Practical 9

Aim :- Layer 2 VLAN Security

a) Connect a new redundant link between SW-1 and SW-2

Step 1 : Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10)

Step 2 : Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5)

Note : If using the simple PDU GUI packet, be sure to ping twice to allow for ARP

b) Create a Redundant Link Between SW-1 and SW-2

Step 1 :- Connect SW-1 and SW-2

Using a crossover cable, connect port F0/23 on SW-1 to port F0/23 on SW-2

Step 2 :- Enable trunking, including all trunk security mechanisms on the line between SW-1 and SW-2

```
SW-1(config)# interface f0/23
SW-1(config-if)# switchport mode trunk
SW-1(config-if)# switchport trunk native vlan 15
SW-1(config-if)# switchport nonegotiate
SW-1(config-if)# no shutdown
```

SW-2 (config)# interface f0/23
SW-2 (config-if)# switchport mode trunk
SW-2 (config-if)# switchport trunk native vlan 15
SW-2 (config-if)# switchport nonegotiate
SW-2 (config-if)# no shutdown.

c) Enable VLAN 20 as a Management VLAN

Step 1:- Enable a management VLAN (VLAN 20) on SW-A

a) Enable VLAN 20 on SW-A

SW-A (config)# vlan 20
SW-A (config-vlan)# exit

b) Create an interface VLAN 20 and assign an IP address within the 192.168.20.0/24 network.

SW-A (config)# interface vlan 20
SW-A (config-if)# ip address 192.168.20.1 255.255.255.0

Step 2 :- Enable the same management VLAN on all other switches

a) Create the management VLAN on all switches: SW-B, SW-1, SW-2 and central

SW-B (config)# vlan 20
SW-B (config)# exit

SW-1(config)# vlan 20
SW-1(config-vlan)# exit

SW-2(config)# vlan 20
SW-2(config-vlan)# exit

Central(config)# vlan 20
Central(config-vlan)# exit

b) Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24 network.

SW-B(config)# interface vlan 20
~~SW-B(config)#~~ SW-B(config-if)# ip address 192.168.20.2 255.255.255.0

SW-1(config)# interface vlan 20
SW-1(config-if)# ip address 192.168.20.3 255.255.255.0

SW-2(config)# interface vlan 20
SW-2(config-if)# ip address 192.168.20.4 255.255.255.0

Central(config)# interface vlan 20
Central(config-if)# ip address 192.168.20.5 255.255.255.0

Step 3: Connect and configure the management PC

Connect the management PC to SW-A port F0/1 and ensure that it is assigned an available IP address within the 192.168.20.0/24 network.

Step 4: On SW-A, ensure the management PC is part of VLAN 20

```
SW-A(config)# interface f0/1
SW-A(config-if)# switchport access vlan 20
SW-A(config-if)# no shutdown
```

Step 5: Verify connectivity of the management PC to all switches

The management PC should be able to ping SW-A, SW-B, SW-1, SW-2, and central.

d) Enable the Management PC to Access Router R1

Step 1: Enable a new subinterface on router R1

a) Create subinterface g0/0.3 and set encapsulation to dot1q 20 to account for VLAN 20

```
R1(config)# interface g0/0.3
R1(config-subif)# encapsulation dot1q 20
```

b) Assign an IP address within the 192.168.20.0/24 network

R1(config)# interface g0/0.3
R1(config-subif)# ip address 192.168.20.100 255.255.255.0

Step 2: Verify connectivity between the management PC and R1

Be sure to configure the default gateway on the management PC to allow for connectivity.

Step 3:- Enable Security

a) Create an ACL that allows only the Management PC to access the router.

R1(config)# access-list 101 deny ip any 192.168.20.0 0.0.0.255
R1(config)# access-list 101 permit ip any any
R1(config)# access-list 102 permit ip host 192.168.20.50 any

b) Apply the ACL to the proper interface.

R1(config)# interface g0/0.1
R1(config-subif)# ip access-group 101 in
R1(config-subif)# interface g0/0.2
R1(config-subif)# ip access-group 101 in
R1(config-subif)# line vty 0 4
R1(config-subif)# access-class 102 in

48

Step 4 : Verify Security

a) Verify only the Management PC can access the router

PC > ssh -l SSHadmin 192.168.20.100

b) From the management PC, ping SW-A, SWB, and R1

c) From D1, ping the management PC

Practical 10

Aim :- Configure and Verify a Site-to-Site IPsec VPN using CLI

Part 1 : Configure IPsec Parameters on R1

Step 1 :- Test Connectivity

Ping from PC-A to PC-C

Step 2 :- Enable the Security Technology package

a) On R1, issue the show version command to view the Security Technology package license information.
b) If the Security Technology package has not been enabled, use the following command to enable the package.

```
R1(config)# license boot module c1900 technology-package
                securityK9
```

c) Accept the end-user license agreement
d) Save the running-config and reload the router to enable the security license
e) Verify that the Security Technology package has been enabled by using the show version command.

Step 3 :- Identify interesting traffic on R1

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255
                192.168.3.0 0.0.0.255
```

Step 4: Configure the IKE Phase1 ISAKMP ~~plo~~ policy on R1

```
R1 (config)# crypto isakmp policy 10
R1 (config-isakmp)# encryption aes 256
R1 (config-isakmp)# authentication pre-share
R1 (config-isakmp)# group 5
R1 (config-isakmp)# exit
R1 (config)# crypto isakmp key vpnpa55 address 10.2.2.2
```

Step 5: Configure the IKE Phase 2 IPsec policy on R1

a) Create the transform-set VPN-SET to use esp-aes and ~~esp-aes~~ esp-sha-hmac

```
R1 (config)# crypto ipsec transform-set VPN-SET esp-aes
              esp-sha-hmac.
```

b) Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together.

```
R1 (config)# crypto map VPN-MAP 10 ipsec-isakmp
R1 (config-crypto-map)# description VPN connection to R3
R1 (config-crypto-map)# set peer 10.2.2.2
R1 (config-crypto-map)# set transform-set VPN-SET
R1 (config-crypto-map)# match address 110
R1 (config-crypto-map)# exit
```

Step 6: Configure the crypto map on the outgoing interface

```
R1(config)# interface s0/1/0
R1(config-if)# crypto map VPN-MAP
```

Part 2: Configure IPsec Parameteters on R3

Step 1: Enable the Security Technology package

a) On R3, issue the show version command to verify that the Security Technology package license information has been enabled.

b) If the Security Technology package has not been enabled, enable the package and reload R3.

Step 2: Configure router R3 to support a site-to-site VPN with R1.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255
                192.168.1.0 0.0.0.255
```

Step 3: Configure the IKE Phase 1 ISAKMP properties on R3

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2
```

Step4 : Configure the IKE Phase 2 IPsec policy on R3

a) Create the transform-set VPN-SET to use esp-aes and esp-sha-hmac

```
R3 (config) # crypto ipsec transform-set VPN-SET esp-aes
              esp-sha-hmac
```

b) Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together.

```
R3 (config) # crypto map VPN-MAP 10 ipsec-isakmp
R3 (config-crypto-map) # description VPN connection to R1
R3 (config-crypto-map) # set peer 10.1.1.2
R3 (config-crypto-map) # set transform-set VPN-SET
R3 (config-crypto-map) # match address 110
R3 (config-crypto-map) # exit
```

Step5 : Configure the crypto map on the outgoing interface.

```
R3 (config) # interface S0/0/1
R3 (config-if) # crypto map VPN-MAP
```

54

53

Part 3 : Verify the IPsec VPN

Step 1 :- Verify the tunnel prior to interesting traffic

Issue the show crypto ipsec sa

Step 2 :- Create interesting traffic

Ping PC-C from PC-A

Step 3 :- Verify the tunnel after interesting traffic

On R1, re-issue the show crypto ipsec sa command.

Step 4 : Create uninteresting traffic

Ping PC-B from PC-A

Step 5 : Verify the tunnel

On R1, re-issue the show crypto ipsec sa command.

Practical 11

Aim :- Configuring ASA Basic Settings and Firewall Using CLI

Part 1 : Verify Connectivity and Explore the ASA

Step 1 : Verify connectivity

The ASA is not currently configured. However, all routers, PCs, and the DMZ server are configured. Verify that PC-C can ping any router interface. PC-C is unable to ping the ASA, PC-B, or the DMZ server.

Step 2 : Determine the ASA version, interfaces and license

Use the show version command to determine various aspects of this ASA device.

Step 3 : Determine the file system and contents of flash memory

a) Enter privileged EXEC mode. A password has not been set. Press Enter when prompted for a password.
b) Use the show file system command to display the ASA file system and determine which prefixes are supported.
c) Use the show flash : or show disk0 : command to display the contents of flash memory.

Part 2: Configure ASA Settings and Interface Security Using the CLI

Step 1: Configure the hostname and domain name

a) Configure the ASA hostname as CCNAS-ASA
b) Configure the domain name as ccnasecurity.com

Step 2: Configure the enable mode password

Use the enable password command to change the privileged EXEC mode password to ciscoenpa55.

Step 3: Set the date and time.

Use the clock set command to manually set the date and time.

Step 4: Configure the inside and outside interfaces.

a) Configure a logical VLAN 1 interface for the inside network (192.168.1.0/24) and set the security level to the highest setting of 100

```
CCNAS-ASA(config)# interface vlan1
CCNAS-ASA(config-if)# nameif inside.
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# security-level 100
```

b) Create a logical VLAN 2 interface for the outside network (209.165.200.224/29)

```
CCNAS-ASA(config-if)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
CCNAS-ASA(config-if)# ip address 209.165.200.226 225.225.225.248
CCNAS-ASA(config-if)# security-level 100
```

c) Use the following verification commands to check your configurations.

1) Use the show interface ip brief command to display the status for all ASA interfaces.
2) Use the show ip address command to display the information for the Layer 3 VLAN interfaces.
3) Use the show switch vlan command to display the inside and outside VLANs configured on the ASA and to display the assigned ports.

Step 5: Test connectivity to the ASA

a) You should be able to ping from PC-B to the ASA inside interface address (192.168.1.1). If the pings fails, troubleshoot the configuration as necessary.
b) From PC-B, ping the VLAN 2 (outside) interface at IP address 209.165.200.226. You should not be able to ping this address.

... the object portion that

Part 3 - Configuring Routing, Address Translation and Inspection Policy Using the CLI

Step 1 : Configure a static default route for the ASA

a) Create a "quad zero" default route using the route command, associate it with the ASA outside interface, and point to the R1 G0/0 IP address (209.165.200.225) as the gateway of last resort

```
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0
                    209.165.200.225
```

b) Issue the show route command to verify the static default route is in the ASA routing table.

c) Verify that the ASA can ping the R1 S0/0/0 IP address 10.1.1.1. If the ping is unsuccessful, troubleshoot as necessary

Step 2 : Configure address translation using PAT and network objects.

a) Create network object inside-net and assign attributes to it using the subnet and nat commands.

```
CCNAS-ASA(config)# object network inside-net
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
```

b) The ASA splits the configuration into the object portion that defines the network to be translated and the actual ~~not~~ nat command parameters

c) From PC-B attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should fail.

d) Issue the show nat command on the ASA to see the translated and untranslated hits.

Step 3 : Modify the default MPF application inspection global service policy.

a) Create the class-map, policy-map and service-policy. Add the inspection of ICMP traffic to the policy map list using the following commands.

```
CCNAS=ASA(config)# class-map inspection_default
CCNAS=ASA(config-cmap)# match default-inspection-traffic
CCNAS=ASA(config-cmap)# exit
CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-pmap-c)# inspect icmp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config-)# service-policy global_policy global
```

b From PC-B, attempt to ping the R1 G0/0 interface at IP address 209.165.200.225.

Part 4 : Configure DHCP, AAA, and SSH

Step 1 : Configure the ASA as a DHCP server

a) Configure a DHCP address pool and enable it on the ASA inside interface.

CCNAS-ASA (config) # dhcpd address 192.168.1.5-192.168.1.36 inside

b) Specify the IP address of the DNS server to be given to clients (optional)

CCNAS-ASA(config)# dhcpd dns 209.165.201.2 interface inside

c) Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (inside)

CCNAS-ASA (config) # dhcpd enable inside

d) Change PC-B from a static IP address to a DHCP client, and verify that it receives IP addressing information.

Step 2 : Configure AAA to use the local database for authentication.

a) Define a local user named admin by entering the username command. Specify a password of adminpa55

CCNAS-ASA (config) # username admin password adminpa55

b) Configure AAA to use the local ASA database for SSH user authentication.

```
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
```

Step 3: Configure remote access to the ASA

a) Generate an RSA key pair, which is required to support SSH connections. Because the ASA device has RSA keys already in place, enter no when prompted to replace them

```
CCNAS-ASA(config)# crypto key generate rsa modulus 1024
Do you really want to replace them? [yes/no]: no
ERROR: Failed to create new RSA keys named <Default-RSA-Key>
```

b) Configure the ASA to allow SSH connections from any host on the inside network (192.168.1.0/24) and from the remote management host at the branch office 172.16.3.3 on the outside network.

```
CCNAS-ASA(config)# ssh 192.168.1.0 255.255.255.0 inside
CCNAS-ASA(config)# ssh 172.16.3.3 255.255.255.255 outside
CCNAS-ASA(config)# ssh timeout 10
```

c) Establish an SSH session from PC-C to the ASA (209.165.200.226)

```
PC> ssh -l admin 209.165.200.226
```

d) Establish an SSH session from PC-B to the ASA (192.168.1.1)

PC> ssh -l admin 192.168.1.1

Part 5: Configure a DMZ, Static NAT, and ACLs

Step 1: Configure the DMZ interface VLAN 3 on the ASA

a) Configure DMZ VLAN 3, which is where the public access web server will reside.

```
CCNAS-ASA(config)# interface vlan 3
CCNAS-ASA(config-if)# ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)# no forward interface vlan 1
CCNAS-ASA(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default
CCNAS-ASA(config-if)# security-level 70
```

b) Assign ASA physical interface E 0/2 to DMZ VLAN 3 and enable the interface

```
CCNAS-ASA(config-if)# interface Ethernet 0/2
CCNAS-ASA(config-if)# switchport access vlan 3
```

c Use the following verification commands to check your configurations:

1] Use the show interface ip brief command to display the status for all ASA interfaces.
2] Use the show ip address command to display the information for the Layer 3 VLAN interfaces
3] Use the show switch vlan command to display the inside and outside VLANs configured on the ASA and to display the assigned ports.

Step 2: Configure static NAT to the DMZ server using a network object.

```
CCNAS-ASA(config)# object network dmz-server
CCNAS-ASA(config-network-object)# host 192.168.2.3
CCNAS-ASA(config-network-object)# nat (dmz,outside)
                                  static 209.165.200.227
CCNAS-ASA(config-network-object)# exit
```

Step 3: Configure an ACL to allow access to the DMZ server from the Internet

```
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit icmp
                    any host 192.168.2.3
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit tcp any
                    host 192.168.2.3 eq 80
CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface
                    outside
```

Step 4: Test access to the DMZ server

At the time this Packet Tracer activity was created, the ability to successfully test outside access to the DMZ web server was not in place; therefore, successful testing is not required.