ASSIGNMENT#2

Networks & Cyber - II

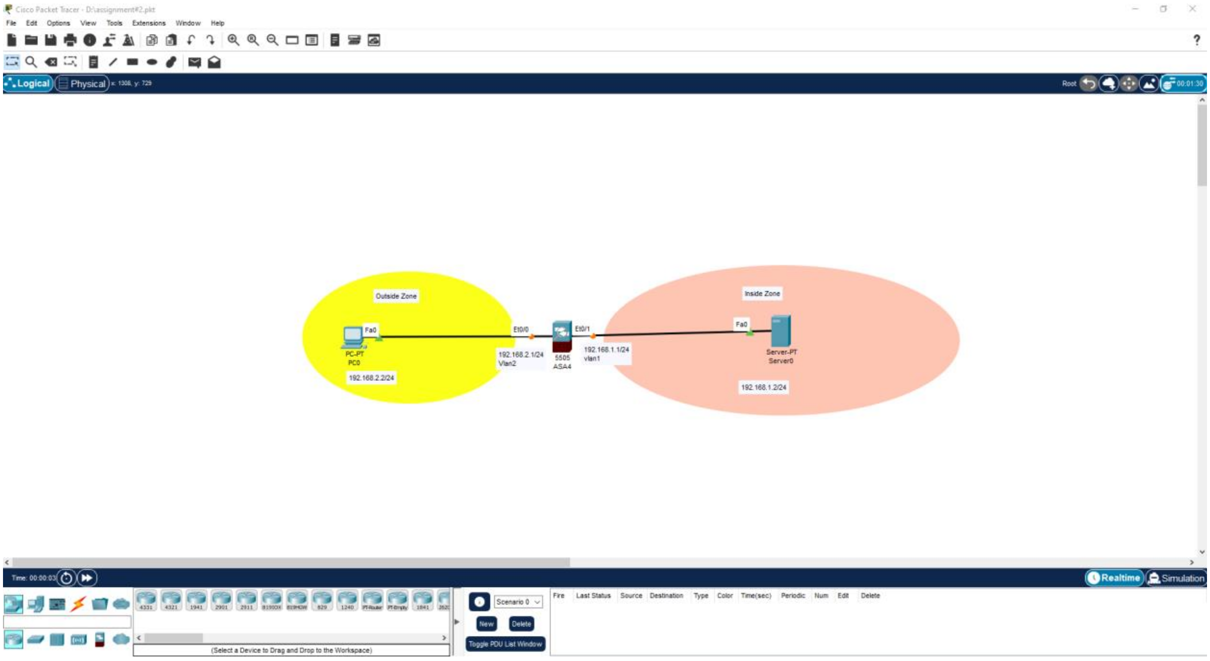
Ahmad Abdullah i22-1609

Table of Contents

Introduction

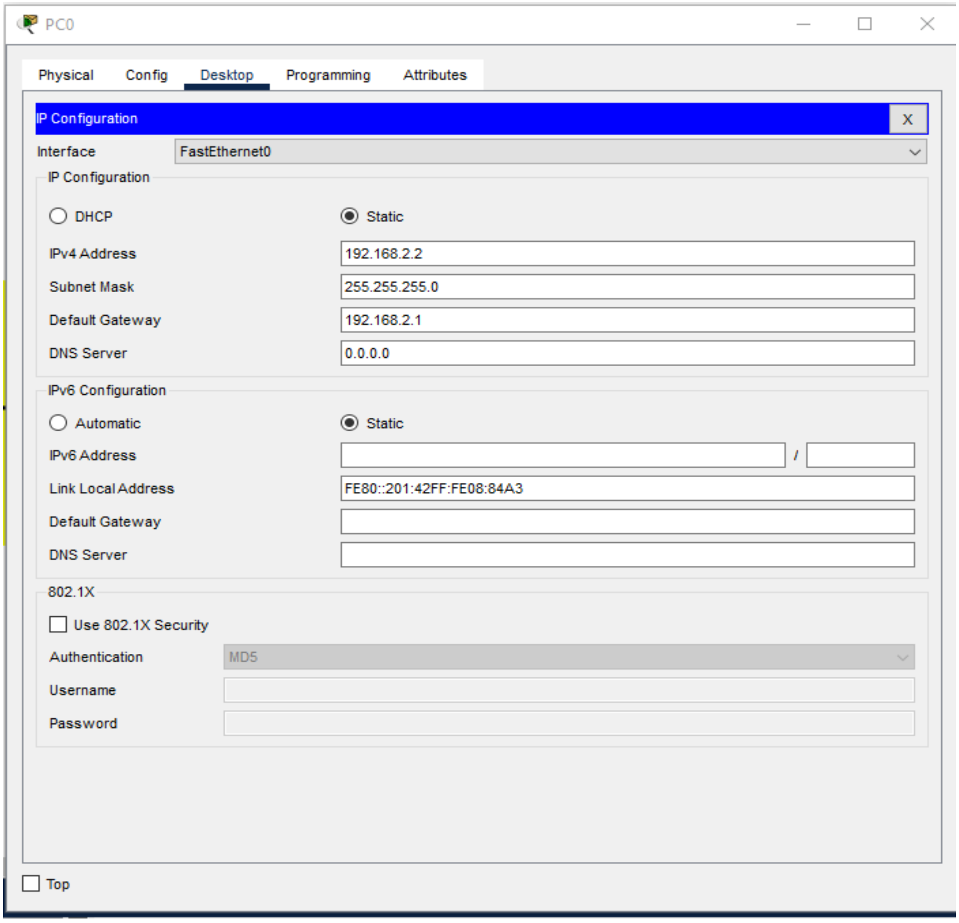
In this assignment, we were required to configure the ASA firewall. The configuration required setting up VLANs, mapping them to ethernet ports, NATing the web server’s IP and then configuring the access list to allow or deny certain services for outside networks.

The basic topology was given to us which is shown below.



Details & Steps

First, we needed to set static IPs for both the client and server and give them their respective subnets i.e. 255.255.255.0 and give them their default gateway.



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:42FF:FE08:84A3

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

After that, our only work was at ASA firewall 5505 ASA4. Configuring VLAN interfaces and then mapping ethernet interfaces on them was the next step using commands.

#enable

#configure terminal

#interface Vlan2 choosing vlan2 interface which is connected to outside network

#nameif outside for identifying the outside port

#security-level 0 setting security level to 0 because our concern is inside the network

#ip address 192.168.2.1 255.255.255.0

#no shutdown

#exit

Next up was to set up the vlan 1 on ethernet port 0/1.

#configure terminal

#interface Vlan1 choosing vlan1 interface which is connected to the inside network

#nameif inside for identifying the outside port

#security-level 100 setting security level to 100 because our concern is inside the network

#ip address 192.168.1.1 255.255.255.0

#no shutdown

#exit

The third step was to map those ethernet ports on these VLANs.

#interface Ethernet0/0

#switchport access vlan 2 maps VLAN 2 to Ethernet0/0

#no shutdown

#exit

#interface Ethernet0/1

#switchport access vlan 1 maps VLAN 1 to Ethernet0/1

#no shutdown

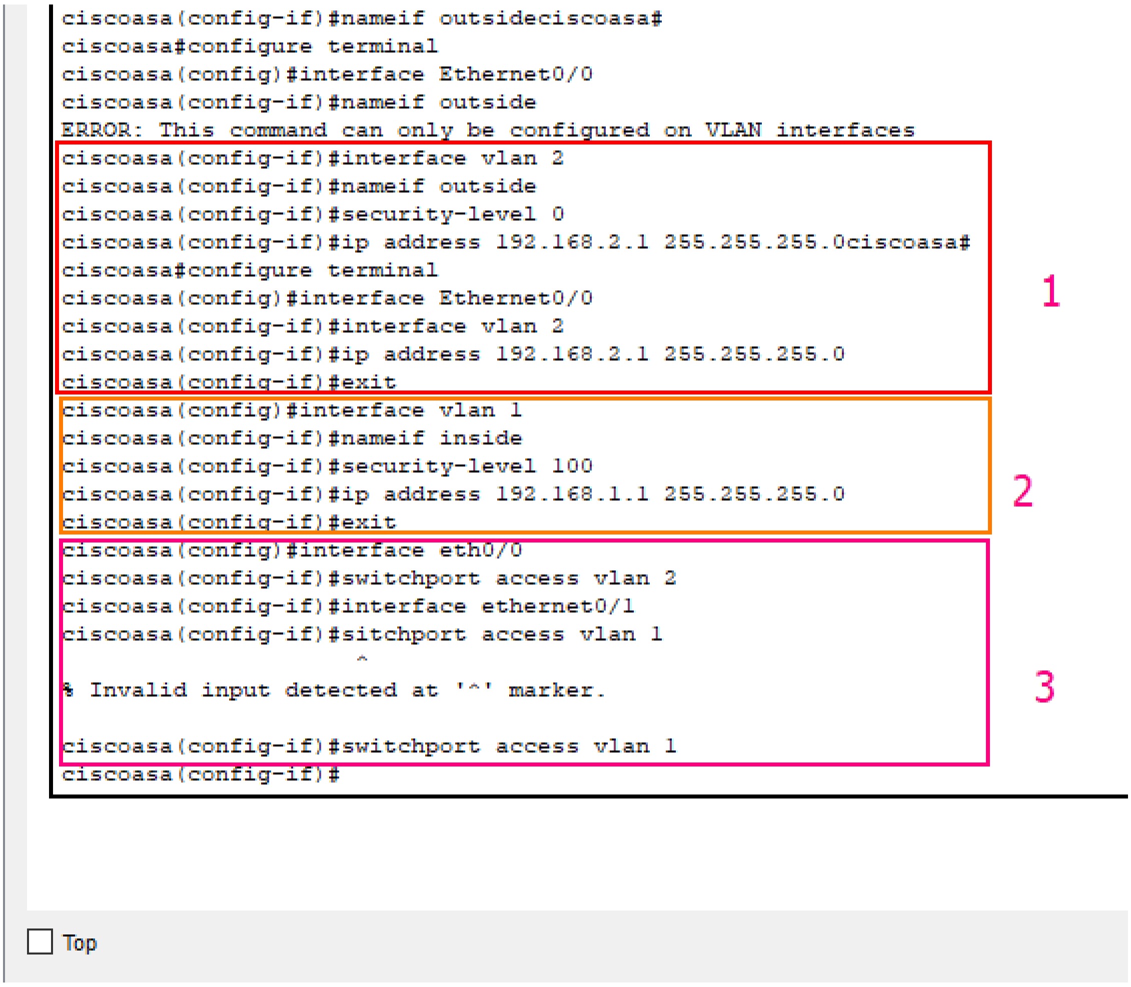
#exit

The fourth step was to do NATing on the server side to make the inner network secure to an extent.

#object network obj_server

#host 192.168.1.2

#nat (inside,outside) static 192.168.2.10



```
ciscoasa(config-if)#nameif outsideciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#interface Ethernet0/0
ciscoasa(config-if)#nameif outside
ERROR: This command can only be configured on VLAN interfaces
ciscoasa(config-if)#interface vlan 2
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address 192.168.2.1 255.255.255.0ciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#interface Ethernet0/0
ciscoasa(config-if)#interface vlan 2
ciscoasa(config-if)#ip address 192.168.2.1 255.255.255.0
ciscoasa(config-if)#exit
ciscoasa(config)#interface vlan 1
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)#exit
ciscoasa(config)#interface eth0/0
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#interface ethernet0/1
ciscoasa(config-if)#sitchport access vlan 1
                     ^
% Invalid input detected at '^' marker.

ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#
```

The Fifth step is to set an access list to ensure that clients from outside the network can only access certain services such as HTTP and ICMP/Ping.

Commands were as follows:

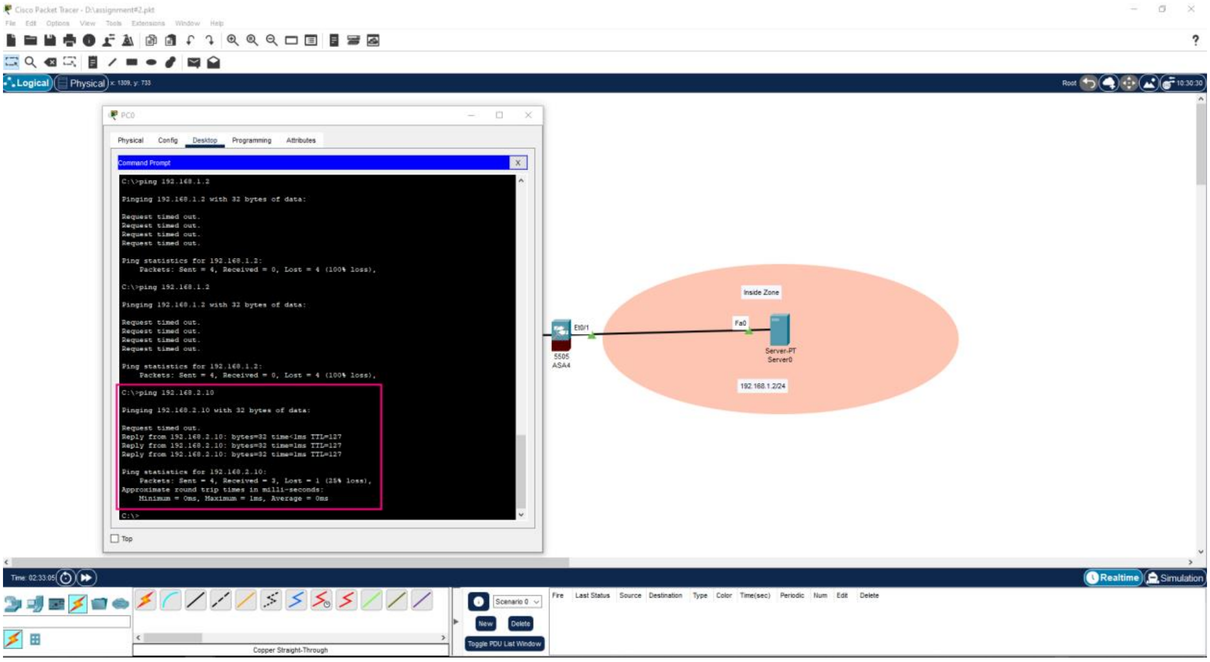
`#access-list 101 permit tcp any host 192.168.2.10 eq 80` for HTTP

`#access-list 101 permit tcp any host 192.168.2.10 eq 443` for HTTPS

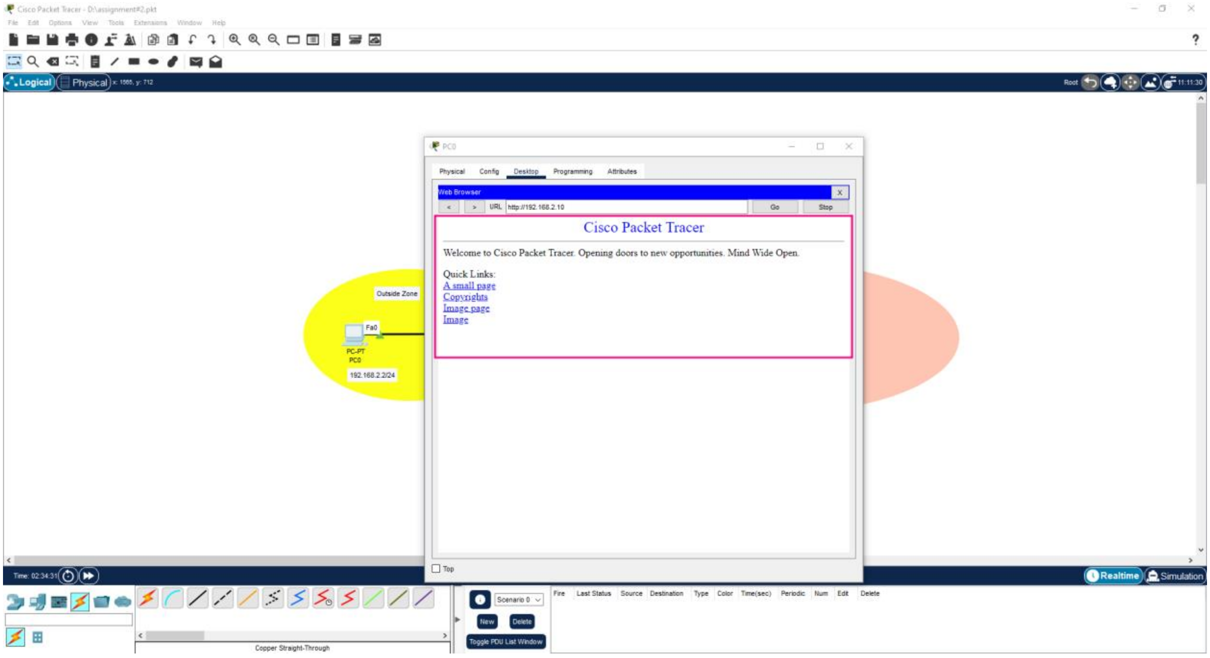
`#access-list 101 permit icmp any host 192.168.2.10 echo`

`#access-list 101 deny ip any any`

These commands will allow TCP connection on ports 80 and 443 from outside to the server and ping to the server. To ensure security and that this server is only used for web services we deny every other type of packet on the firewall.



```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time=1ms TTL=127
Reply from 192.168.2.10: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

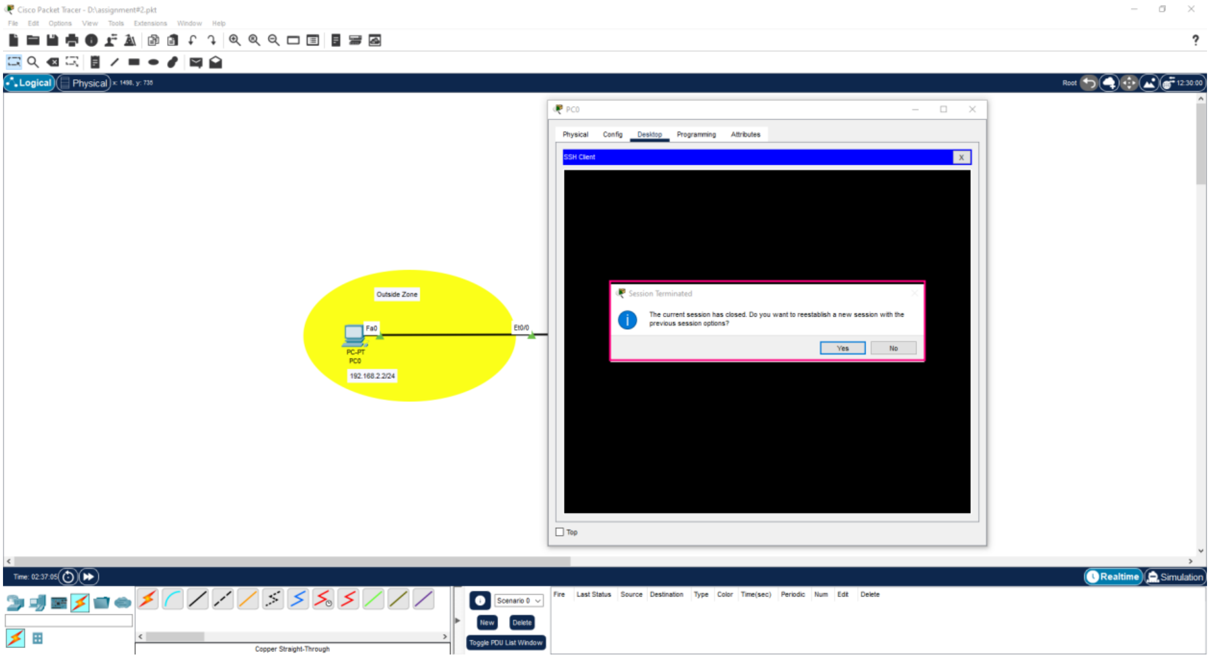


http://192.168.2.10

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image



Session Terminated

The current session has closed. Do you want to reestablish a new session with the previous session options?

Yes No

Outputs

Show Switch Vlan

```
VLAN Name                      Status     Ports

---- ------------------------------- --------- -------------------------------

1    inside                    up         Et0/1, Et0/2, Et0/3, Et0/4Et0/5, Et0/6, Et0/7

2    outside                   up         Et0/0
```

Show Nat

```
Auto NAT Policies (Section 2)

1 (inside) to (outside) source static WebServer 192.168.2.10

translate_hits = 0, untranslate_hits = 0
```

Show Xlate

```
1 in use, 1 most used

Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s - static, T - twice, N - net-to-net

NAT from inside:192.168.1.2/32 to outside:192.168.2.10/32 flags s idle 00:37:53, timeout 0:00:00
```

Show Access List

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300

access-list 101; 4 elements; name hash: 0xd408307a

access-list 101 line 1 extended permit tcp any host 192.168.2.10 eq www(hitcnt=0) 0xd39900e6

access-list 101 line 2 extended permit tcp any host 192.168.2.10 eq 443(hitcnt=0) 0x6db7b052

access-list 101 line 3 extended permit icmp any host 192.168.2.10 echo(hitcnt=0) 0x71107907

access-list 101 line 4 extended deny ip any any(hitcnt=0) 0xc158e801
```

Show running-config

```
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
```

```
ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.2.1 255.255.255.0
!
object network WebServer
host 192.168.1.2
nat (inside,outside) static 192.168.2.10
!
!
access-list 101 extended permit tcp any host 192.168.2.10 eq www
access-list 101 extended permit tcp any host 192.168.2.10 eq 443
access-list 101 extended permit icmp any host 192.168.2.10 echo
access-list 101 extended deny ip any any
!
!
access-group 101 in interface outside
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
```