra and inter security traffic 6
6. Configure NAT Exemption and NAT 6
7. Configure IPSEC IKEv2 6
8. Configure IPSEC VTI Interfaces 8
9. Configure IP SLA monitoring for default and VTI routes 9
10. Configure Active-Standby ASAv1 and ASAv2 9

IV. Verification 10

1. Ping from Host-PC1 to Host-PC2 10
2. Verify traffic encryption 10
3. Verify Traffic switch over to the VTI2 IPSEC tunnel 13
4. Verify DMZ database server reachability 14

Preface: Site-to-Site IPSec IKEv2 VTI VPN Tunnel is used to allow the secure transmission of data, voice and video between two sites (e.g offices or branches). The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.



I. L Lab nodes

1. Image versions used in lab.

- ASAv 9.17
- Router: i86bi_LinuxL3-AdvEnterpriseK9-M2_157_3_May_2018
- Switches: i86bi_linux_l2-adventerprisek9-ms.SSA.high_iron_20190423.bin
- VPCS Node as host

2. Initial configurations

Router, switches and hosts configurations are preloaded in the lab. (Startup configuration).

NOTE: before start the lab, make sure your all nodes has set proper IOL image. Use side bar More Options/Wipe all nodes.

II. L Lab objective

Configure IP SEC IKEv2 VTI redundancy tunnels from Site HQ to Site 100. Host-PC1 must able to ping Host-PC2 and vice versa. If Primary Internet fails traffic must automatically switch to Backup internet and use VTI2 IPSEC tunnel.

III. S Solution

1. Configure ASAv1 and ASAv3 Interfaces and default route

ASAv1

The HQ office has two internet connection, primary via VLAN20 20.1.1.0/24 and Backup internet via VLAN30 30.1.1.0/24 network.

```
hostname ASAv1
enable password cisco

interface GigabitEthernet0/0
 no shut
 description Internet
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/0.20
 description isp1
 vlan 20
 nameif outside1
 security-level 0
 ip address 20.1.1.252 255.255.255.0 standby 20.1.1.253
!
interface GigabitEthernet0/0.30
 description isp2
 vlan 30
 nameif outside2
 security-level 0
 ip address 30.1.1.252 255.255.255.0 standby 30.1.1.253
!
interface GigabitEthernet0/1
 no shut
 nameif inside
 security-level 100
 ip address 192.168.101.252 255.255.255.0 standby 192.168.101.253
!
interface GigabitEthernet0/2
 no shut
 nameif dmz
 security-level 80
 ip address 192.168.102.252 255.255.255.0 standby 192.168.102.253

route outside1 0.0.0.0 0.0.0.0 20.1.1.254 1
route outside2 0.0.0.0 0.0.0.0 30.1.1.254 10
```

ASAv3

```
hostname ASAv3
enable password cisco

interface GigabitEthernet0/0
 no shut
 description internet
 nameif outside
 security-level 0
 ip address 40.1.1.66 255.255.255.192
!
interface GigabitEthernet0/1
 no shut
 nameif inside
```

```
 security-level 100
 ip address 192.168.103.254 255.255.255.0

route outside 0.0.0.0 0.0.0.0 40.1.1.65 1
```

2. Creating ASAv objects

Create extended ASAv objects

ASAv1

```
object network default-gw1
 host 20.1.1.254
object network default-gw2
 host 30.1.1.254
object network  inside-lan-hq
 subnet 192.168.101.0 255.255.255.0
object network dmz-lan-hq
 subnet 192.168.102.0 255.255.255.0
object network  inside-lan-rm
 subnet 192.168.103.0 255.255.255.0

object-group network DMZ-ACCESS
 network-object object inside-lan-hq
 network-object object inside-lan-rm
```

ASAv3

```
object network default-gw
 host 40.1.1.65
object network  inside-lan-rm
 subnet 192.168.103.0 255.255.255.0
object network  inside-lan-hq
 subnet 192.168.101.0 255.255.255.0
object network dmz-lan-hq
 subnet 192.168.102.0 255.255.255.0

access-group outside_access_in in interface outside
```

3. Configure DHCP Pools for inside network

ASAv1

```
dhcpd address 192.168.101.10-192.168.101.20 inside
dhcpd dns 8.8.8.8 interface inside
dhcpd domain eve.lab interface inside
dhcpd enable inside
```

ASAv3

```
dhcpd address 192.168.103.10-192.168.103.20 inside
dhcpd dns 8.8.8.8 interface inside
dhcpd domain eve.lab interface inside
```