Performance Assessment – Firewall and Port Security

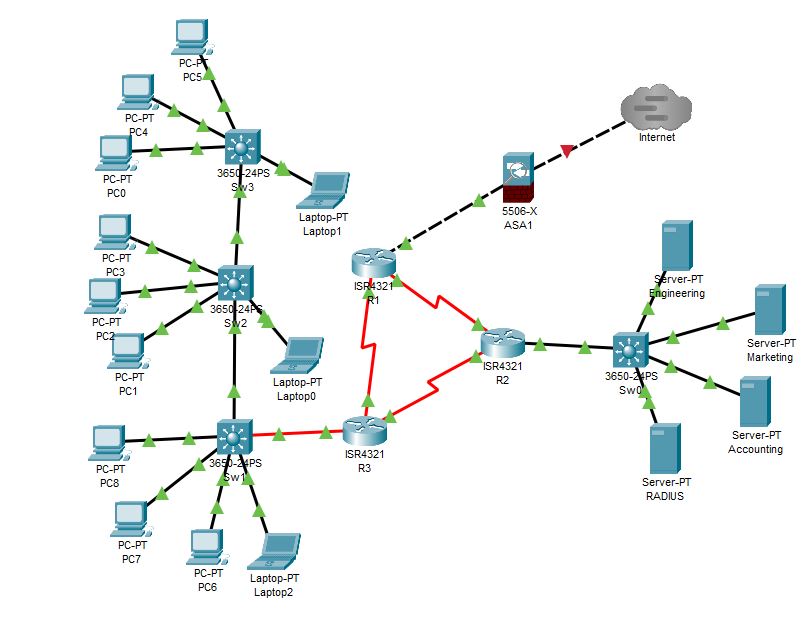
In this lab you will be reviewing the networking that you have learned in your program. You will be using Packet Tracer for the lab.

Your network will a class B network based on a number assigned by your professor, which you will be using for the duration of the class. In the lab anytime you see an underline you should fill in this number.

**Student network: 10.\_\_\_\_.0.0/16**

**Task 1 – Add a firewall to your network**

**Using the network you completed 1.4 Performance Assessment: ACLs, you are going to add a firewall and program them to permit only specific traffic to your network.**



**Adding a firewall**

First place one ASA5506 firewall into your network as shown in the diagram. Change the name of each ASA to match the diagram.

Change the programming on your R1 router by changing the G0/0/1 address to 11.2.0.\_\_\_ 255.255.255.0

R1(config)# interface G0/0/1

R1(config-if)# ip address 11.2.0.\_\_\_ 255.255.255.0

Update OSPF on R1 to include the new address of G0/0/1. First let’s remove the original OSPF configuration-

(config) #router ospf 1

*(config-router) #no network 11.0.0.0 255.255.255.0 area 0*

Now let’s update OSPF to include the new address of G0/0/1.

(config) #router ospf 1

(config-router) #network 11.2.0.0 255.255.255.0 area 0

Now program your ASA1 interfaces. You will need to go into enable mode and then hit Enter key when prompted for a password.

ciscoasa>en

Password:

ciscoasa#

(config) #interface GigabitEthernet1/1

(config-if) #nameif inside

(config-if) #security-level 100

(config-if) #ip address 11.2.0.1 255.255.255.0

(config-if) #interface GigabitEthernet1/2

(config-if) #nameif outside

(config-if) #security-level 0

(config-if) #ip address 11.0.0.20 255.255.255.0

(config-if) #interface GigabitEthernet1/3

(config-if) #nameif DMZ

(config-if) #security-level 50

(config-if) #ip ip address 172.16.1.1 255.255.255.0

Program your extended ACL per the below information

(config) #access-list OUTSIDE extended permit icmp any any echo-reply

(config) #access-list OUTSIDE extended permit ip any 11.0.0.0 255.255.255.0

(config) #access-list OUTSIDE extended permit ip any 10.0.0.0 255.0.0.0

Apply the access-list to the outside interface

(config) #access-group OUTSIDE in interface outside

Create the NAT for your network allowing communication from inside to outside the firewall.

(config) #object network LAN

(config-network-object) #subnet 11.2.0.0 255.255.255.0

(config-network-object) #nat (inside,outside) dynamic interface

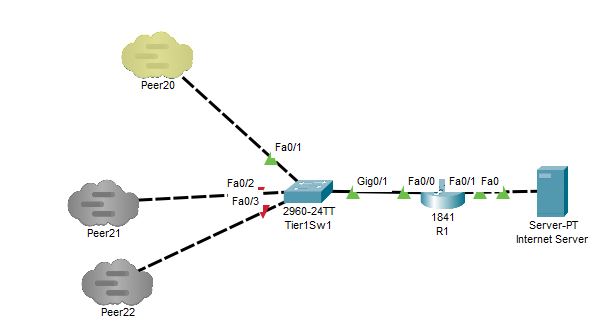
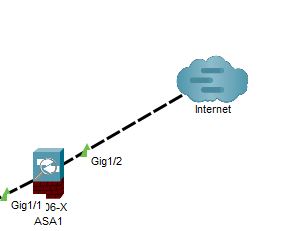
Setup OSPF for your firewall

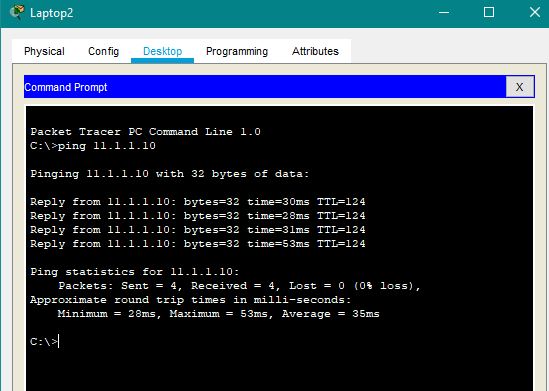
(config) #router ospf 1

(config-router) #network 11.2.0.0 255.255.255.0 area 0

(config-router) #network 11.0.0.0 255.255.255.0 area 0

Verify that your connection through the firewall works by connecting to the Tier1 network via Multiuser cloud and ping the Teir1 Internet Server (11.1.1.10) to verify connectivity. You can ping from one of PCs/laptops, but keep in mind we turned off the Internet for Marketing (VLAN 20) in the last lab.





**Deliverables**

* + Screenshot of your working network
  + Screenshot of the firewall configuration (show run)
  + Screenshot of routing table from the firewall (show route)
  + Screenshot of a successful ping from one of the PCs/laptops to the Tier 1 Internet Server

PASTE SCREENSHOTS BELOW

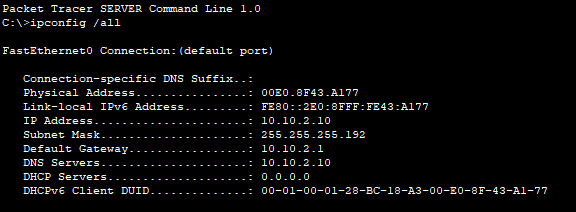
**Task 2 – Add port security**

Port security is a basic network security procedure. In this process you are limiting the systems that can be connected to your network by specifying the valid MAC addresses that can be connected through a switch.

You can either manually enter the MAC addresses for valid systems or let the system dynamically learn the MAC addresses and then turn off dynamic learning.

When configured with a MAC address, or group of MAC addresses, the switch will forward only packets for these devices. Any other packets received will be discarded.

Go to the Engineering Server and open up a command prompt. At the command prompt type ***ipconfig /all*** to determine your MAC address. The MAC address, or Physical Address, will look like this XXXX.XXXX.XXXX.



Now that you have the MAC address of the Engineering Server, you will configure port security on the switch port it connects to. Make sure you configure only the port that the Engineering Server plugs into the switch- GigabitEthernet1/0/X represents this port below.

Sw0(config)# **interface GigabitEthernet 1/0/X**

Sw0(config-if)# **switchport port-security**

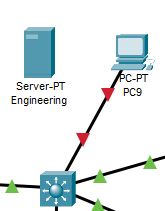
Sw0(config-if)# **switchport port-security mac-address XXXX.XXXX.XXXX**

Capture your configuration of this port with a screenshot.

We will now test the port security we just configured. Add a PC and move the cable from the switch to Engineering Server over to the PC. Statically assign the IP address, subnet mask and default gateway for the PC to match the Engineering Server.

Go to the switch and run the following command:

Sw0# **show interface GigabitEthernet 1/0/X**

****

What happens to the link between the PC and switch? What does the show interface command display about the port in regards to port security?

We will now unplug the PC and plug in the Engineering Server.

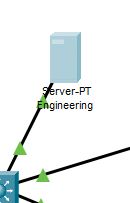
Next remove port security from the switch port and “bounce” the port.

Sw0(config-if)# **no switchport port-security mac-address XXXX.XXXX.XXXX**

Sw0(config-if)# **shutdown**

Sw0(config-if)# **no shutdown**

Your server should now be back to normal and be able to communicate with the network. Test network connectivity by pinging a device on the network. Take a screenshot.



**Deliverables**

* Screenshot of port security configured on switch port
* Answer the questions about port-security
* Screenshot of ping from Engineering Server to a device on the network

PASTE SCREENSHOTS BELOW