**NAME: P.NITYASREE**

**REGNO: 17MIS1007**

**COURSE: INFORMATION SECURITY MANAGEMENT[CSE 3502]**

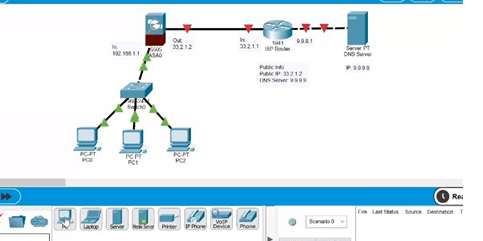
**FACULTY: ANUSHA**

**LAB EXERCISE-3 FIREWALL**

**Step 1 : Design a topology**

Computers connected via switch. It has a gateway to the internet via a router from the ISP, which is further connected to a DNS Server to lookup queries and give results. We add a firewall between the ISP router and the private network to monitor and filter incoming and outgoing packets.

**Step 2 : Make connections :**

**Step 3: Decide on IPs**

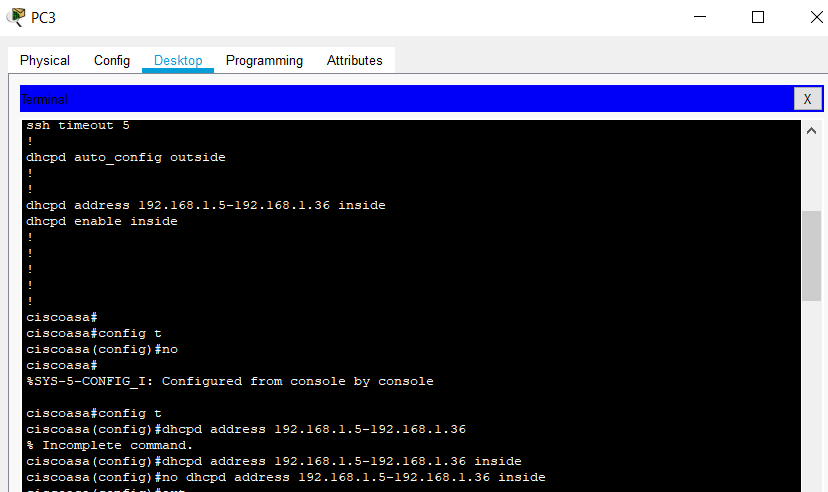
**ISP / Public Info :**

The ISP will provide an IP to communicate with the internet, called a public IP. Put that in your outgoing Firewall. We assume something like 33.2.1.2, and keeping a similar IP scheme, the ISP router in has 33.2.1.1. That will be your gateway.

**Private info :**

192.168.1.1 as incoming for firewall.

**Step 4 :Configure IP**

****

**Step 4.1 - The ASA Firewall**

**Inside**

* config t -In the int (interface) vlan1
* ip add [our inside ip] [our mask] (here, 192.168.1.1 255.255.255.0 for inside / private network)
* nameif inside
* security-level 0
* int [what physical port is connected for our inside firewall] (here, et0/0)
* switchport access vlan 1

**Outside**

* Config t -Int vlan 2
* Ip add [our outside ip] [our mask] (here, 33.2.1.2 255.0.0.0 for outside / public network)
* Nameif outside
* Security-level 100
* Int [what physical port is connected for our outside firewall] (here, et0/1)
* Switchport access vlan 2
* Exit

Inside - interface connected with private network

Outside - interface connected with public network

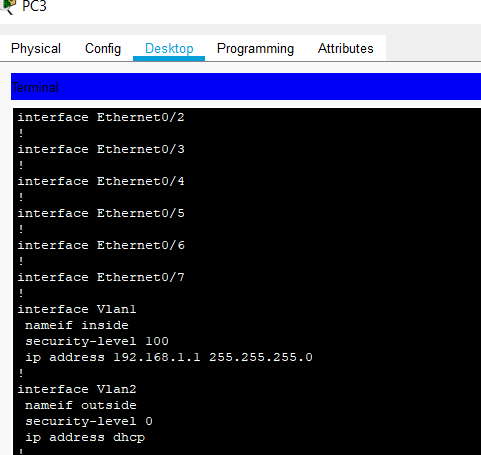
Nameif - gives interface a name

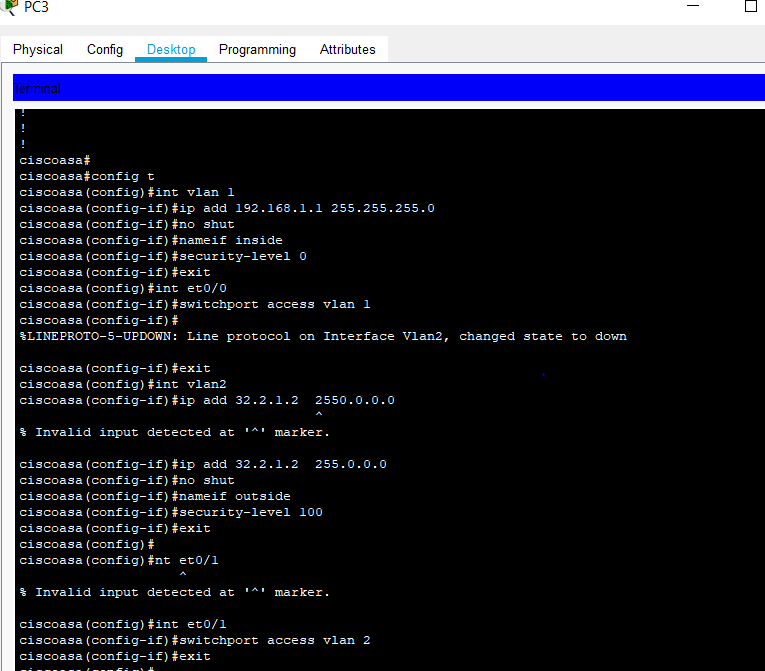
Security level: 0-100

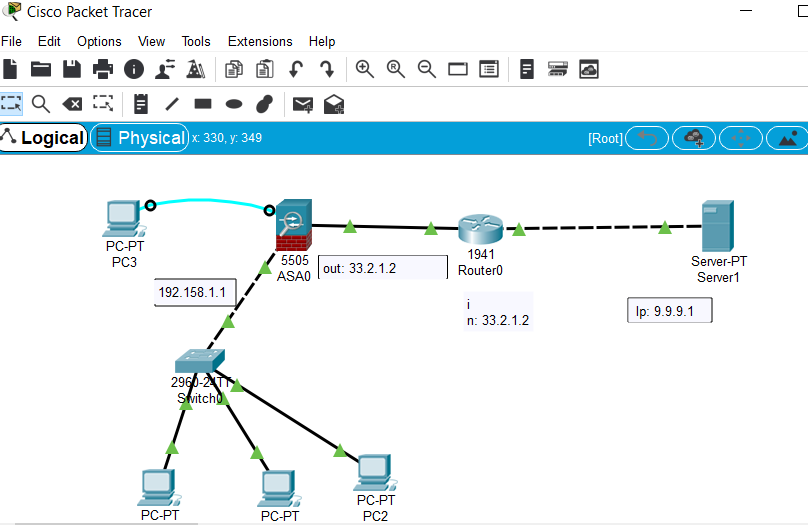
0: high asf security - Inside

100: lax asf - Outside

1-99: flexible - DMZ







**Step 4.2 - The Router**

Go to the CLI  and enable

* Int gig0/0
* Ip add [router in ip] (here, 33.2.1.1 255.0.0.0)
* No shut
* Exit
* Int gig0/1
* Ip add [router out ip] (here, 9.9.9.1)
* No shut
* Ctrl+c

Router in is gig0/0

Router out is gig0/1

**Step 5**

Set up the server

IP: 9.9.9.9

Subnet Mask: 255.0.0.0

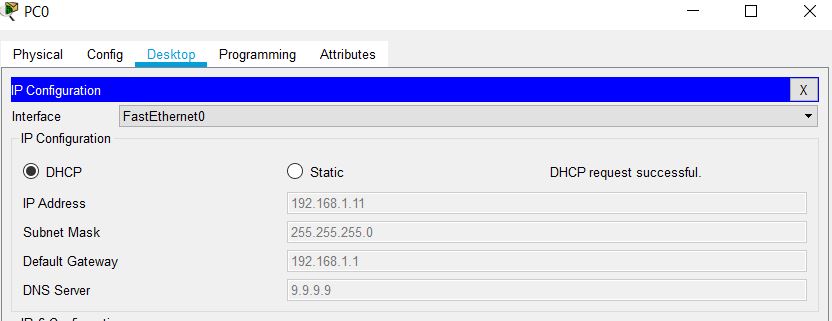
Default Gateway: 9.9.9.1

**Step 6**

Set up DHCP and DNS Server on the ASA

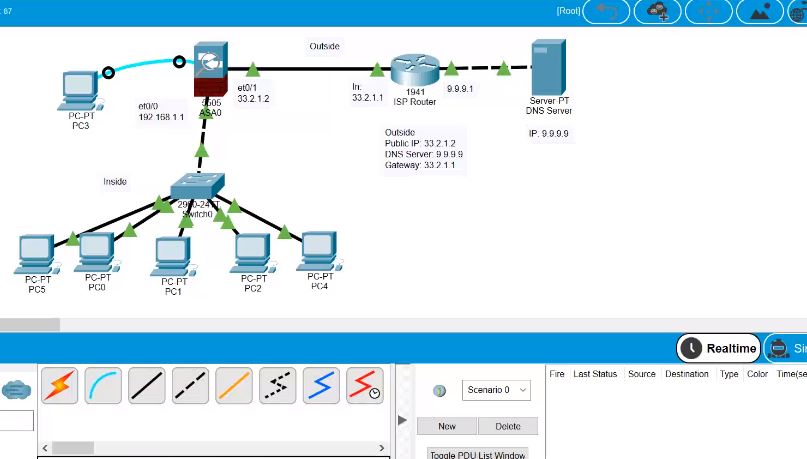
Open up Terminal on Server console

* Conf t
* Dhcpd address [inside ip range for network] (here, let's say 192.168.1.10-192.168.1.30) inside
  + The range depends on the number of computers you want in your network
  + 10 - 30 is the range we specified here
* Dhcpd dns 9.9.9.9 interface inside
  + Basically configuring the DNS Ip on the dhcp server
* exit



Set DHCP on for the PCs and see if it works

**Step 7 : Configure default route on ASA**



Open up terminal again

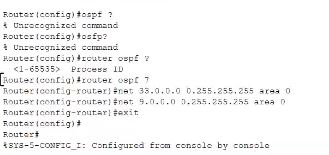
* Config t
* Route outside 0.0.0.0 0.0.0.0 33.2.1.1
  + Any IP
  + Any subnet
  + 33.2.1.1 is the IP of the router

**Step 8**

Configure Dynamic Route using OSPF Routing protocol!

 Go to router's CLI

* Config t
* Ospf 1
  + 1 - Process ID
* Net 33.0.0.0 0.255.255.255 area 0
  + Networks connected? 33 and 9
  + 0.255.255.255 means anything with 33.x.x.x IP is included
    - If it was 33.1.0.0 0.0.255.255, anything with 33.1.x.x IP is included
* Net 9.0.0.0 0.255.255.255 area 0

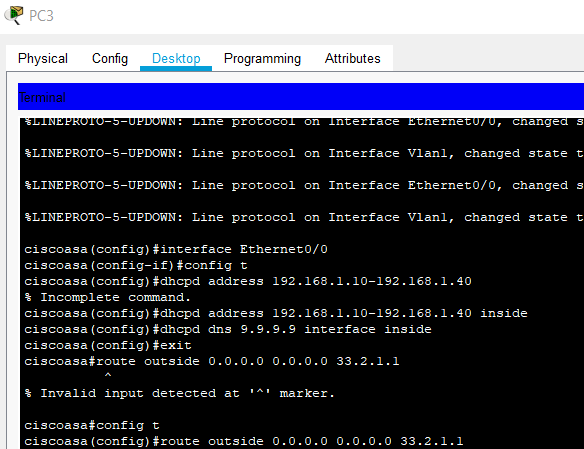


**Step 9** :

configure a way for the inside network to communicate with the outside using NAT

Terminal of the ASA:

* Config t
* Object network [name of object network]
* Subnet [subnet IP] [subnet mask]
  + Here, our private network runs on IP 192.168.1.0
  + So, our subnet can be 192.168.1.0 and the mask can be 255.255.255.0 or even 192.168.0.0 255.255.0.0 or even 192.0.0.0 255.0.0.0
* Nat (inside, outside) dynamic interface
  + NAT - Network Address Translation. Network address translation is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. So, we basically connect the private and public ips.



A subnet is a smaller division of a bigger network.

 192.168.0.0

192.168.1.1

192.168.1.2

192.168.2.1

192.168.3.1

192.168.3.2

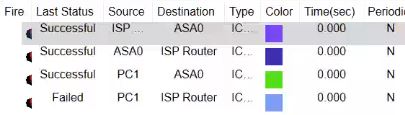
192.168.3.3

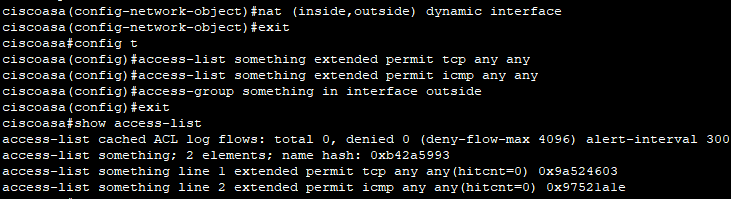
**Step 10**

ACL on the firewall

Terminal of ASA:

* Config t
* Access-list [nameoflist] extended permit tcp any any
  + Any source
  + Any destination
* Access-list [nameoflist] extended permit icmp any any
  + Allows icmp packets too
* Access-group [nameoflist] in interface outside
  + In for input traffic
  + Out for output traffic
  + Activates ACL and gives input traffic to the outside network





END