CSE 3502

INFORMATION SECURITY MANAGEMENT

Lab Assessment – 1

L19+L20 | SJT516
Dr. Lavanya K

WINTER SEMESTER 2021-22

by

SHARADINDU ADHIKARI

19BCE2105

Exp 1: Firewall Configuration

PART 1: Introduction to Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

- A network firewall is a system or a group of systems used to control access between two networks - a trusted network and an untrusted network — using pre-configured rules or filters.

- It is basically a device that provides secure connectivity between networks. A Firewall can be hardware based or software based.

- It is primarily used to implement and enforce one or more security policies for communication between networks.

- A Firewall can be constructed using single or multiple routers, and can be bootstrapped on both single host and multiple host systems to safeguard against intrusion attempts.

- There are two commonly used types of firewall policies:
  - Whitelisting — The firewall denies all connections except for those specifically listed as acceptable.
  - Blacklisting — The firewall allows all connections except those specifically listed as unacceptable.

- Different types of firewall include:
  - Packet-filtering firewall: A packet-filtering firewall is a primary and simple type of network security firewall. It has filters that compare incoming and outgoing packets against a standard set of rules to decide whether to allow them to pass through.
  - Stateful packet-filtering firewall: Stateful inspection techniques employ a dynamic memory that stores the state tables of the incoming and established connections. Any time an external host requests a connection to your internal host, the connection parameters are written to the state tables.
  - Proxy firewall: Proxy firewalls aim for the Application layer in the OSI model for their operations.
  - Web application firewall (WAF): Web application firewalls are built to provide web applications security by applying a set of rules to an HTTP conversation.

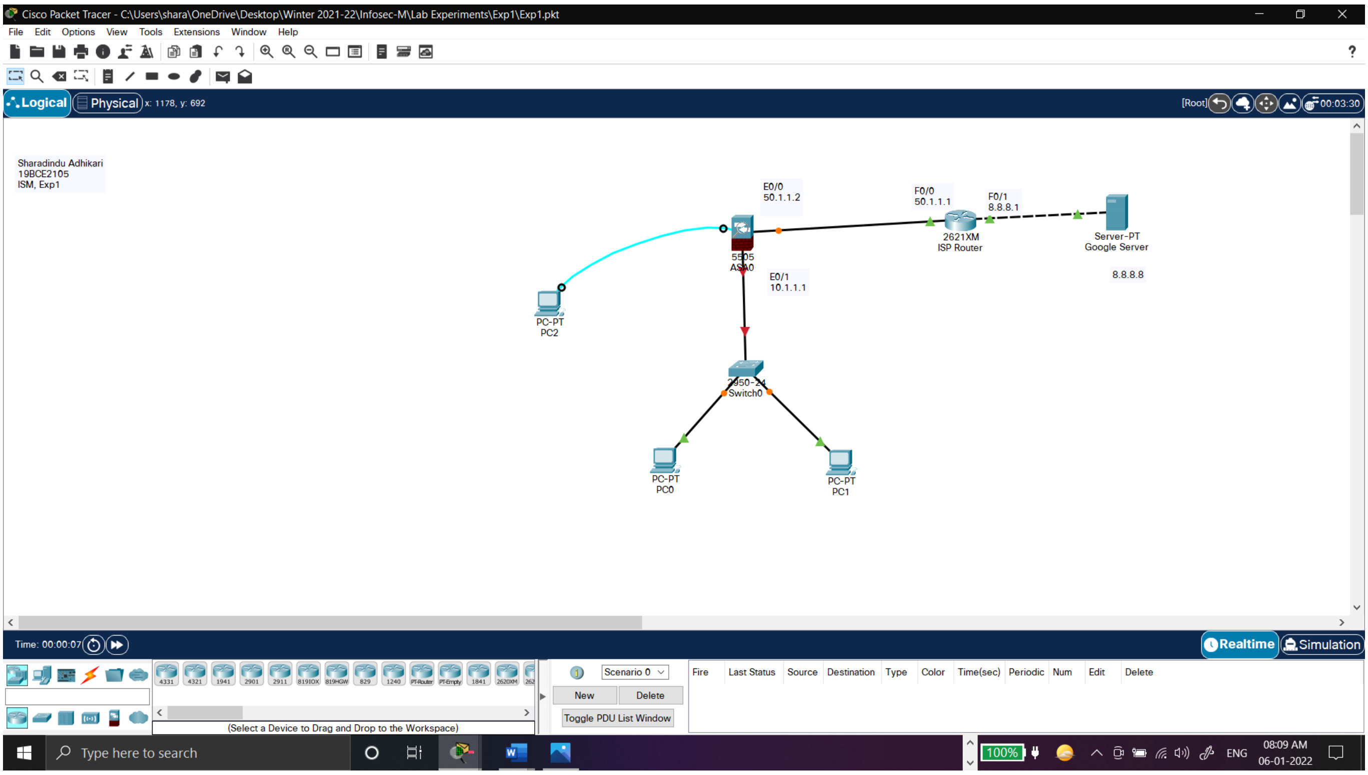
PART 2: Components in Network Firewall Configuration

Component	IP Address
PC-PT	
PC0	10.1.1.12
PC1	10.1.1.11
ASA Firewall	
Ethernet Port 0/0	50.1.1.2
Ethernet Port 0/1	10.1.1.1
Router	
Fast Ethernet 0/0	50.1.1.1
Fast Ethernet 0/1	8.8.8.1
Google Server	
Fast Ethernet 0/0	8.8.8.8

Firewall:	The Cisco ASA 5505 Firewall
Switch:	WS-C2950-24 switch, 24 port, 10/100 auto-sensing and auto-negotiating
PC0, PC1:	PCs connected to switch functioning as local computers protected by firewall
PC2:	PC connected to firewall to configure it using command line
Router:	Cisco 2621XM Multiservice Router
Server:	A Domain Name System (DNS) server resolves host names into IP addresses

PART 3: Firewall Configuration

Step 1: Make topology



Step 2: Configure ASA IP

2.1. enabling firewall

`ciscoasa>en`

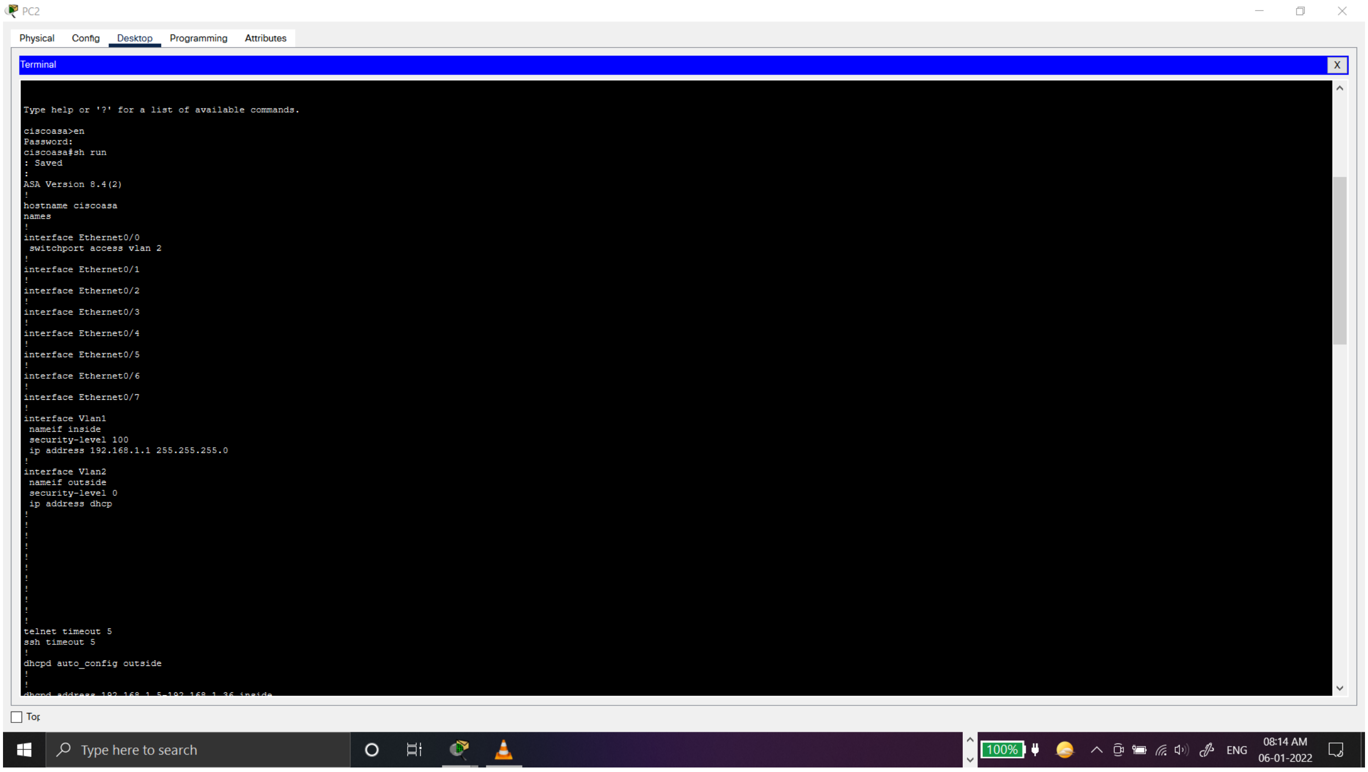
2.2. checking default configuration of ASA firewall

`ciscoasa#sh running-config`

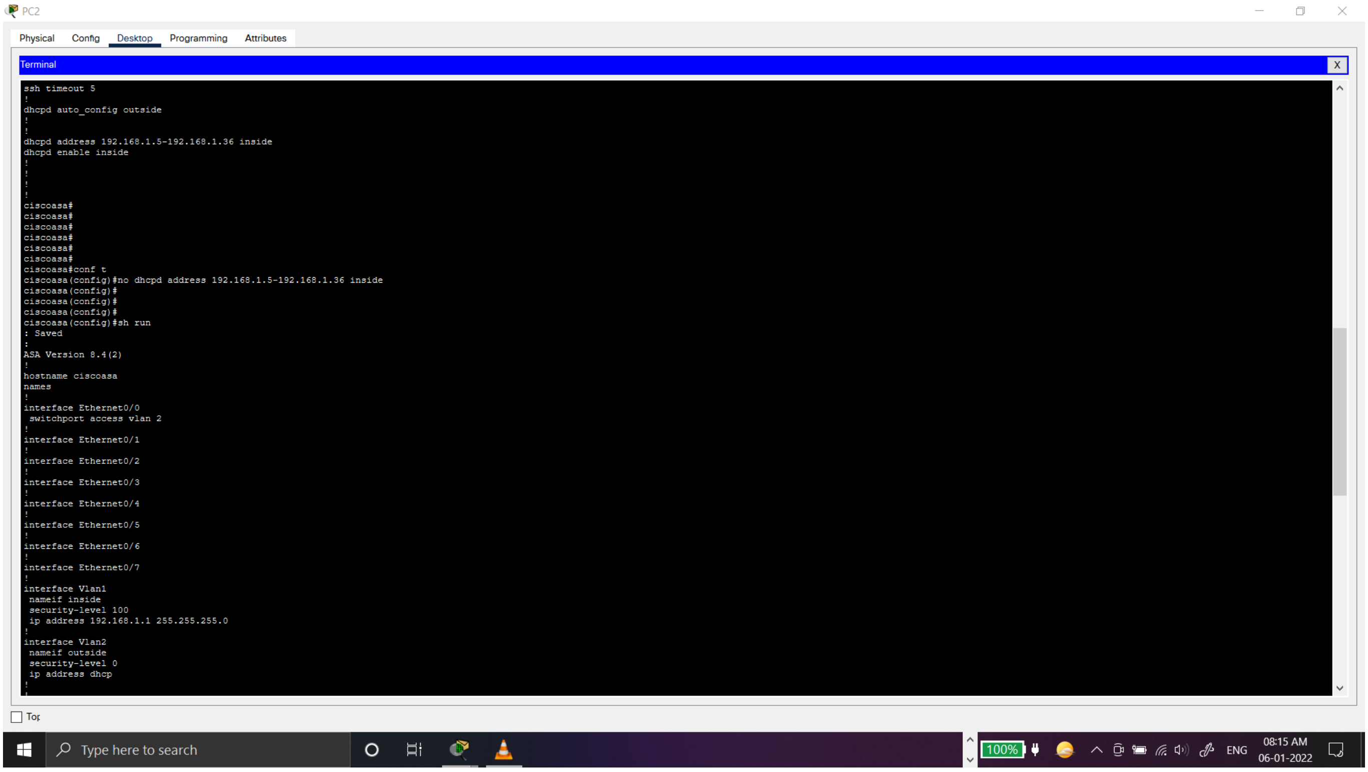
No configuration found for ethernet interfaces
Some pre-configurations related to VLAN interfaces found
Also, by default, DHCPD server is enabled and configured on the ASA
Now, we need to remove these default settings

2.3. removing default configurations on ASA and reconfiguring ASA

- Entering global configuration mode
  `ciscoasa#conf t`
- Removing DHCP configurations
  `ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.36 inside`
- Reconfiguring VLAN 1 IP address and operation modes
  `ciscoasa(config)#int vlan 1` (entering VLAN 1 configuration mode)
  `ciscoasa(config-if)#ip add 10.1.1.1 255.0.0.0` (changing IP address)
  `ciscoasa(config-if)#no shut` (enabling no shut down mode)
  `ciscoasa(config-if)#nameif inside` (set VLAN 1 as inside interface (interface that connects to local network))
  `ciscoasa(config-if)#security-level 100` (setting security as lowest on interface VLAN 1)
  `ciscoasa(config-if)#exit` (exiting VLAN 1 configuration mode)
  `ciscoasa(config)#`
  `ciscoasa(config)#int e0/1` (entering configuration for ethernet-port 0/1)
  `ciscoasa(config-if)#switchport access vlan 1` (setting port as VLAN 1)



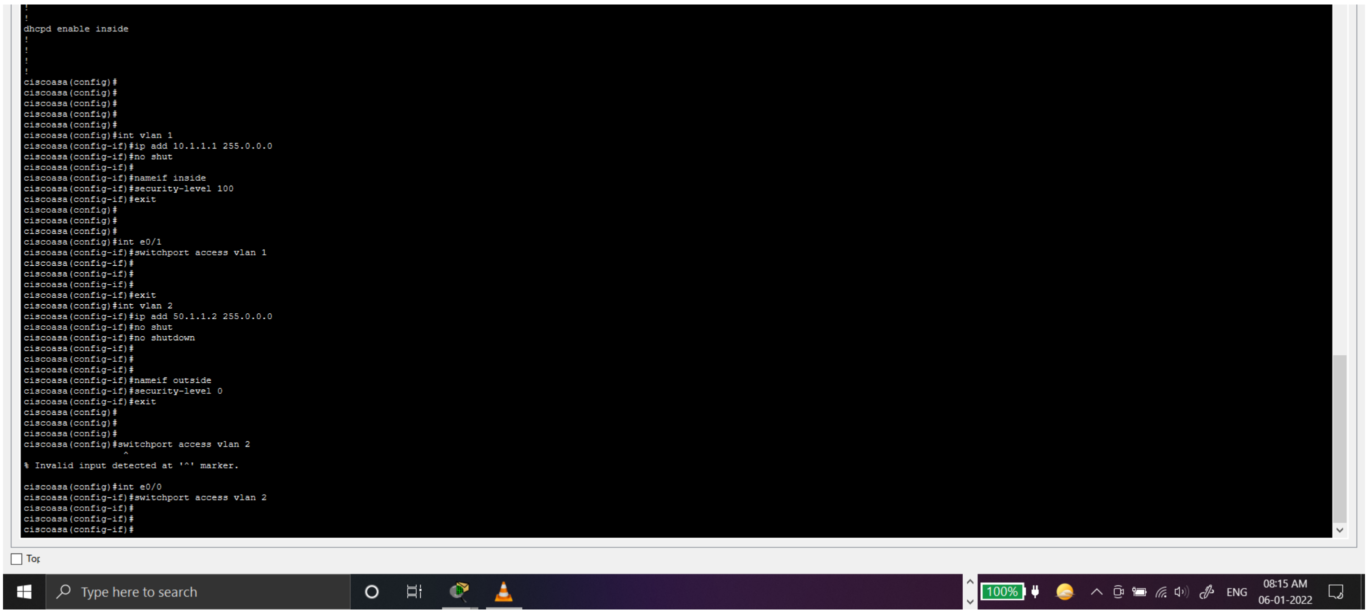
```
Type help or '?' for a list of available commands.

ciscoasa>en
Password:
ciscoasa#sh run
: 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 dhcp
!
!
!
!
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
!
dhcpd address 192.168.1.5-192.168.1.36 inside
```



```
ssh timeout 5
!
dhcpd auto_config outside
!
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
!
!
!
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#conf t
ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.36 inside
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#sh run
: 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 dhcp
!
```

- Reconfiguring VLAN 2 IP address and operation modes and following same steps as VLAN 1

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



```
!
!
dhcpd enable inside
!
!
!
!
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
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)#
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#int e0/1
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#exit
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)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#switchport access vlan 2
                  ^
% Invalid input detected at '^' marker.

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

Step 3: Configure Router and Server IPs

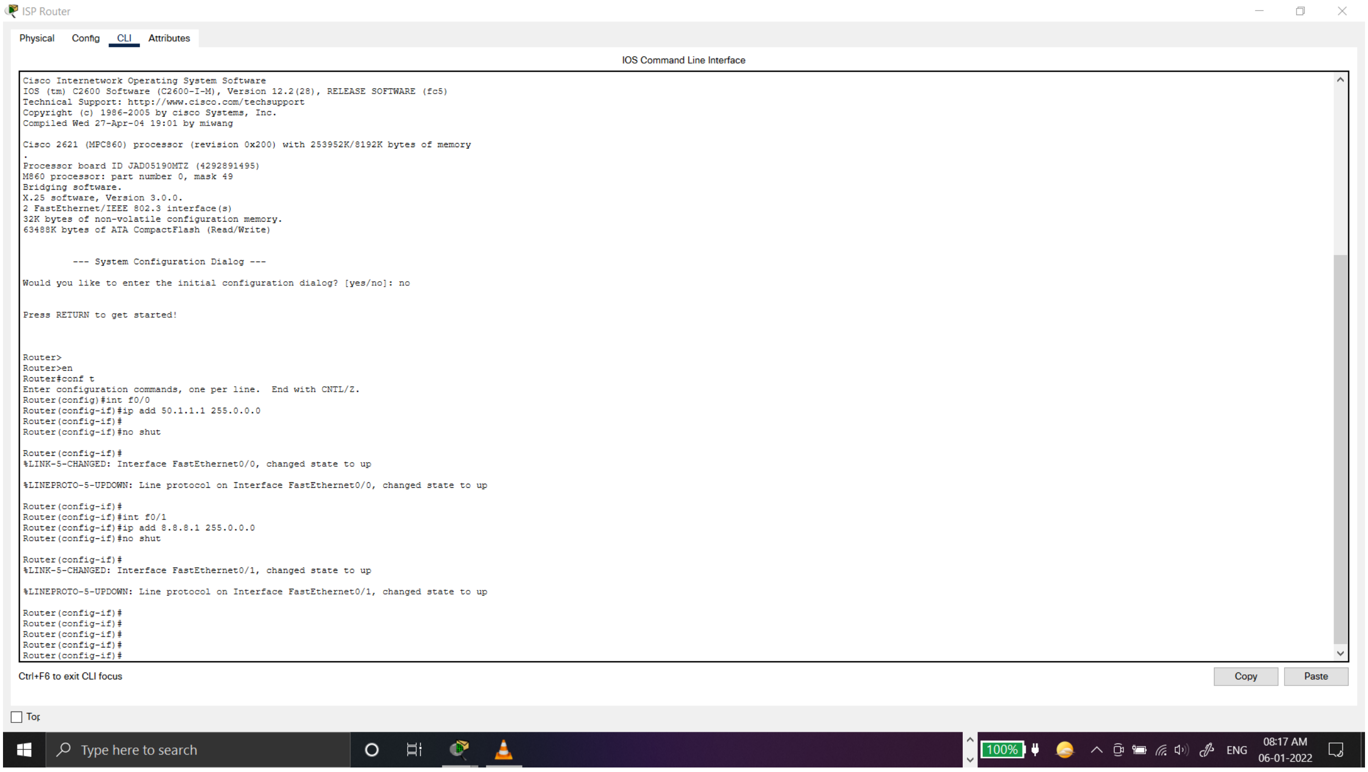
3.1. Configuring Router IP

3.1.1. Enabling router

```
Router>en
Router#
Router#conf t
```

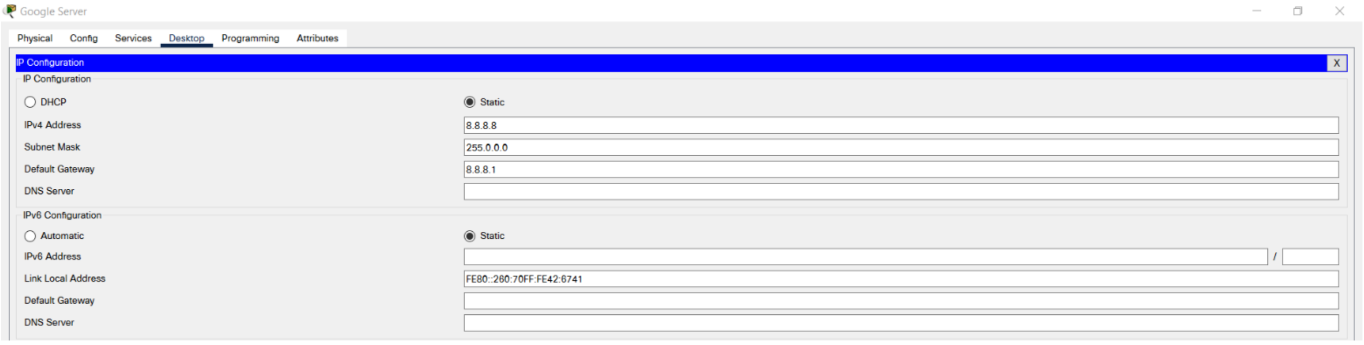
3.1.2. Configuring Fast Ethernet ports

```
Router(config)#int f0/0
Router(config-if)#ip add 50.1.1.1 255.0.0.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#int f0/1
Router(config-if)#ip add 8.8.8.1 255.0.0.0
Router(config-if)#no shut
```



```
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

Cisco 2621 (MPC860) processor (revision 0x200) with 253952K/8192K bytes of memory
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#ip add 50.1.1.1 255.0.0.0
Router(config-if)#
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#
Router(config-if)#int f0/1
Router(config-if)#ip add 8.8.8.1 255.0.0.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
```

3.2. Configuring Google Server IP



IP Configuration

○ DHCP ● Static

IPv4 Address: 8.8.8.8

Subnet Mask: 255.0.0.0

Default Gateway: 8.8.8.1

DNS Server:

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::260:70FF:FE42:6741

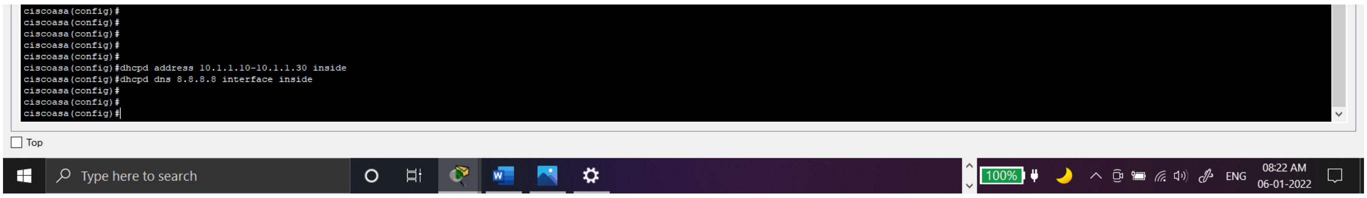
Default Gateway:

DNS Server:

Step 4: Configure DHCP Server and DNS IP on ASA

We're configuring DHCP and DNS so that local computers connected to the (local) network automatically get the IP address.

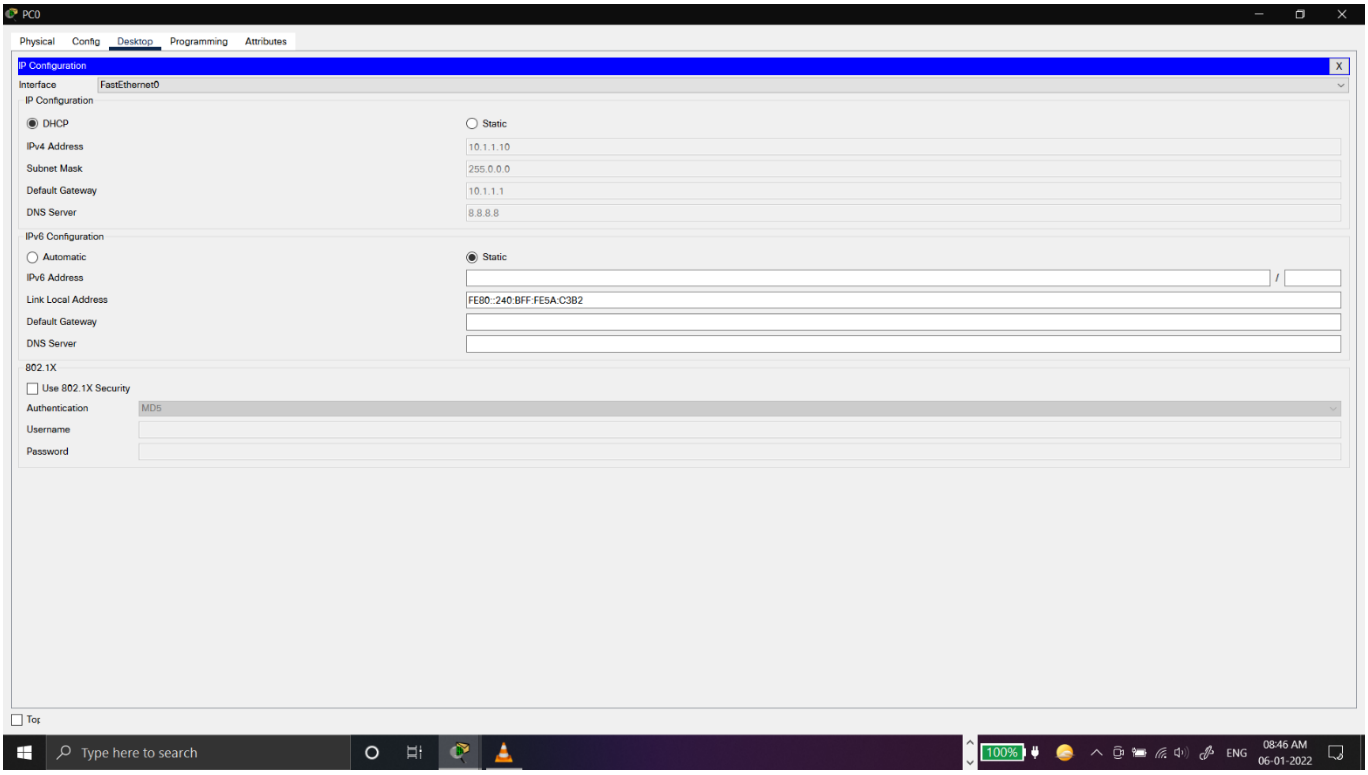
`ciscoasa(config)#dhcpd address 10.1.1.10-10.1.1.30 inside` (to provide range of IP addresses to the computers on local network interfaced with firewall)
`ciscoasa(config)#dhcpd dns 8.8.8.8 interface inside` (to provide IP configuration of DNS server)



```
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#dhcpd address 10.1.1.10-10.1.1.30 inside
ciscoasa(config)#dhcpd dns 8.8.8.8 interface inside
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
```

Step 5:

5.1. Testing automatic IP receiving using DHCP pf local computers.



PC0

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 10.1.1.10

Subnet Mask: 255.0.0.0

Default Gateway: 10.1.1.1

DNS Server: 8.8.8.8

IPv6 Configuration

○ Automatic ● Static

IPv6 Address:

Link Local Address: FE80::240:BFF:FE5A:C3B2

Default Gateway:

DNS Server:

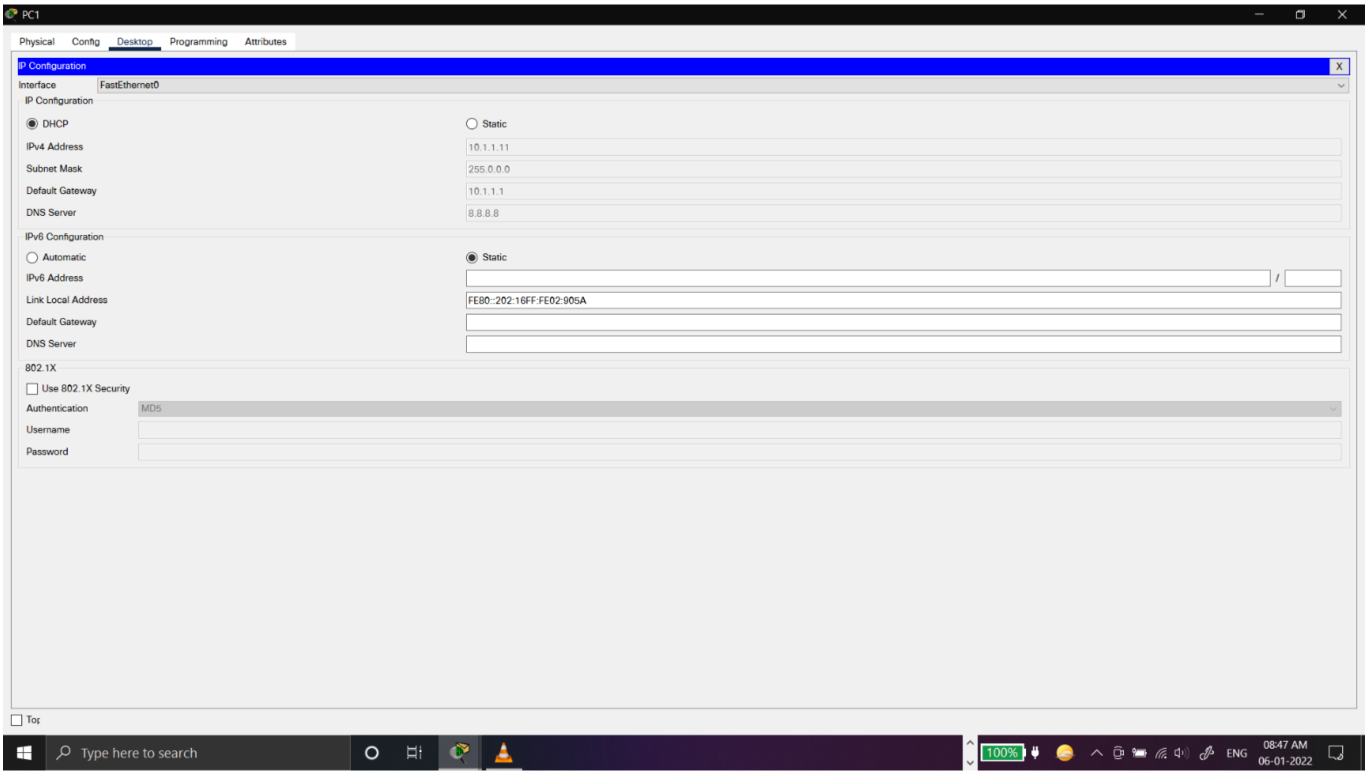
802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 10.1.1.11

Subnet Mask: 255.0.0.0

Default Gateway: 10.1.1.1

DNS Server: 8.8.8.8

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::202:16FF:FE02:905A

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

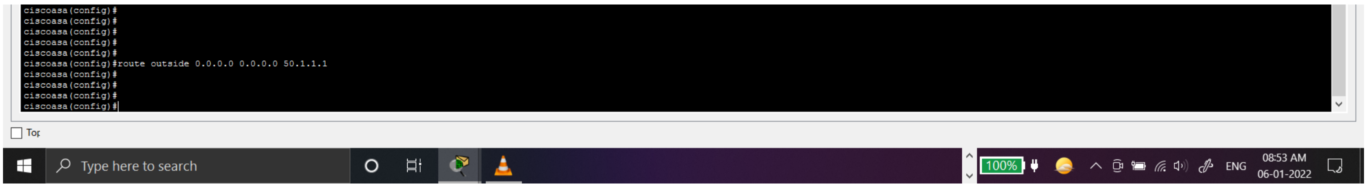
Authentication: MD5

Username:

Password:

5.2. Configuring Default Route on ASA:
ASA firewall has only one route to reach all the other networks, which is why we configure the default routing.

`ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 50.1.1.1` (any IP address with any subnet mask should be directed to 50.1.1.1 because that's the IP of router)



```
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 50.1.1.1
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
```

<u>Step 6:</u> Configure OSPF on ISP Router

Configuring OSPF dynamic routing protocol on Router

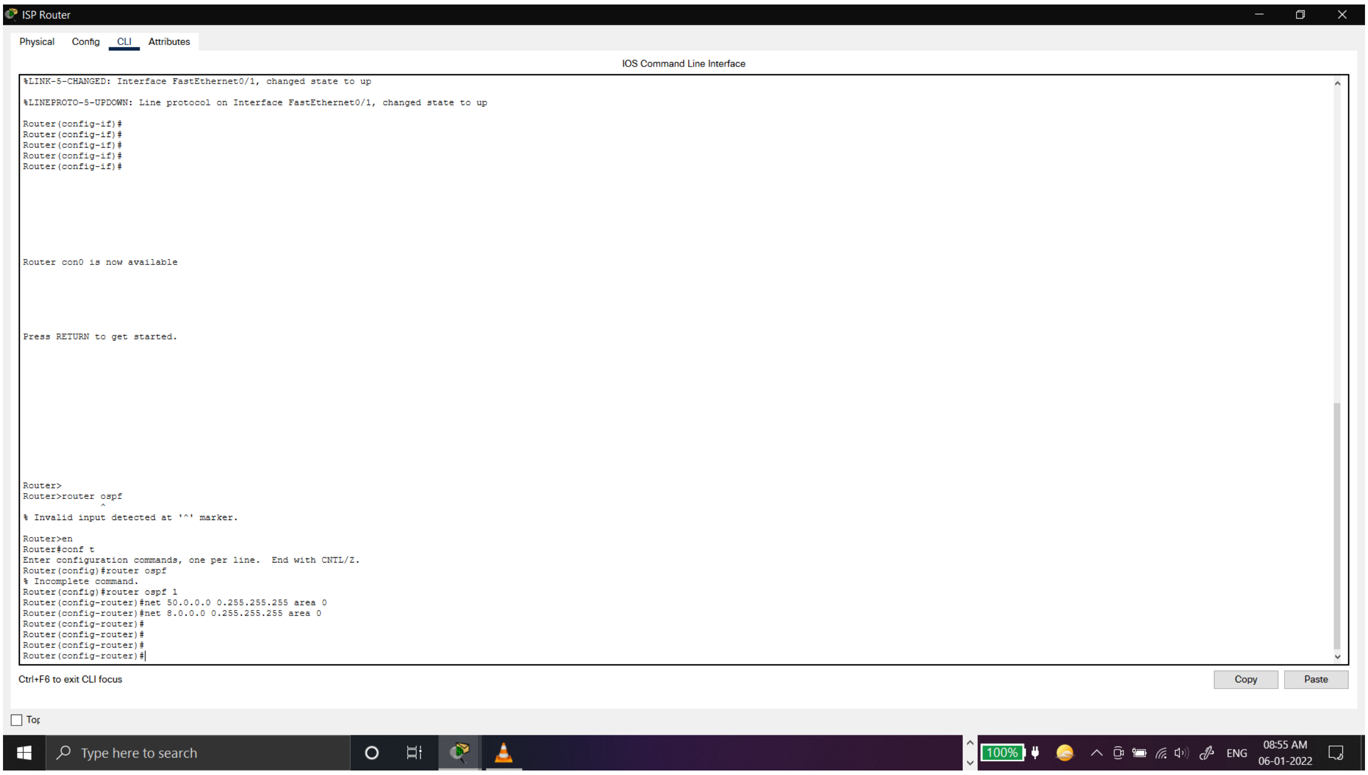
```
Router>en
Router#conf t
```

`Router(config)#router ospf ?` (to get process IDs)

`Router(config)#router ospf 1` (to enter ospf protocol process)

`Router(config-router)#net 50.0.0.0 0.255.255.255 area 0` (configuring networks (2 networks connected to router) connected to ISP router)

`Router(config-router)#net 8.0.0.0 0.255.255.255 area 0` (same as above)



```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#






Router con0 is now available





Press RETURN to get started.










Router>
Router>router ospf
              ^
% Invalid input detected at '^' marker.

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf
% Incomplete command.
Router(config)#router ospf 1
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)#
Router(config-router)#
Router(config-router)#
Router(config-router)#
```

Step 7: Create Object Network & Enable NAT on ASA

7.1. Creating object network

`ciscoasa(config)#object network ?` (to check command required)

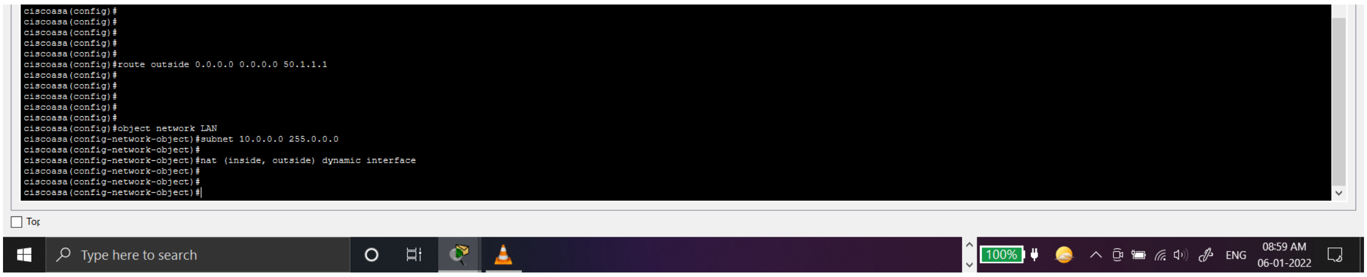
`ciscoasa(config)#object network LAN` (creating object network with LAN ID)

Specifying subnet

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

7.2. Configuring the NAT

`ciscoasa(config-network-object)#nat (inside, outside) dynamic interface` (configuring NAT between inside and outside interface with a dynamic condition)



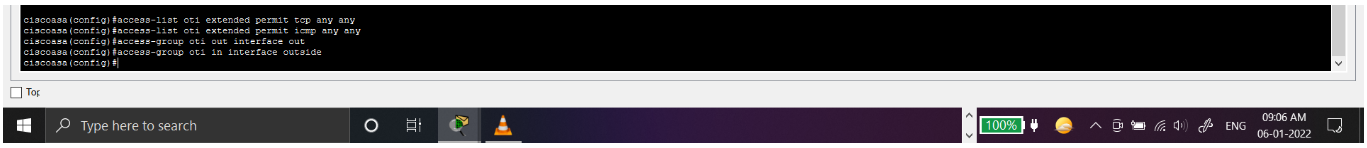
```
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 50.1.1.1
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 10.0.0.0 255.0.0.0
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#nat (inside, outside) dynamic interface
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#
```

Step 8: Create ACL on ASA

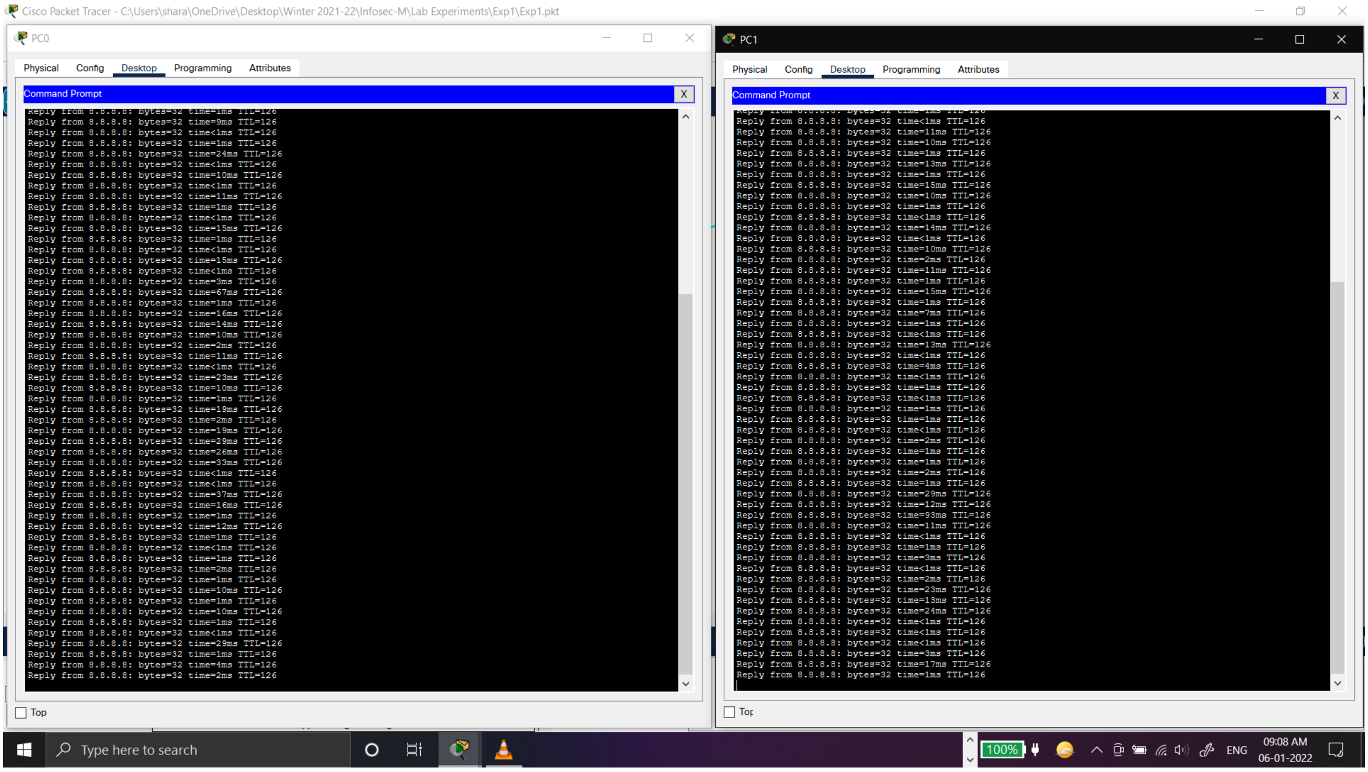
Configuring ACL

```
ciscoasa#conf t
```

`ciscoasa(config)#access-list ism extended permit tcp any any` (naming our access-list ism and configuring it in extended mode permitting tcp from “any” source to “any” destination)
`ciscoasa(config)#access-list ism extended permit icmp any any` (naming our access-list ism and configuring it in extended mode permitting icmp from “any” source to “any” destination)
`ciscoasa(config)#access-group ism in interface outside` (configuring access-list group ism, interfacing it from inside to outside)



```
ciscoasa(config)#access-list oti extended permit tcp any any
ciscoasa(config)#access-list oti extended permit icmp any any
ciscoasa(config)#access-group oti out interface out
ciscoasa(config)#access-group oti in interface outside
ciscoasa(config)#
```



Cisco Packet Tracer - C:\Users\shara\OneDrive\Desktop\Winter 2021-22\Infosec-M\Lab Experiments\Exp1\Exp1.pkt
PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X

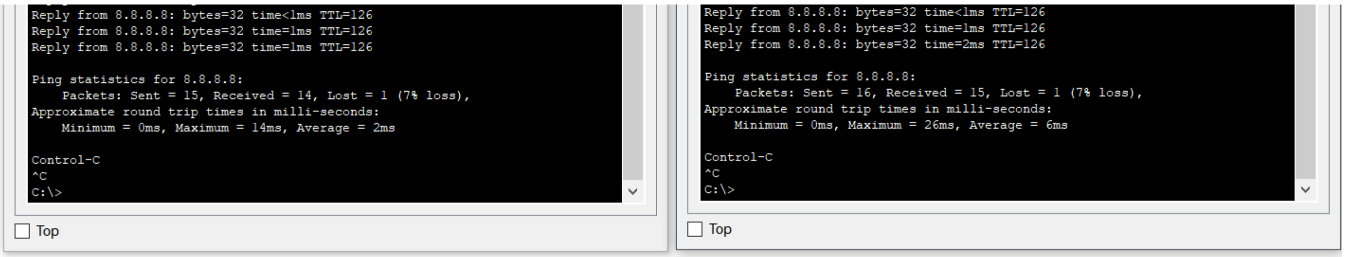
```
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=9ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=24ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=11ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=15ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=15ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=3ms TTL=126
Reply from 8.8.8.8: bytes=32 time=67ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=16ms TTL=126
Reply from 8.8.8.8: bytes=32 time=14ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time=2ms TTL=126
Reply from 8.8.8.8: bytes=32 time=11ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=19ms TTL=126
Reply from 8.8.8.8: bytes=32 time=2ms TTL=126
Reply from 8.8.8.8: bytes=32 time=19ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=33ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=37ms TTL=126
Reply from 8.8.8.8: bytes=32 time=16ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=12ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=2ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=4ms TTL=126
Reply from 8.8.8.8: bytes=32 time=2ms TTL=126
```

```
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=11ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=13ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=15ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=14ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=10ms TTL=126
Reply from 8.8.8.8: bytes=32 time=2ms TTL=126
Reply from 8.8.8.8: bytes=32 time=11ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=15ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=7ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=13ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=4ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=2ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=2ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=12ms TTL=126
Reply from 8.8.8.8: bytes=32 time=93ms TTL=126
Reply from 8.8.8.8: bytes=32 time=11ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=3ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=2ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=13ms TTL=126
Reply from 8.8.8.8: bytes=32 time=24ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=3ms TTL=126
Reply from 8.8.8.8: bytes=32 time=17ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
```

Step 9: Verify

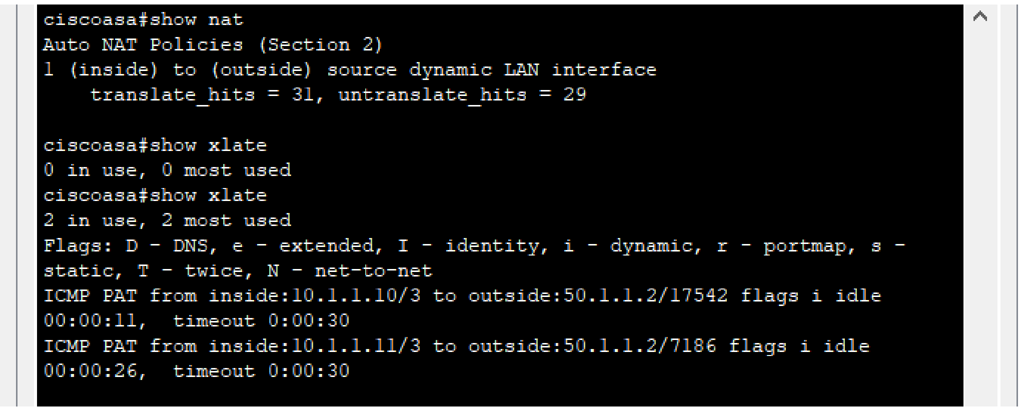
Verifying NAT and XLATE on firewall

`ciscoasa#show nat` (display NAT status)
`ciscoasa#show xlate` (display xlate status)



```
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 15, Received = 14, Lost = 1 (7% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 2ms

Control-C
^C
C:\>
```

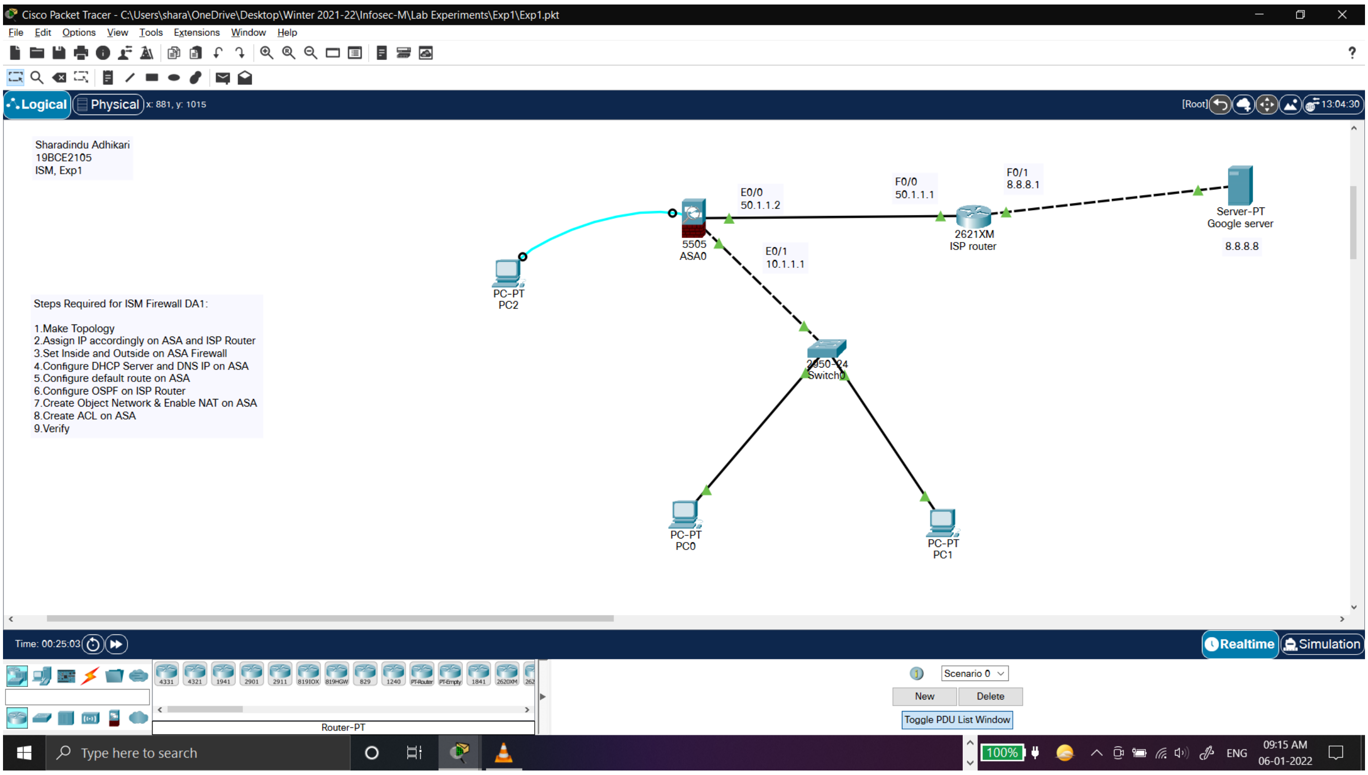
```
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=2ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 16, Received = 15, Lost = 1 (7% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 26ms, Average = 6ms

Control-C
^C
C:\>
```



```
ciscoasa#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic LAN interface
    translate_hits = 31, untranslate_hits = 29

ciscoasa#show xlate
0 in use, 0 most used
ciscoasa#show xlate
2 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s -
static, T - twice, N - net-to-net
ICMP PAT from inside:10.1.1.10/3 to outside:50.1.1.2/17542 flags i idle
00:00:11,  timeout 0:00:30
ICMP PAT from inside:10.1.1.11/3 to outside:50.1.1.2/7186 flags i idle
00:00:26,  timeout 0:00:30
```

Hence firewall is working.

Final Topology:

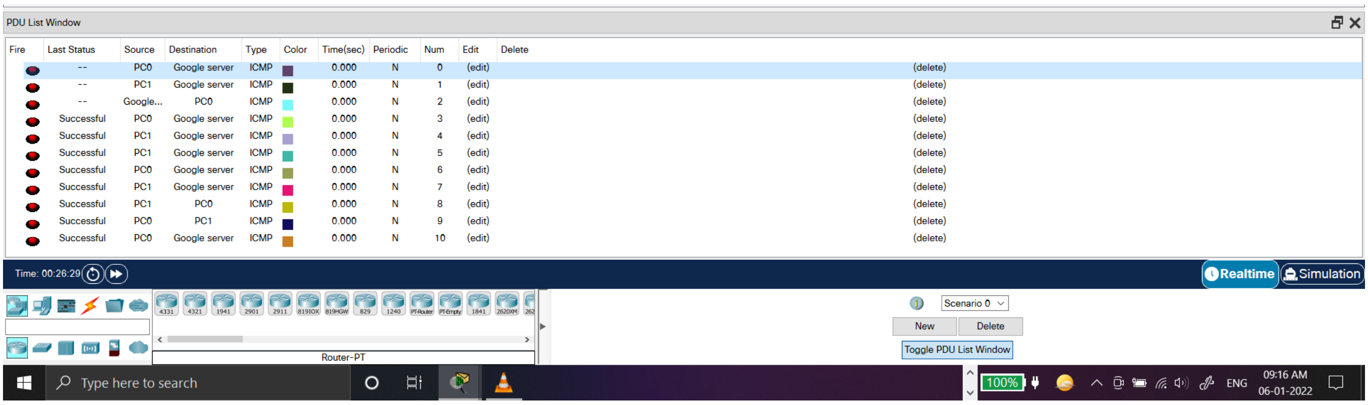


Sharadindu Adhikari
19BCE2105
ISM, Exp1

Steps Required for ISM Firewall DA1:

1.Make Topology
2.Assign IP accordingly on ASA and ISP Router
3.Set Inside and Outside on ASA Firewall
4.Configure DHCP Server and DNS IP on ASA
5.Configure default route on ASA
6.Configure OSPF on ISP Router
7.Create Object Network & Enable NAT on ASA
8.Create ACL on ASA
9.Verify

PDUs:



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
🔴	--	PC0	Google server	ICMP	🟪	0.000	N	0	(edit)	(delete)
🔴	--	PC1	Google server	ICMP	⬛	0.000	N	1	(edit)	(delete)
🔴	--	Google...	PC0	ICMP	🟦	0.000	N	2	(edit)	(delete)
🔴	Successful	PC0	Google server	ICMP	🟩	0.000	N	3	(edit)	(delete)
🔴	Successful	PC1	Google server	ICMP	🟪	0.000	N	4	(edit)	(delete)
🔴	Successful	PC1	Google server	ICMP	🟩	0.000	N	5	(edit)	(delete)
🔴	Successful	PC0	Google server	ICMP	🟫	0.000	N	6	(edit)	(delete)
🔴	Successful	PC1	Google server	ICMP	🟥	0.000	N	7	(edit)	(delete)
🔴	Successful	PC1	PC0	ICMP	🟨	0.000	N	8	(edit)	(delete)
🔴	Successful	PC0	PC1	ICMP	🟦	0.000	N	9	(edit)	(delete)
🔴	Successful	PC0	Google server	ICMP	🟧	0.000	N	10	(edit)	(delete)