

CSE3502

INFORMATION SECURITY MANAGEMENT

Prof. Ayesha S.

LABORATORY MANUAL

LAB- 7

Submitted by

Harshit Maheshwari – 19BCE1040



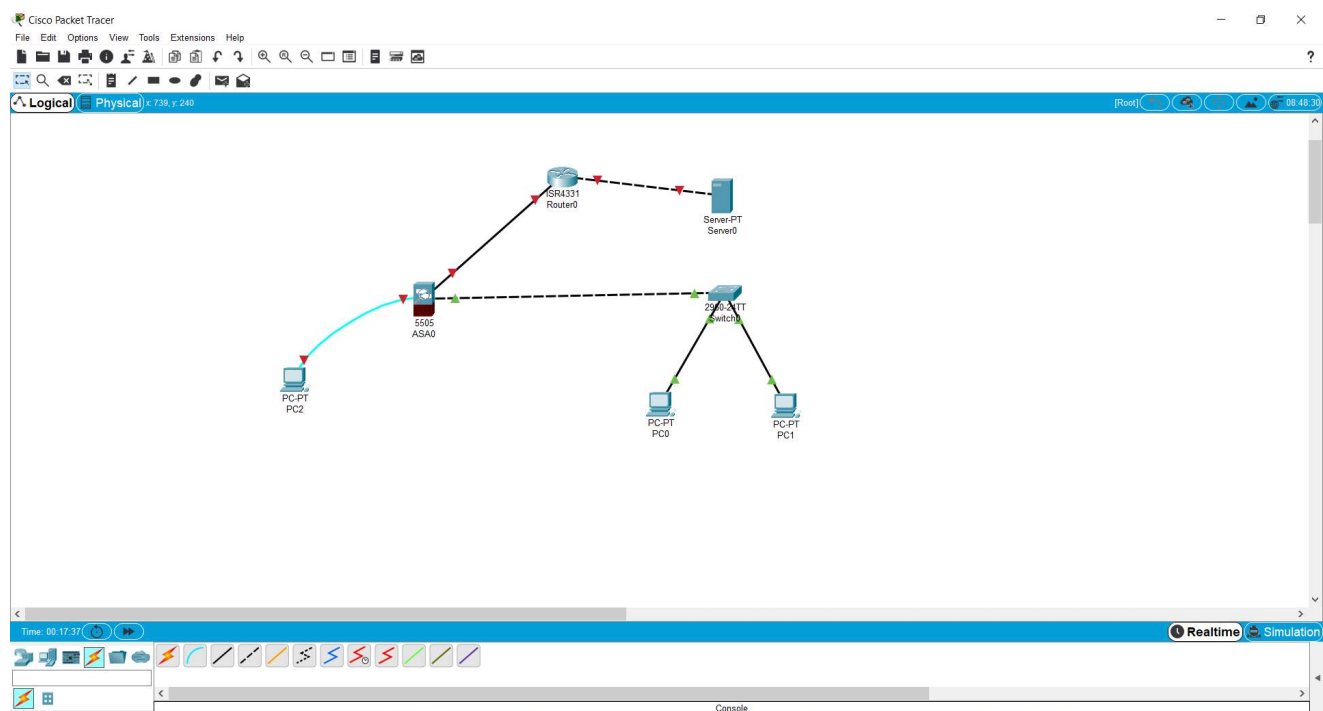
VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

3rd March 2022

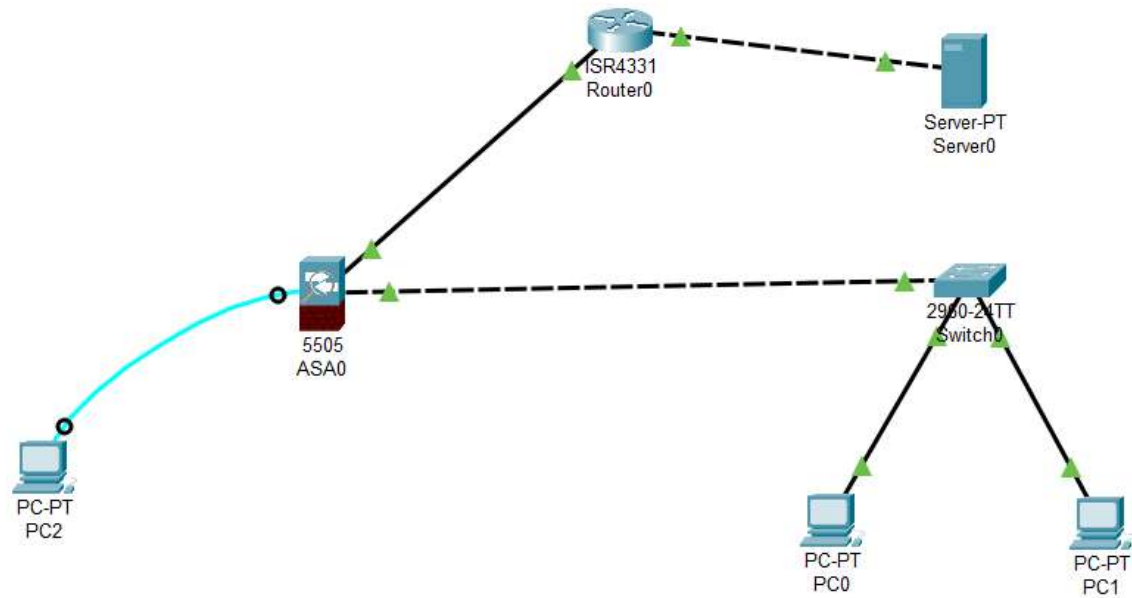
AIM- Create a network topology with a CISCO ASA Firewall, Router, Switch, 3 PCs and a Server. Here, a PC is to be connected with ASA Firewall and two PCs are to be connected with switch. Do the following: 1. Create two VLANs 2. Configure the Router, Server and Firewall. 3. Ensure the firewall functionality by demonstrating the packet transmission between the PCs and Server. 4. Apply NAT 5. Use DHCP and ICMP protocols 6. Ping the connected PCs NAT Configuration

PROCEDURE:

Step 1- Create a Topology



Step 2- Turn on the router



Step 3- Configuring 1 st VLAN with firewall.

Cisco Packet Tracer

File Edit Options View Tools Extensions Help

Logical Physical 11:51, v 195

```
terminal
ciscoasa(config)#conf t
ciscoasa(config)#sh running-config
: Saved
:
ASA Version 9.4(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 dhcp
!
!
!
More -->
```

```
!  
telnet timeout 5  
ssh timeout 5  
!  
dhcpd auto_config outside  
!  
!  
dhcpd address 192.168.1.5-192.168.1.36 inside  
dhcpd enable inside  
!  
!  
!  
!
```

```
ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.36 inside  
ciscoasa(config)#
```

Setting Security Level as 100 means Insite traffic incoming as this is a Local Area Network.

```
% Incomplete command.  
ciscoasa(config)#int vlan 1  
ciscoasa(config-if)#ip add 10.1.1.1 255.0.0.0  
ciscoasa(config-if)#no shut  
ciscoasa(config-if)#nameif inside  
ciscoasa(config-if)#security-level 100  
ciscoasa(config-if)#exit  
ciscoasa(config)#
```

Step 4- Configuring 2nd VLAN with firewall.

0 Security in Firewall means Outside traffic

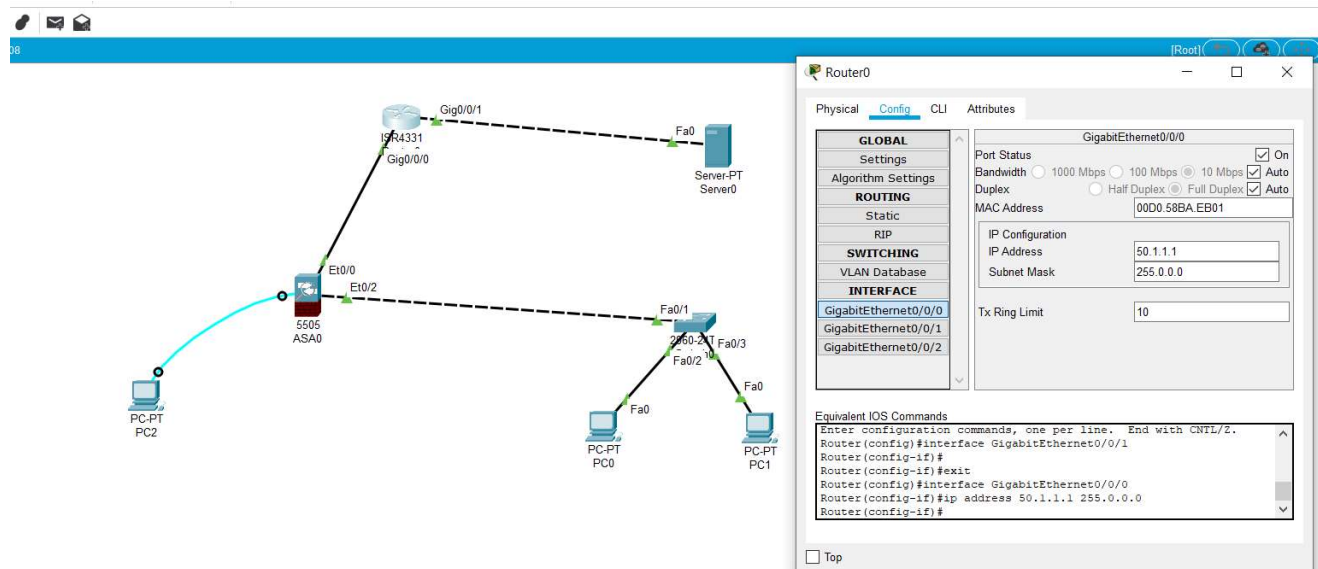
```
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#int e0/2
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#exit
ciscoasa(config)#v
^
% Invalid input detected at '^' marker.

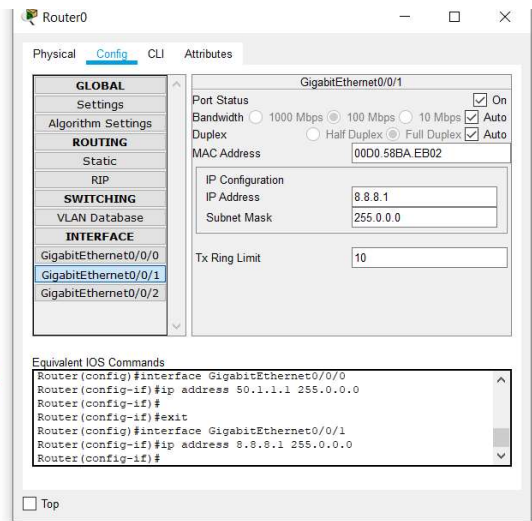
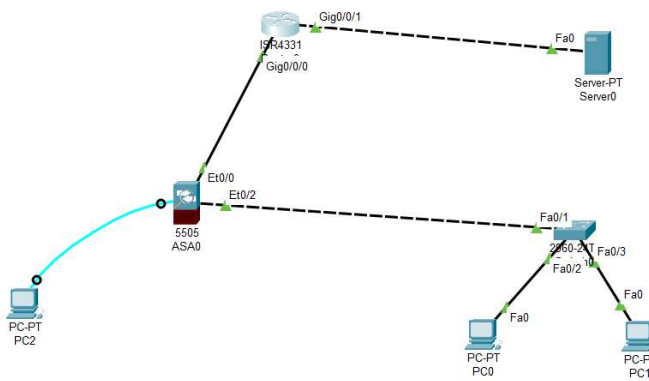
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip add 50.1.1.2 255.0.0.0
ciscoasa(config-if)#no shut
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#exit
ciscoasa(config)#intint e0/0
^
% Invalid input detected at '^' marker.

ciscoasa(config)#int e0/0
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#
```

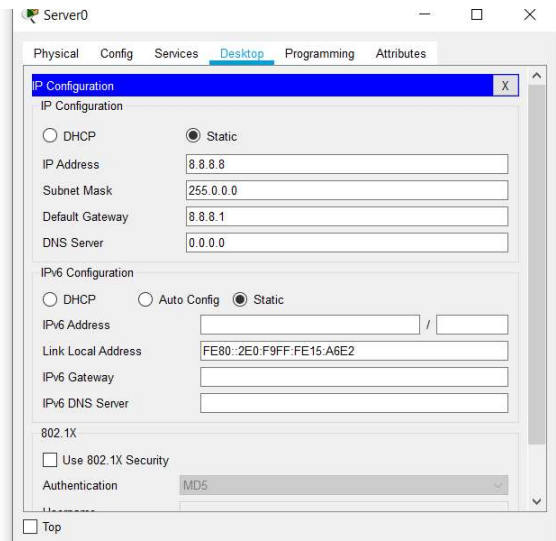
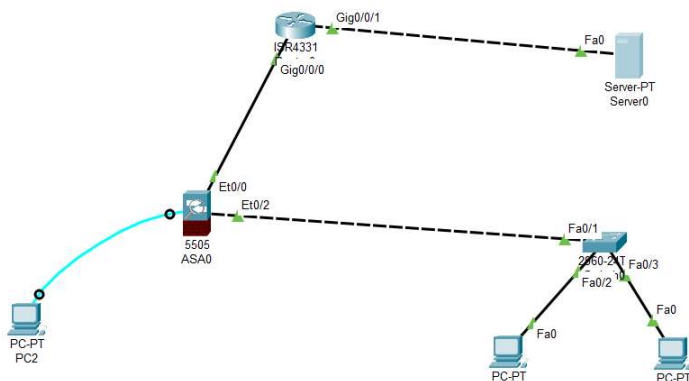
☐ Top

Step 5- Setting the IP Address on Router

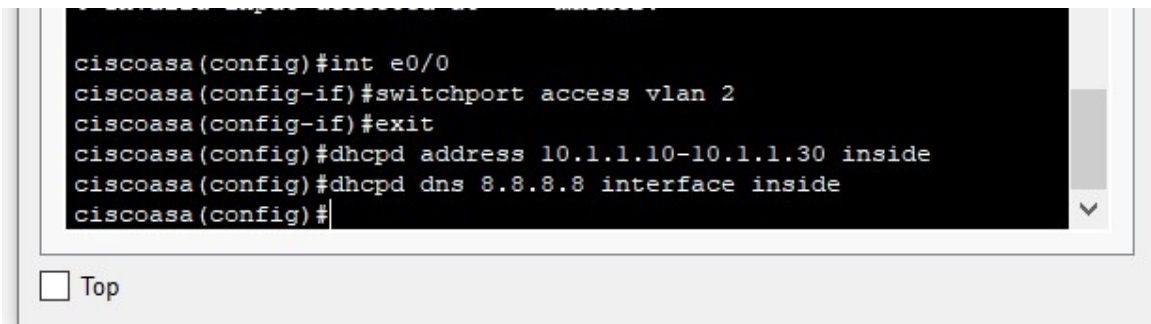




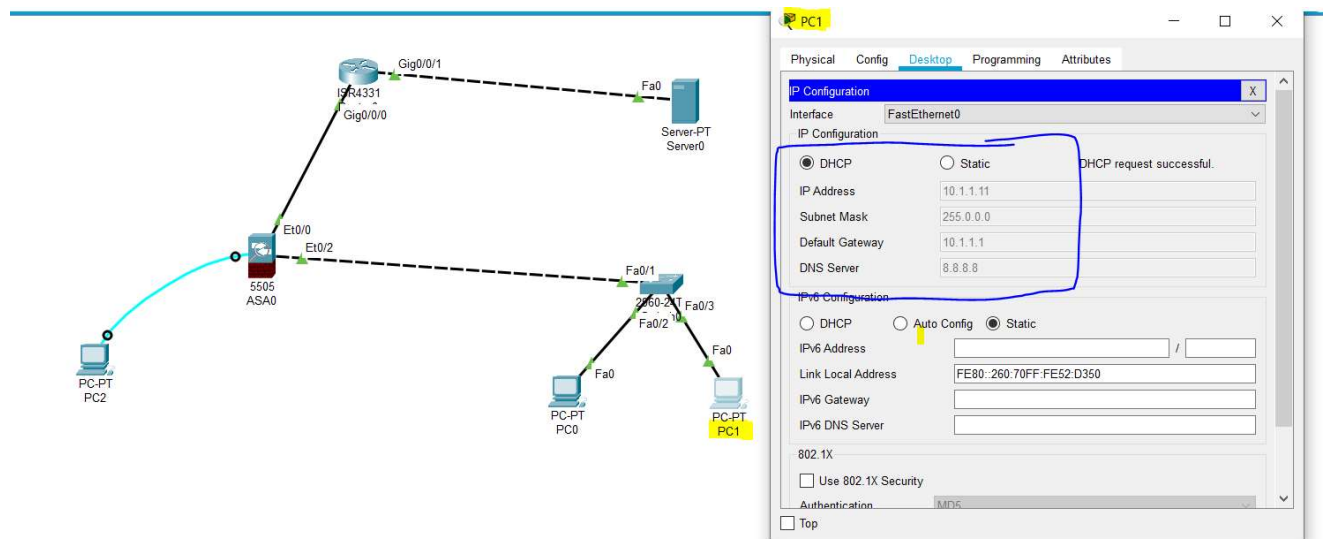
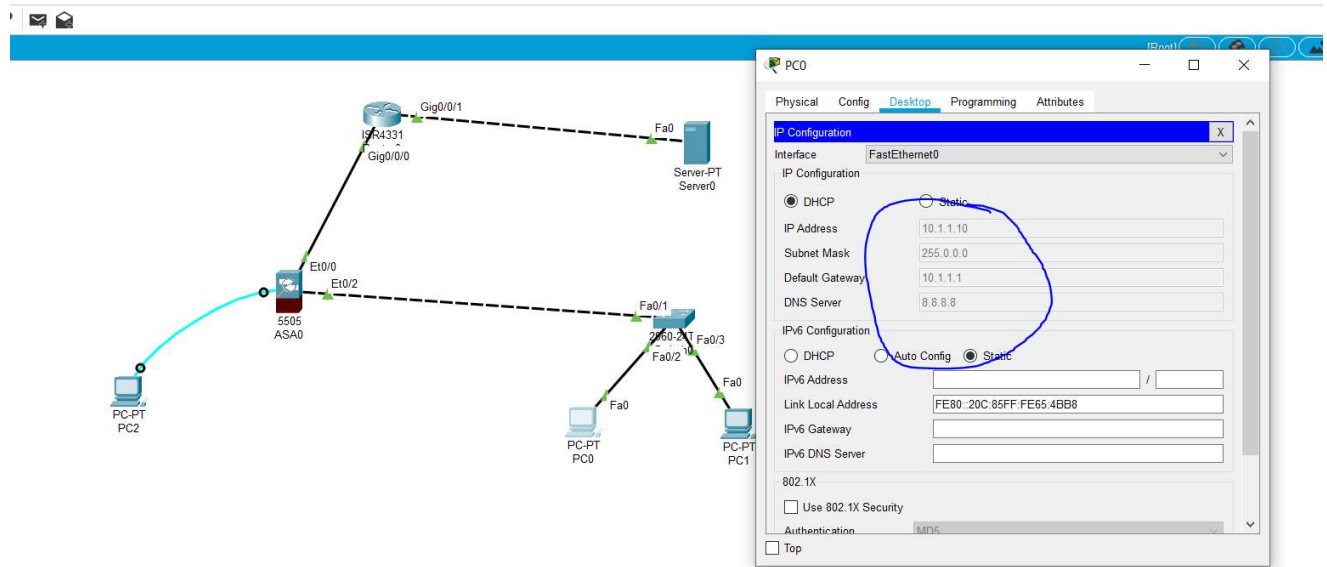
Step 6- Setting the IP Address on the Server



Step 6- Setting DHCPD range for Firewall via the PC-2 and the DNS IP



Step 6- Checking the DNS on the PC's:



Step 7- Configuring Default Route on ASA

```
% Invalid input detected at marker.  
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 50.1.1.1  
ciscoasa(config)#
```

☐ Top

Step 8- Setting up OSPF on the Router

```
Router>enable  
Router#  
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#interface GigabitEthernet0/0/0  
Router(config-if)#  
Router(config-if)#exit  
Router(config)#interface GigabitEthernet0/0/1  
Router(config-if)#exit  
Router(config)#router ospf ?  
  <1-65535> Process ID  
Router(config)#router ospf  
% Incomplete command.  
Router(config)#router ospf ?  
  <1-65535> Process ID  
Router(config)#router ospf 1  
Router(config-router)#net 50.0.0.0 ?  
  A.B.C.D OSPF wild card bits  
Router(config-router)#net 50.0.0.0 0.255.255.255 area 0  
Router(config-router)#net 8.0.0.0 0.255.255.255 area 0  
Router(config-router)#
```

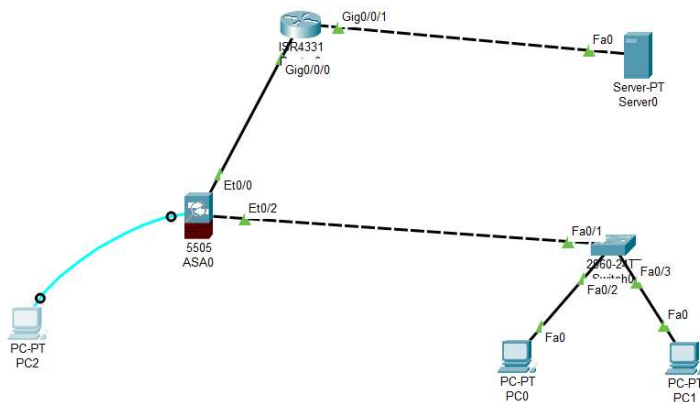
Ctrl+F6 to exit CLI focus

Copy

Paste

☐ Top

Step 9- Creating an object network



```
PC2
Physical Config Desktop Programming Attributes
Terminal
Type help or '?' for a list of available commands.
ciscoasa>object network ?
% Unrecognized command
ciscoasa>object network object network LAN
% Invalid input detected at '^' marker.
ciscoasa>conf t
^
% Invalid input detected at '^' marker.
ciscoasa>en
Password:
ciscoasa#conf t
ciscoasa(config)#object network ?
% Unrecognized command
ciscoasa(config)#object network ?
configure mode commands/options:
WORD Specifies object ID (1-64 characters)
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 10.0.0.0 255.0.0.0
ciscoasa(config-network-object)#
```

Step 10- Enable NAT on ASA

```
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 10.0.0.0 255.0.0.0
ciscoasa(config-network-object)#nat ?

network-object mode commands/options:
( Open parenthesis for (<internal_if_name>,<external_if_name>)
pair
ciscoasa(config-network-object)#nat (inside, Outside) dynamic
interface
ciscoasa(config-network-object)#
```

☐ Top

