CONTENT

1. Overview

In this project we have designed and implemented a network for company A using ASA 5520 firewall and Edge router. Firewall has 4 named networks with defined security levels connected to it. The management network is implemented through which we can manage edge router, ASA firewall, INSIDE, DMZ and OUTSIDE switch. The inside network can access the OUTSIDE and DMZ network, from OUTSIDE network the PC with AnyConnect VPN can securely access the INSIDE network using VPN-Tunnel and from OUTSIDE network the DMZ is accessible.

2. Policy Requirements

The following is a short list of policies that would be typical of security policy. The design and implementation must incorporate these policies.

- In our topology we have company A which has ASA 5520 firewall and an edge router to protect the company network from public.
- The company network should be named and assigned a specific security level.
- The server in the DMZ zone should be accessible from public and INSIDE network.
- Company INSIDE network should be accessible from OUTSIDE network only by establishing connection from AnyConnect-VPN client with ASA firewall.
- All the network devices should be accessible from management network.
- All switches should be enabled with port-security.
- All access to and from the Internet must connect via NAT.

3. Topology

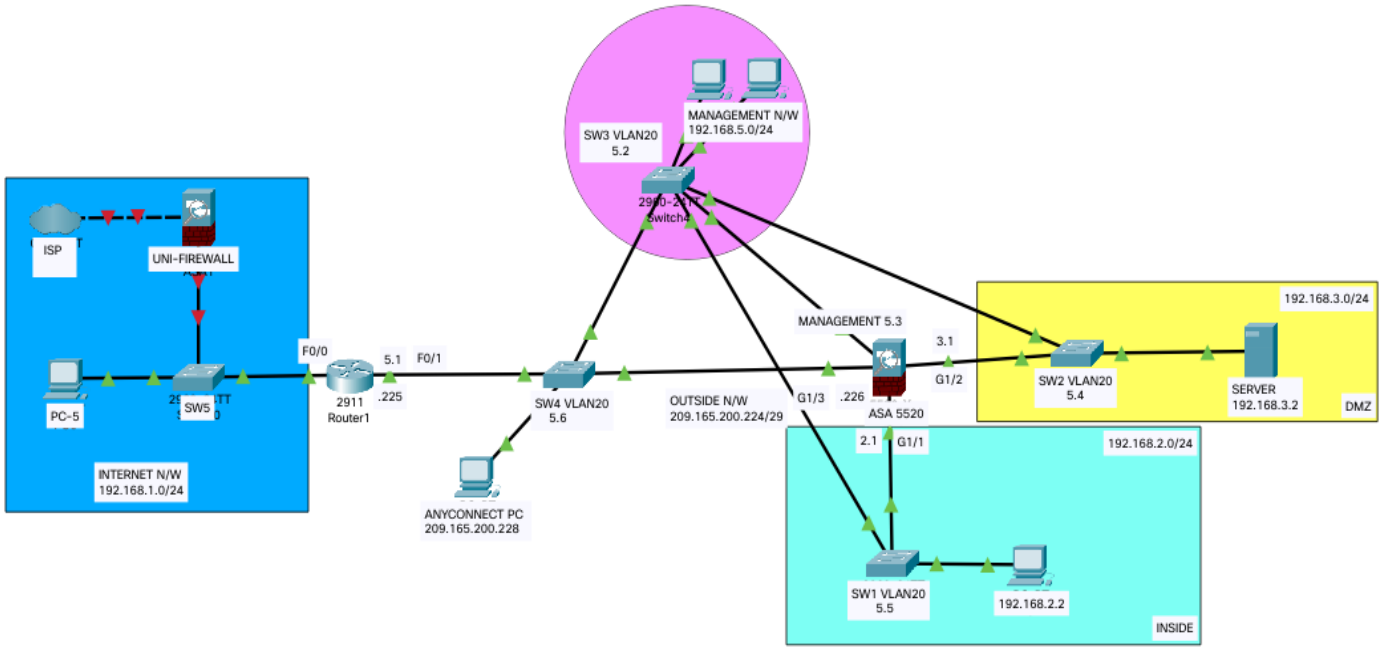

Figure 1 Network Topology

The above topology is an illustration of actual topology implemented in lab. The hardware devices used to build the network in lab are as follows:

- 1 cisco 2800 series router
- 5 cisco catalyst 2960 switch
- ASA 5520 firewall

- 6 PC

4. ASA

- In the above topology ASA 5520 has been used. The interfaces are configured with the security level being minimum 0 to maximum 100. The basic rule in ASA is that, traffic can flow from higher security level to lower security level but cannot travel from lower to higher security level.

- The configuration of interfaces with security level is done as follows:
    a) Asa(config)#interface G1/1
       Asa(config-if)#nameif INSIDE
       Asa(config-if)#security-level 100
       Asa(config-if)#ip address 192.168.2.1 255.255.255.0
       Asa(config-if)#no shutdown

    b) Asa(config)#interface G1/3
       Asa(config-if)#nameif OUTSIDE
       Asa(config-if)#security-level 0
       Asa(config-if)#ip address 209.165.200.226 255.255.255.248
       Asa(config-if)#no shutdown

    c) Asa(config)#interface G1/2
       Asa(config-if)#nameif DMZ
       Asa(config-if)#security-level 50
       Asa(config-if)#ip address 192.168.3.1 255.255.255.0
       Asa(config-if)#no shutdown

    d) Asa(config)#interface M0/0
       Asa(config-if)#nameif management
       Asa(config-if)#security-level 50
       Asa(config-if)#ip address 192.168.5.3 255.255.255.0
       Asa(config-if)#no shutdown

- Now the route to travel outside is given as the gateway of edge router.
       Asa(config)#route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225

- With the default configurations ASA will allow a host to ping the interface which is connected to. However, ping from an internal host to the internet would normally fail.
- ASA doesn't track ICMP sessions/connections, making it stateless. Because ICMP packets do not themselves contain any connection information. Being stateless, ASA will let the ICMP echo request from Inside to Outside, but it will not allow the ICMP echo reply from Outside to Inside.
- Below you will find the ICMP inspection configuration:
    a) Asa(config)#class-map inspection_default
       Asa(config-cmap)#match default-inspection-traffic

    b) Asa(config)#policy-map global_policy
       Asa(config-pmap)# class inspection_default
       Asa(config-pmap-c)# inspect icmp

Asa(config-pmap-c)# inspect http

c) Asa(config)#service-policy global_policy global

- Once the above commands are implemented, we can successfully access http and icmp from INSIDE to OUTSIDE network
- We will configure NAT on ASA in later steps.

5. Edge router configuration:

- As this is edge router, we have to implement NAT here and this router is accessible from management network, for that we need to configure management network sub-interface Fa0/1.20 on router.
- From outside 192.168.1.0/24 network DMZ should be accessible for that static NAT is also implemented here.

a) R1(config)#interface Fa0/0
R1(config-if)#ip address dhcp
R1(config-if)#ip nat outside
R1(config-if)#no shutdown

b) R1(config)#interface Fa0/1.10
R1(config-if)#encapsulation dot1Q 10
R1(config-if)#ip address 209.165.200.225 255.255.255.248
R1(config-if)#ip nat inside
R1(config-if)#no shutdown

c) R1(config)#ip access-list extended R_NAT
R1(config-ext-nacl)#permit ip any

d) R1(config)#ip nat inside source list R_NAT interface FastEthernet0/0 overload

e) R1(config)#ip nat inside source static tcp 209.165.200.227 80 interface FastEthernet0/0 80

f) R1(config)#ip nat inside source static tcp 209.165.200.227 443 interface FastEthernet0/0 443

g) R1(config)#interface Fa0/1.20
R1(config-if)#encapsulation dot1Q 20
R1(config-if)#ip address 192.168.5.1 255.255.255.0
R1(config-if)#ip nat inside
R1(config-if)#no shutdown

- Now we need to implement NAT on ASA, so that INSIDE network can access the OUTSIDE network and OUTSIDE network can access DMZ network. Here we need one static NAT to map network traffic from an external IP address to an internal IP address for DMZ access. We have to make network objects for interfaces and then implement the NAT.

a) Asa(config)#object network INSIDE-NET
asa (config-network-object)# subnet 192.168.2.0 255.255.255.0
asa (config-network-object)# nat (INSIDE,OUTSIDE) dynamic interface

b) Asa(config)#object network DMZ-SERVER
asa (config-network-object)# subnet 192.168.3.0 255.255.255.0
asa (config-network-object)# nat (DMZ,OUTSIDE) static 209.165.200.227

- For OUTSIDE network to access DMZ we need to implement ACL on OUTSIDE interface.
  a) Asa(config)#access-list OUTSIDE-DMZ extended permit tcp any host 192.168.3.2 eq www
  Asa(config)#access-list OUTSIDE-DMZ extended permit tcp any host 192.168.3.2 eq https
  Asa(config)#access-list OUTSIDE-DMZ extended permit icmp any host 192.168.3.2
  Asa(config)#access-group OUTSIDE-DMZ in interface OUTSIDE

6. Switch configuration:

- SW3 has the management network connected to it, from the management network PCs the ASA firewall, Edge router, SW1, SW2 and SW4 can be managed. For that separate VLANS for Management network are configured and to make the Router accessible from management PCs the interface G0/1 of SW4 is configured as Trunk.

- We have implemented Port-security and port-fast on the switch SW3. Port-security makes it sure not to accept the connection from more than certain number of PC mac-addresses or defined PC mac-addresses. If new PC with mac-address tries to connect the port it results in violation shutdown mode and the port gets shutdown. To enable immediate transition into the forwarding state, we can enable the STP port fast feature.

a) SW4(config)#vlan 10
SW4(config-vlan)#name 209NETWORK
SW4(config)#vlan 20
SW4(config-vlan)#name MGMT_NW
SW4(config)#vlan 99
SW4(config-vlan)#name FOR_TRUNK

b) SW4(config)#interface Fa0/1
SW4(config-if)#switchport access vlan 20
SW4(config-if)# switchport mode access
SW4(config-if)#spanning-tree portfast
SW4(config-if)#switchport port-security
SW4(config-if)#switchport port-security maximum 1
SW4(config-if)#switchport port-security mac-address sticky
SW4(config-if)#switchport port-security violation shutdown

c) SW4(config)#interface range Fa0/22 – 24
SW4(config-if-range)#switchport access vlan 10
SW4(config-if-range)# switchport mode access
SW4(config-if-range)#spanning-tree portfast
SW4(config-if-range)#switchport port-security
SW4(config-if-range)#switchport port-security maximum 2
SW4(config-if-range)#switchport port-security mac-address sticky

SW4(config-if-range)#switchport port-security violation shutdown

d) SW4(config)#interface G0/2
SW4(config-if)#switchport mode trunk
SW4(config-if)#switchport trunk native vlan 99
SW4(config-if)#switchport trunk allowed vlan 10,20

e) SW4(config)#interface vlan 20
SW4(config-if)#ip address 192.168.5.6 255.255.255.0
SW4(config)#ip default-gateway 192.168.5.1

f) SW3(config)#vlan 20
SW3(config-vlan)#name MGMT_NW

g) SW3(config)#interface range Fa0/1 – 6
SW3(config-if-range)#switchport access vlan 20
SW3(config-if-range)# switchport mode access
SW3(config-if-range)#spanning-tree portfast
SW3(config-if-range)#switchport port-security
SW3(config-if-range)#switchport port-security maximum 1
SW3(config-if-range)#switchport port-security mac-address sticky
SW3(config-if-range)#switchport port-security violation shutdown

h) SW3(config)#interface vlan 20
SW3(config-if)#ip address 192.168.5.2 255.255.255.0
SW3(config)#ip default-gateway 192.168.5.1

- To access switches via SSH using local database we need domain name, username and password as follows:

a) SW3(config)#ip domain-name netsec.com
SW3(config)#username admin secret cisco
SW3(config)#crypto key generate rsa general-keys modulus 2048
SW3(config)# line vty 0 6
SW3(config-line)#login local
SW3(config-line)#transport input ssh
SW3(config-line)# login

b) SW4(config)#ip domain-name netsec.com
SW4(config)#username admin secret cisco
SW4(config)#crypto key generate rsa general-keys modulus 2048
SW4(config)# line vty 0 6
SW4(config-line)#login local
SW4(config-line)#transport input ssh
SW4(config-line)# login

- Now in similar manner we have to configure SW1, SW2. SSH will be implemented, VLANs will be configured for management switches.

a) SW2(config)#vlan 20
SW2(config-vlan)#name MGMT_NW
SW2(config)#interface Fa0/10
SW2(config-if)#switchport access vlan 20
SW2(config)#ip default-gateway 192.168.5.1
SW2(config)#interface vlan 20
SW2(config-if)#ip address 192.168.5.4 255.255.255.0
SW2(config)#ip domain-name netsec.com
SW2(config)#username admin secret cisco
SW2(config)#crypto key generate rsa general-keys modulus 2048
SW2(config)# line vty 0 6
SW2(config-line)#login local
SW2(config-line)#transport input ssh
SW2(config-line)# login

b) SW1(config)#vlan 20
SW1(config-vlan)#name MGMT_NW
SW1(config)#interface Fa0/10
SW1(config-if)#switchport access vlan 20
SW1(config)#interface vlan 20
SW1(config-if)#ip address 192.168.5.5 255.255.255.0
SW1(config)#ip default-gateway 192.168.5.1
SW1(config)#ip domain-name netsec.com
SW1(config)#username admin secret cisco
SW1(config)#crypto key generate rsa general-keys modulus 2048
SW1(config)# line vty 0 6
SW1(config-line)#login local
SW1(config-line)#transport input ssh
SW1(config-line)# login

7. AnyConnect VPN:

- In the final part if any PC in OUTSIDE network want an access for INSIDE network it needs to be connected via the AnyConnect VPN client.
- The clientless WebVPN method does not require a VPN client to be installed on the user's computer. You just open your web browser; enter the IP address of the ASA and you will get access through a web portal. There is no full network access when you use clientless WebVPN. We only have limited access to a number of applications, for example:
  - Internal websites (HTTP and HTTPS)
  - Web applications
  - Windows file shares
  - Email servers (POP3, IMAP, SMTP)
  - Microsoft Outlook Web Access

- AnyConnect VPN offers full network access. The remote user will use the AnyConnect client to connect to the ASA and will receive an IP address from a VPN pool, allowing full access to the network.
- We have used clientless WebVPN only for the installation of the AnyConnect VPN client. The remote user will open a web browser, enters the IP address of the ASA and then user needs to download the AnyConnect VPN client to establish the connection.
- First step is to enable clientless WebVPN and then load AnyConnect image from ASA flash as follows:

    a) Asa(config)# webvpn
    Asa(config-webvpn)# anyconnect image flash:*/anyconnect.pkg _file_name*

- This following command enables WebVPN on the outside interface and we also need to enable anyconnect.
    a) Asa(config-webvpn)# enable outside
    Asa(config-webvpn)# anyconnect enable

- All the traffic coming through VPN-tunnel should be permitted INSIDE. The following command bypass the access-list on OUTSIDE interface for VPN-tunnel:
    a) Asa(config)# sysopt connection permit-vpn

- The following configuration steps for asa VPN are:
- Configure a local pool of ip addresses for VPN-connection
- Configure group policy
- Configure the tunnel-group to bind the group policies and VPN pool together
- Make a group name for remote users using the tunnel –group commands
- Configure username, passwords and assign them for remote-access.
- NAT exemption is needed to stop ASA from translating VPN pool addresses

    a) Asa(config)# ip local pool VPN_POOL 192.168.10.1-192.168.10.254 mask 255.255.255.0

    b) Asa(config)# access-list VPN_ACL extended permit ip any
    Asa(config)#group-policy ANYCONNECT_POLICY internal
    Asa(config)# group-policy ANYCONNECT_POLICY attributes
    Asa(config-group-policy)# vpn-tunnel-protocol ssl-client ssl-clientless
    Asa(config-group-policy)#vpn-filter value VPN_ACL
    Asa(config-group-policy)# split-tunnel-policy tunnelall
    Asa(config-group-policy)# dns-server value 8.8.8.8

    c) Asa(config)# tunnel-group MY_TUNNEL type remote-access
    Asa(config)# tunnel-group MY_TUNNEL general-attributes
    Asa(config-tunnel-general)# default-group-policy ANYCONNECT_POLICY
    Asa(config-tunnel-general)# address-pool VPN_POOL

    d) Asa(config)# tunnel-group MY_TUNNEL webvpn-attributes
    Asa(config-tunnel-webvpn)# group-alias SSL_USERS enable

```
Asa(config)# webvpn
Asa(config-webvpn)# tunnel-group-list enable
```

e)
```
Asa(config)# username admin password cisco
Asa(config)# username admin attributes
Asa(config-username)# service-type remote-access
```

f)
```
Asa(config)# access-list NO_NAT extended permit ip 192.168.2.0 255.255.255.0 192.168.10.0 255.255.255.0
Asa(config)#object network VPN_NET
asa (config-network-object)# subnet 192.168.10.0 255.255.255.0
asa (config-network-object)# nat (OUTSIDE,OUTSIDE) dynamic interface
Asa(config)#nat(INSIDE,OUTSIDE) source static INSIDE-NET INSIDE-NET destination static VPN_NET VPN_NET
```

- After all the above implementation if we open web browser in PC (209.165.200.228) and search the ip address 209.165.200.226 it gives a prompt for user-ID and login. Once the details are filled the anyconnect can be downloaded on the PC. After successfully making a connection with 209.165.200.226 via anyconnect the PC can access the INSIDE network and can access the internet at the same time.

8. Future implementation:

- Intrusion prevention system can be implemented in above network to detect the signatures and take an action on incoming packets.
- Intrusion detection system can be implemented to log incoming and outgoing data and send an alert if the signature is detected.
- SPAN protocol can be enabled on switches to log the incoming, outgoing data on interfaces and send a log to a server.