ASSUMPTION UNIVERSITY

FACULTY OF ENGINEERING

COMPUTER ENGINEERING

CE4224 TELECOMMUNICATION NETWORK LABORATORY
SECTION 641
SEMESTER 2/2022

WEEK11
FIREWALL
IN DIFFERENT NETWORK

SUBMITTED TO: **A. Sneha Paudel**
SUBMITTED BY: **Mr. Senee Suksawat ID: 6235107**

DATE: 2023/02/15

Introduction

A firewall is a computer network security system that restricts internet traffic in, out, or within a private network.

This software or dedicated hardware-software unit functions by selectively blocking or allowing data packets. It is typically intended to prevent anyone—inside or outside a private network from engaging in unauthorized web activities and to help prevent malicious activity.

Firewalls can be viewed as gated borders or gateways that manage the travel of permitted and prohibited web activity in a private network. The term comes from the concept of physical walls being barriers to slow the spread of fire until emergency services can extinguish it. Comparably, network security firewalls are for web traffic management typically intended to slow the spread of web threats.

Firewalls create 'choke points' to funnel web traffic, at which they are then reviewed on a set of programmed parameters and acted upon accordingly. Some firewalls also track the traffic and connections in audit logs to reference what has been allowed or blocked.

Firewalls are typically used to gate the borders of a private network or its host devices. As such, firewalls are one security tool in the broader category of user access control. These barriers are typically set up in two locations on dedicated computers on the network or the user computers and other endpoints themselves (hosts).

Objective

Create a simple Local Area Network contains a firewall in Cisco Packet Tracer.
Configure Router and Firewall and understand inside and outside address of NAT.
We should be able to ping successfully from Firewall to PC and Router.

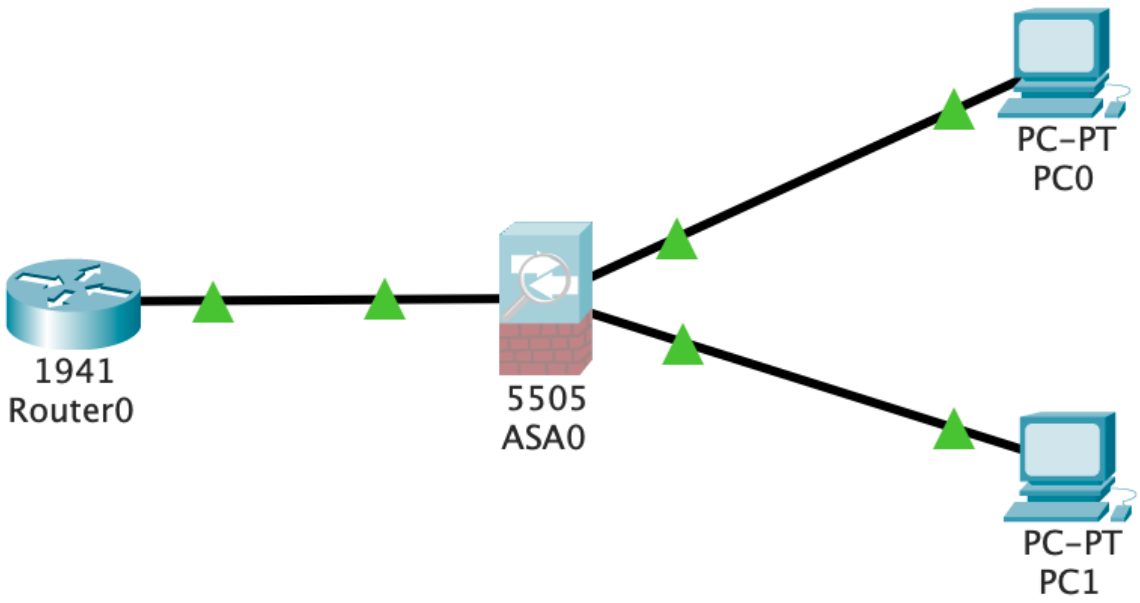
Apparatus

Laptop
Cisco Packet Tracer
2 PC in Cisco Packet
Router (1941 Series)
ASA, adaptive security appliance. (It delivers firewall capabilities)

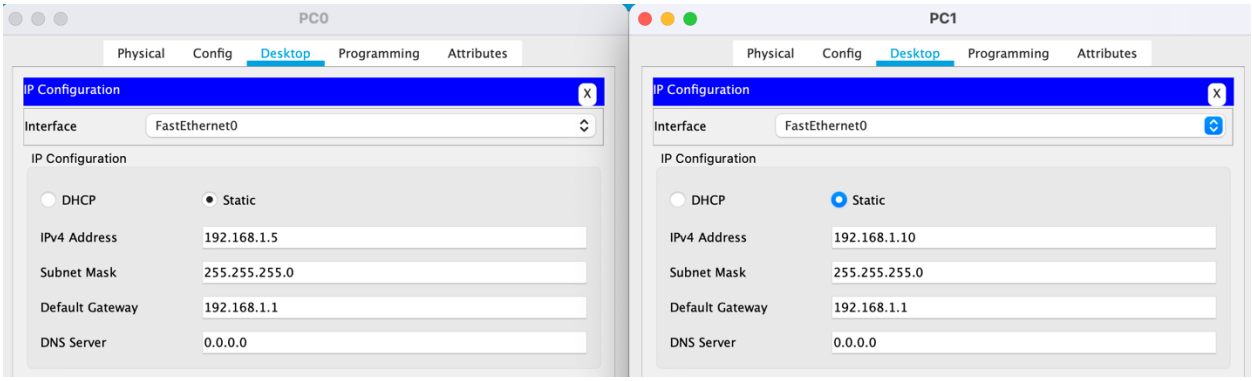
Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	Fast Ethernet	192.168.1.5	255.255.255.0	192.168.1.1
PC2	Fast Ethernet	192.168.1.10	255.255.255.0	192.168.1.1
Router	GigabyteEthernet LAN 2	10.1.1.1 11.1.1.1	255.255.255.0 255.255.255.0	-

Topology



Step 1 Configure the IP Address and Default Gateway for two PCs



Step 2 Configure the router

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Senee
Senee(config)#interface giga 0/0
Senee(config-if)#ip address 10.1.1.1 255.255.255.0
Senee(config-if)#no shutdown

Senee(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

Step 3 Define the dhcp pool for the router and set the IP address to interface Loopback2 to be 11.1.1.1 as assigned

```
Senee(config-if)#exit
Senee(config)#ip dhcp pool isp
Senee(dhcp-config)#network 10.1.1.0 255.255.255.0
Senee(dhcp-config)#default-router 10.1.1.1
Senee(dhcp-config)#exit
Senee(config)#interface 12
                        ^
% Invalid input detected at '^' marker.

Senee(config)#%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 10.1.1.1.

Senee(config)#interface l2

Senee(config-if)#
%LINK-5-CHANGED: Interface Loopback2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, changed state to up

Senee(config-if)#ip address 11.1.1.1 255.255.255.0
Senee(config-if)#exit
Senee(config)#
```

Step 4 Check the connection by pinging

```
ciscoasa#ping 192.168.1.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/23 ms

ciscoasa#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/21 ms

ciscoasa#ping 11.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Step 5 Set the IP route and the NAT for ASA and check ping 11.1.1.1 again

```
ciscoasa#config t
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 10.1.1.1
ciscoasa(config)#object network NAT
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#nat(inside, outside) dynamic interface
                                ^
% Invalid input detected at '^' marker.

ciscoasa(config-network-object)#nat (inside, outside) dynamic interface
ciscoasa(config-network-object)#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.1.1.1 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 2 subnets
C       10.0.0.0 255.255.255.0 is directly connected, outside, Vlan2
C       10.1.1.0 255.255.255.0 is directly connected, outside, Vlan2
C    192.168.1.0 255.255.255.0 is directly connected, inside, Vlan1
S*   0.0.0.0/0 [1/0] via 10.1.1.1
ciscoasa(config-network-object)#ping 11.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.1.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

ciscoasa(config-network-object)#
```

Step 6 Check the result by pinging

```
ciscoasa(config-network-object)#exit
ciscoasa#ping 192.168.1.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/18 ms

ciscoasa#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/18 ms

ciscoasa#ping 11.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

ciscoasa#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms

ciscoasa#
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 dhcp
!
object network NAT
 subnet 192.168.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1
!
!
!
object network NAT
 nat (inside,outside) dynamic interface
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
```

Conclusion

In this experiment, I have learned what is firewall, and how it's works to protect the internet network. And we learned by using real component in cisco packet program which made me more clearly about how it works and how to command in the asa.