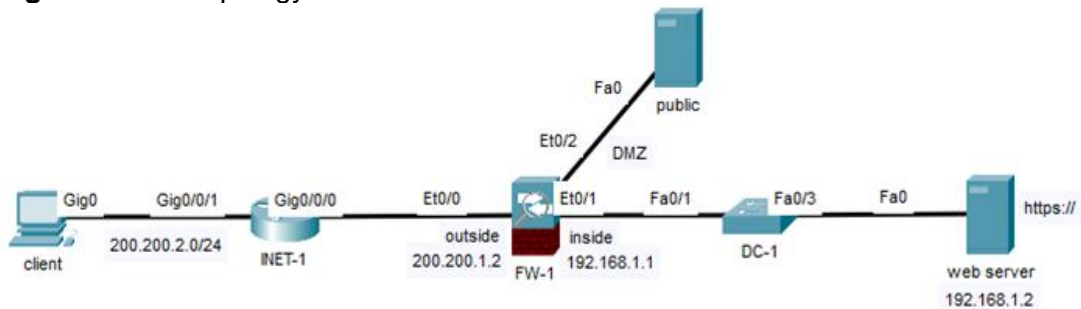


# ASA 5505 Firewall

## Lab Summary

Configure ASA 5505 Firewall with network connectivity from the internet hosts to data center web server.

**Figure 1** Lab Topology



## Lab Configuration

Start Packet Tracer File: **asa firewall.pkt**

Click on *FW-1* icon and select *CLI* folder.

Step 1: Enter global configuration mode

```
ciscoasa> enable
Password: hit <enter>
ciscoasa# config t
```

Step 2: Configure a hostname for the firewall and enable password *ccnaexam*.

```
ciscoasa(config)# hostname FW-1
FW-1(config)# enable password ccnaexam
```

Step 3: Assign Ethernet0/0 (outside) to VLAN 2.

```
FW-1(config)# interface Ethernet0/0
FW-1(config-if)# switchport access vlan 2
```

Step 4: Assign Ethernet0/2 (DMZ) to VLAN 3.

```
FW-1(config-if)# interface Ethernet0/2
FW-1(config-if)# switchport access vlan 3
FW-1(config-if)# exit
```

Step 5: Configure the inside private VLAN interface 1.

```
FW-1(config)# interface Vlan 1  
FW-1(config-if)# nameif inside  
FW-1(config-if)# security-level 100  
FW-1(config-if)# ip address 192.168.1.1 255.255.255.0  
FW-1(config-if)# no shut
```

Step 6: Configure the outside public VLAN interface 2.

```
FW-1(config-if)# interface Vlan 2  
FW-1(config-if)# nameif outside  
FW-1(config-if)# security-level 0  
FW-1(config-if)# ip address 200.200.1.2 255.255.255.0  
FW-1(config-if)# no shut
```

Step 7: Configure VLAN interface 3 for DMZ server.

```
FW-1(config-if)# interface Vlan 3  
FW-1(config-if)# no forward interface vlan 1  
FW-1(config-if)# nameif dmz  
FW-1(config-if)# security-level 50  
FW-1(config-if)# ip address 200.200.3.254 255.255.255.0  
FW-1(config-if)# no shut  
FW-1(config-if)# exit
```

Step 8: Configure network address translation for access to private web server.

```
FW-1(config)# object network webserver  
FW-1(config-network-object)# host 192.168.1.2  
FW-1(config-network-object)# nat (inside,outside) static 200.200.1.2
```

Step 9: Configure a firewall rule (ACL) named HTTPS to explicitly permit access from internet user (client) to web server.

```
FW-1(config-network-object)# access-list HTTPS extended permit tcp  
                                  200.200.0.0 255.255.0.0 host 192.168.1.2 eq 443
```

Step 10: Apply firewall rule HTTPS inbound on the outside interface of firewall.

```
FW-1(config)# access-group HTTPS in interface outside
```

Step 11: Configure a default route to INET-1 router for routing to the internet.

```
FW-1(config)# route outside 0.0.0.0 0.0.0.0 200.200.1.1 1  
FW-1(config)# end
```

## Step 12: Verify Lab

Open a web browser on client desktop and connect to web server. This will verify network address translation and the firewall rule is working correctly. Run this command twice to work correctly with Packet Tracer firewall.

client: **https://200.200.1.2** (yes)

Verify that ping traffic is not permitted from the internet since there is no explicit firewall rule configured.

client: c:/>**ping 200.200.1.2** (no)