VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

CSE 3502
Information Security Management
Lab Report – 1
Firewall Configuration

Winter Semester 2022-23

Name:Aditya Krishna

Reg No.:20BCE0456

Guided by: Prof. Lavanya K

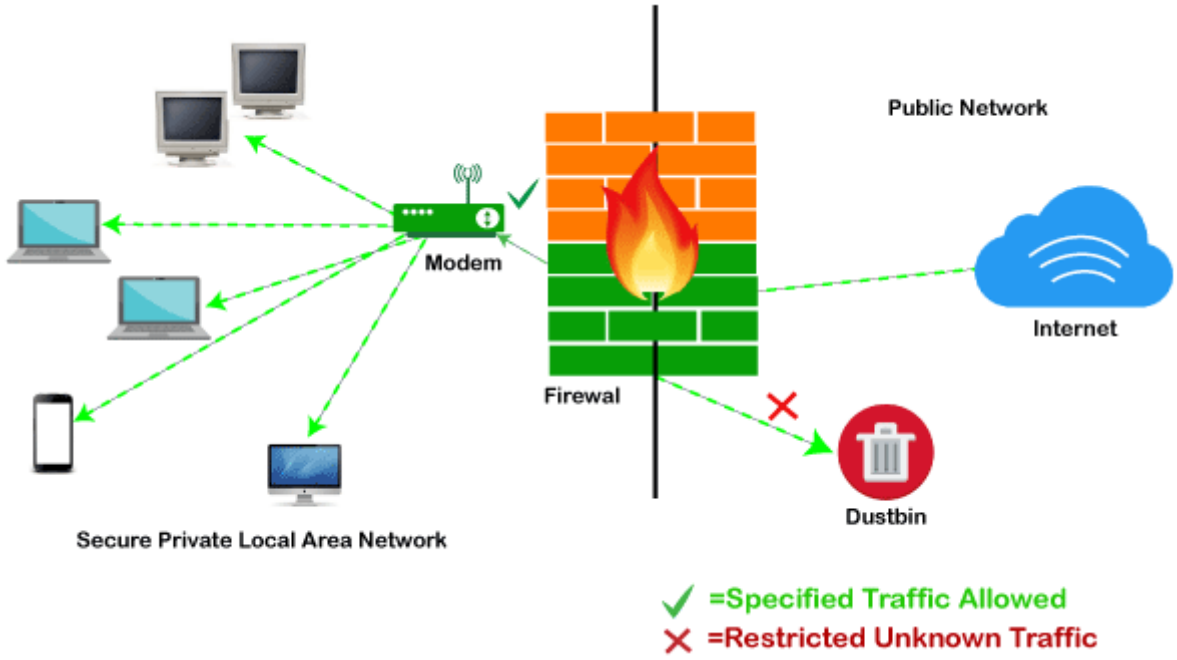
22nd Dec, 2022

Introduction to Firewall

A firewall is a type of network security system that keeps an eye on and regulates incoming and outgoing network traffic in accordance with pre-established security rules. Typically, a firewall creates a wall between a trustworthy network and an unreliable network, like the Internet.
The firewall may fully block some traffic or all traffic, perform verification on some or all of the traffic, or any combination of these depending on the organization's firewall policy. There are two types of firewall policies that are frequently used:

Whitelisting – The firewall only allows connections that are explicitly identified as acceptable, rejecting all other connections.

Blacklisting - The firewall accepts all connections with the exception of those that are expressly identified as unsuitable (blacklisting).



Firewalls can be standalone systems or they can be included in other infrastructure devices, such as routers or servers.

Type of Firewall	***Parameters / Purpose***	***Layer of Working***	***Protocols***	***Attacks***
Packet-filtering firewall	Source & Destination IP Addresses Source & Destination Port Numbers Protocols	Layer 3 of OSI Model	ICMP ARP RARP BOOTP DHCP	DoS attacks

Stateful firewall	Source & Destination IP Addresses Source & Destination Port Numbers It has state table, dynamic memory.	Layer 4 of OSI Model	UDP ICMP	DDoS and Vulnerability attacks
Proxy firewall	Shielding and filtering mechanism between internal and external networks. Used for authentication schemes.	Application layer of OSI Model	DNS FTP HTTP ICMP SMTP	Vulnerability attacks
Web application firewal	Protects Web app by applying set of rules to HTTP conversation	Application layer of OSI Model	HTTP HTTPS	SQL injection attack XSS attack DDoS attacks

Components of Firewall:

1. Perimeter router

It is used to provide a link to the public networking system like the internet, or a distinctive organization. It performs the routing of data packets with the help of an appropriate routing protocol. It also provides the filtering of packets and addresses translations.

2. Firewall

The provision of distinctive levels of security and supervises traffic among each level. Most of the firewalls are present near the router that provides security from external threats, but sometimes the firewall is present in the internal network to protect from internal attacks.

3. Virtual Private Network (VPN)

Its function is to provide a secure connection among two machines or networks. It provides the secure remote access of the network, thereafter connecting two WAN networks on the same platform while not being physically connected.

4. Intrusion Detection System (IDS)

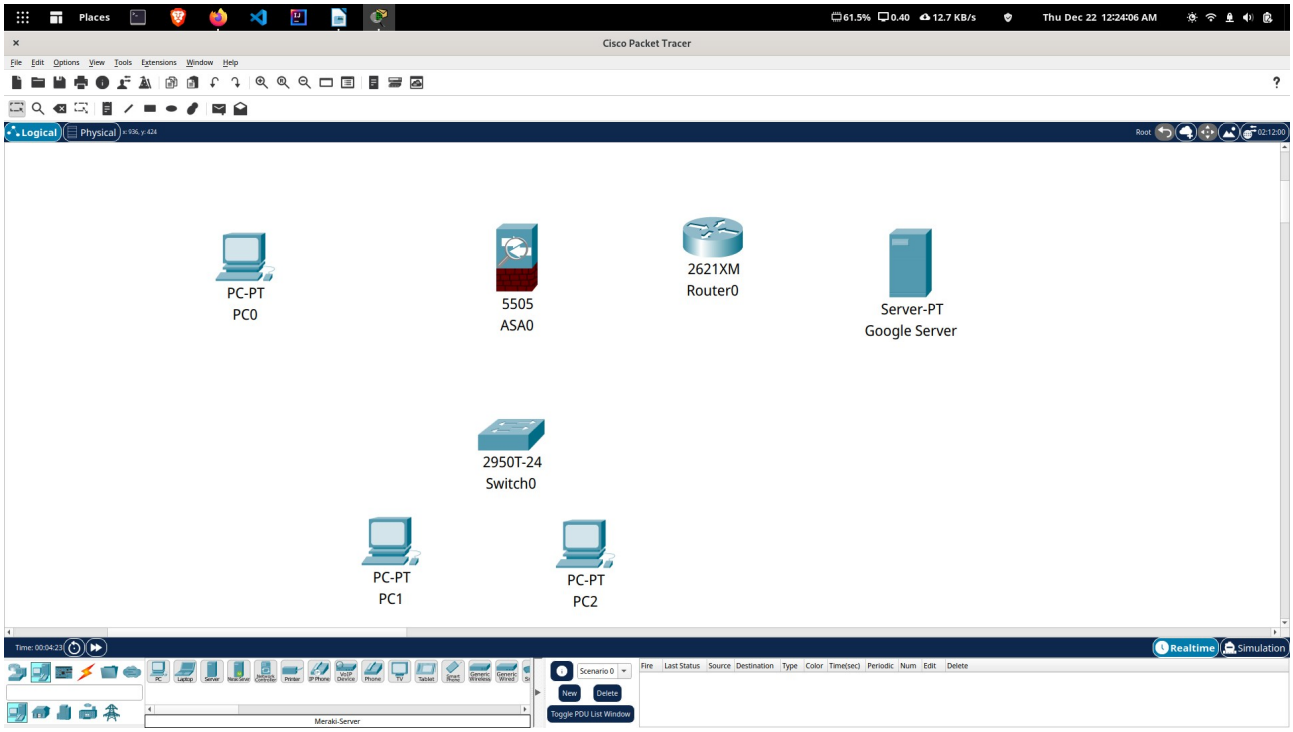
It is used to identify, investigate, and resolve unauthorized attacks. A hacker can attack the network in various ways. It can execute a denial-of-service (DoS) attack or an attack from the backside of the network through some unauthorized access.

Firewall configuration using CISCO packet tracer

Note : For all the demonstrations, timestamp is provided at the top-right of the screen snapshot.

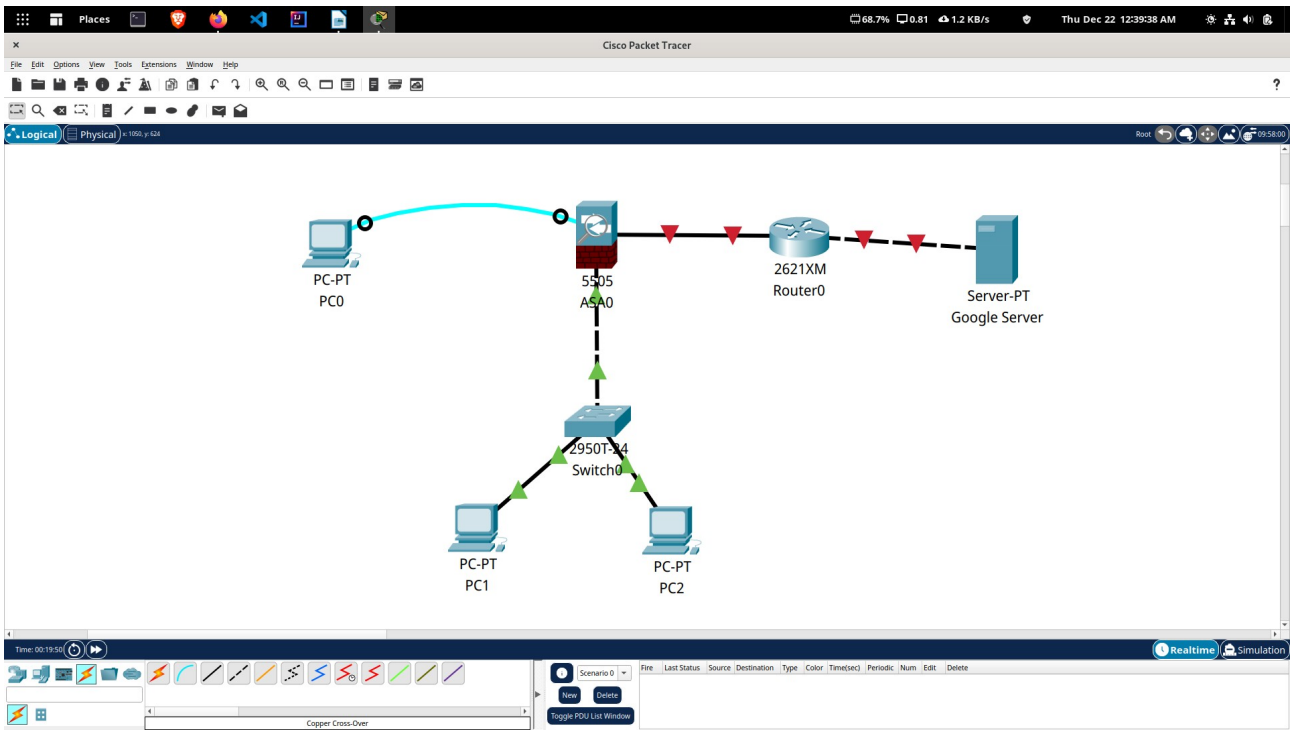
Components:

1. PCs – PC0, PC1 & PC2
2. Switch 2950-24T – Switch0
3. Firewall 5505 – ASA0
4. Router 2621XM – ISP Router
5. Server PT – Google Server



Step 1: Making the topology

Component	**Connected to**	**Via**
PC0 – FA0	Switch0 – FA0/1	Copper Straight-through
PC1 – FA0	Switch0 – FA0/2	Copper Straight-through
Switch0 – FA0/3	ASA0 – Ethernet0/1	Copper Cross-Over
PC2 – RS232	ASA0 - Console	Console
ASA0 – Ethernet0/0	ISP Router – FA0/0	Copper Straight-through
ISP Router – FA0/1	Google Sever – FA0	Copper Cross-Over

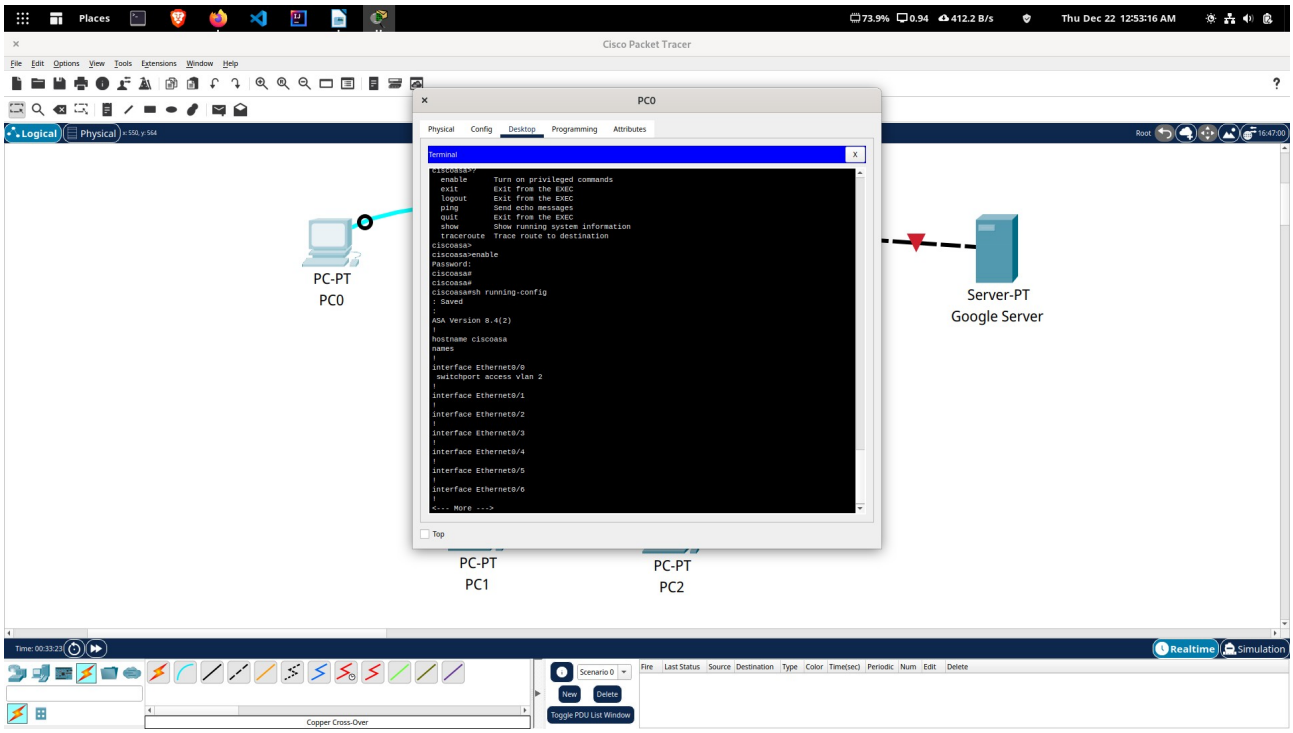


Step 2 : Assigning IP Address to ASA and ISP Router

Device	**Connection**	**IP Address**
ASA0	Ethernet0/0	50.1.1.2
ISP Router	FA0/0	50.1.1.1
ISP Router	FA0/1	8.8.8.1
Google Server	FA0	8.8.8.8
ASA0	Ethernet0/1	10.1.1.1

For this click on PC0 -> Desktop -> Terminal

To enable and check the basic pre-configuration of firewall, use the commands:
en
sh running-config



PC0

Physical Config Desktop Programming Attributes

Terminal

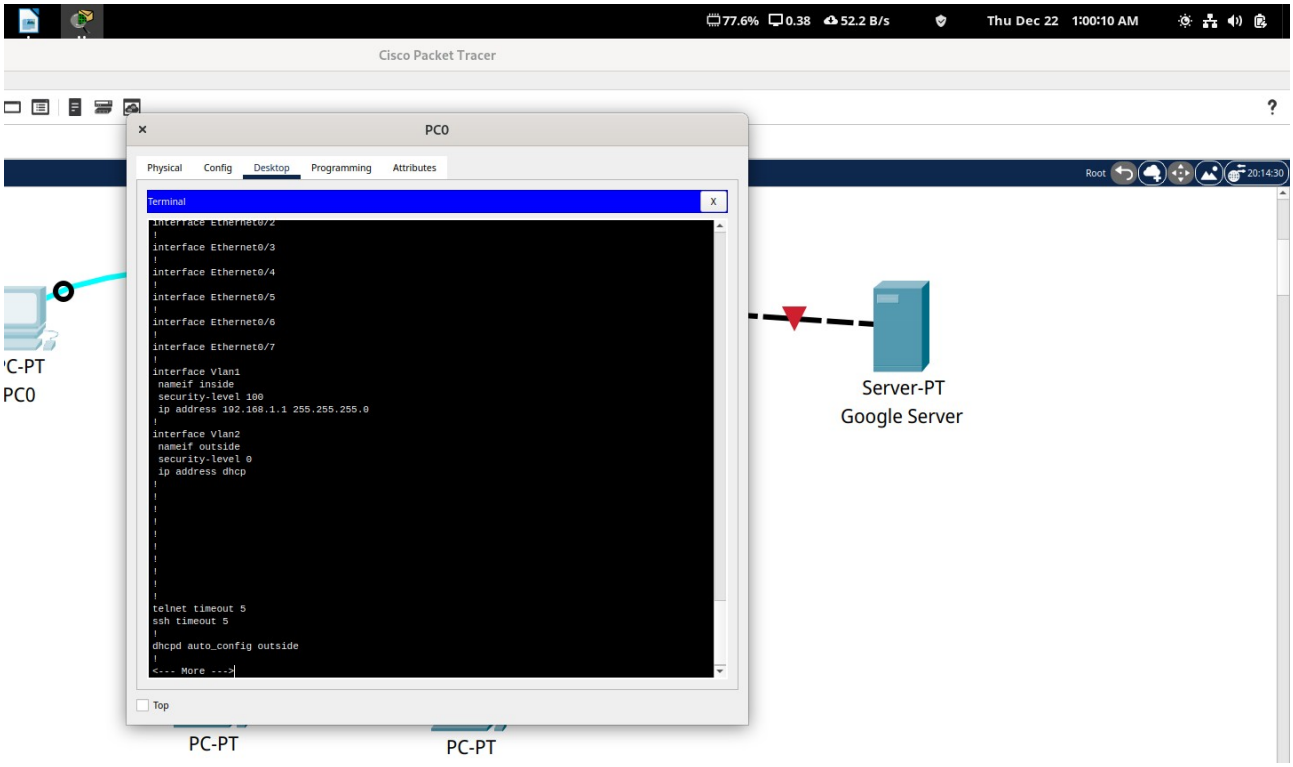
```
Logout
Type help or '?' for a list of available commands.

ciscoasa>?
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  quit        Exit from the EXEC
  show        Show running system information
  traceroute  Trace route to destination
ciscoasa>
ciscoasa>enable
Password:
ciscoasa#
ciscoasa#
ciscoasa#sh running-config
: 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
<--- More --->
```

Remove default configuration settings :

conf t

no dhcpd address 192.168.1.5-192.168.1.36 inside

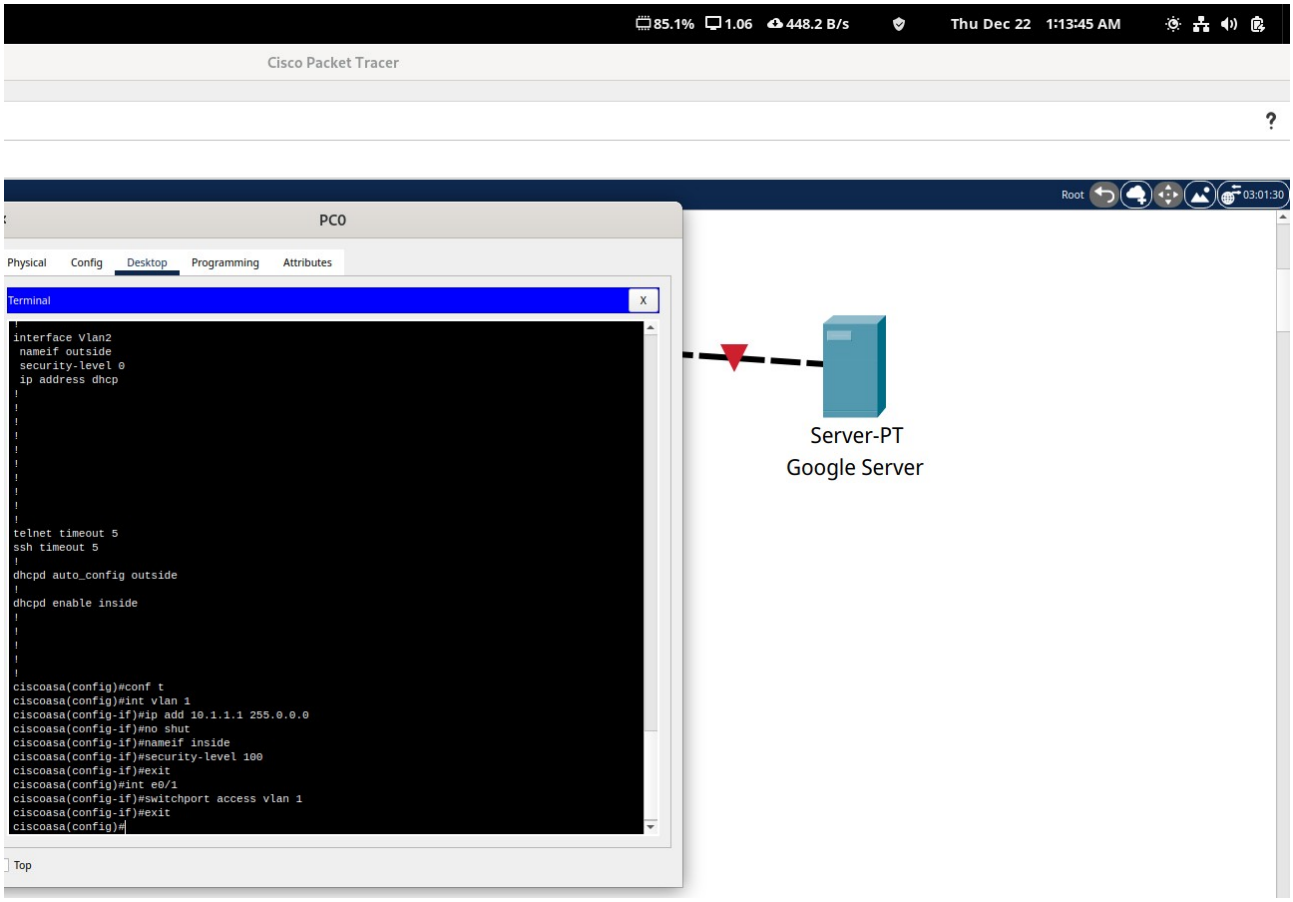
sh running-config



Step 3 : Setting Inside and Outside on ASA Firewall

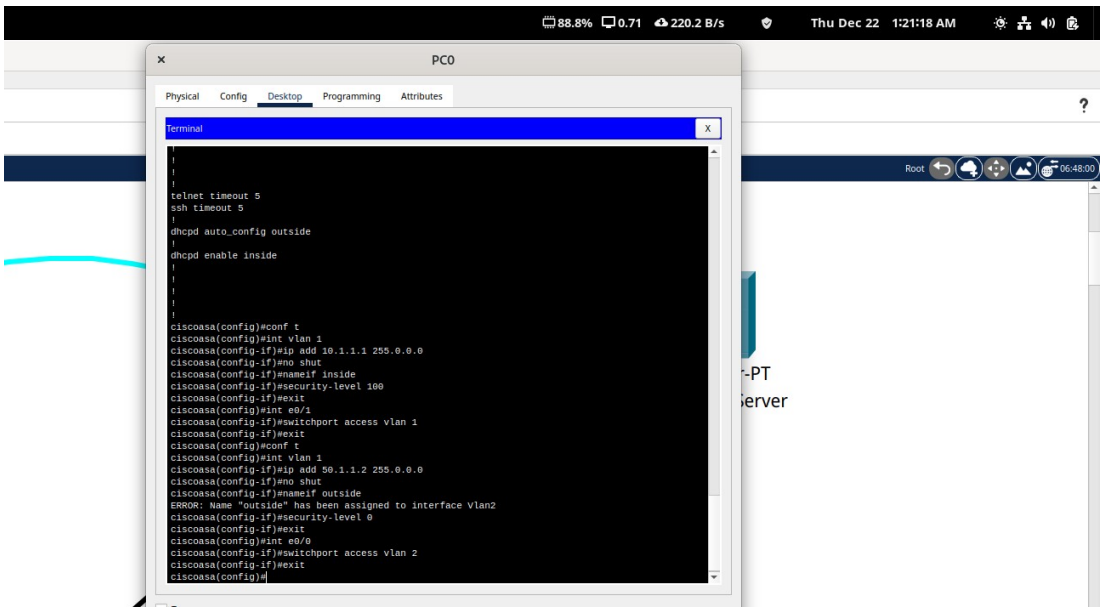
Setting IP Address and Security level of vlan1 (inside) using CLI of PC0

conf t
int vlan 1
ip add 10.1.1.1 255.0.0.0
no shut
nameif inside
security-level 100
exit
int e0/1
switchport access vlan 1
exit



Setting IP Address and Security level of vlan2 (outside) using CLI of PC0

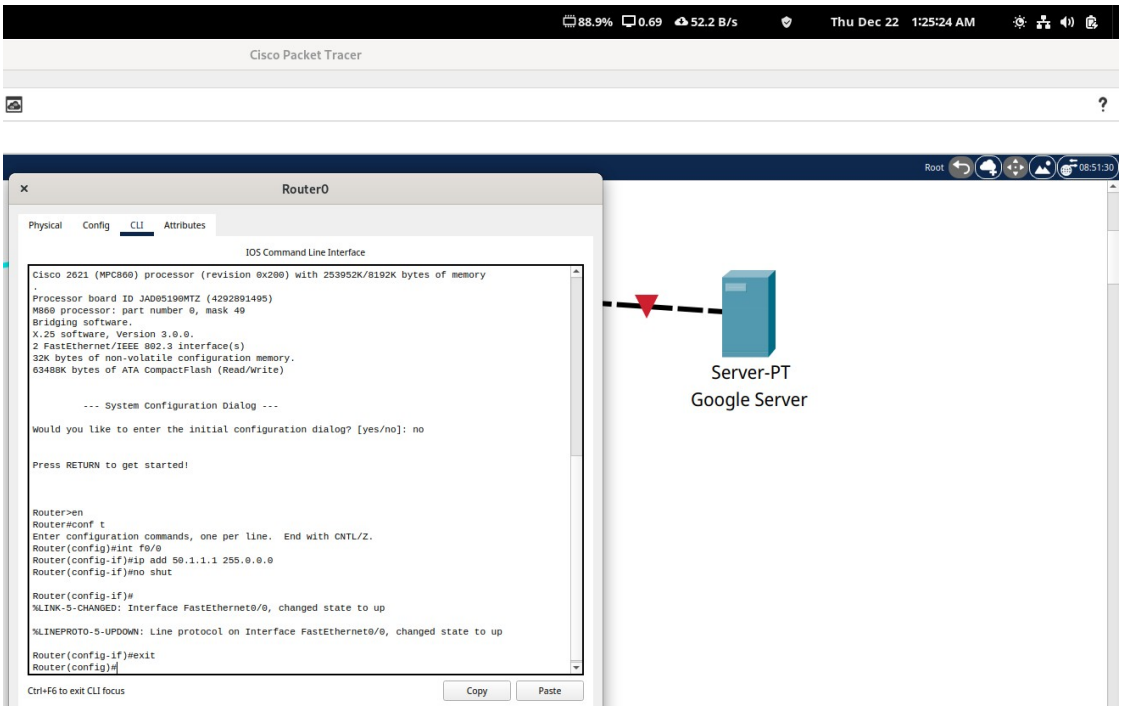
conf t
int vlan 1
ip add 50.1.1.2 255.0.0.0
no shut
nameif outside
security-level 0
exit
int e0/0
switchport access vlan 2
exit



Setting IP Address of ISP Router

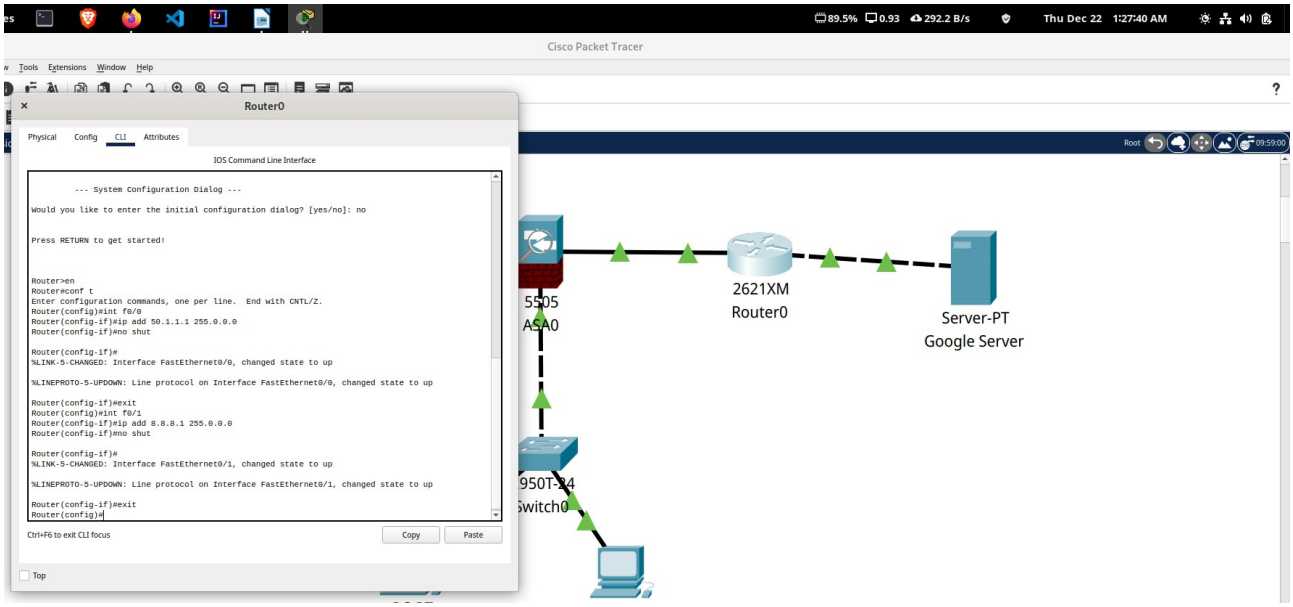
Enable the configuration and then set the IP Address by configuring the FA0/0 interface of the ISP Router.

en
conf t
int f0/0
ip add 50.1.1.1 255.0.0.0
no shut
exit

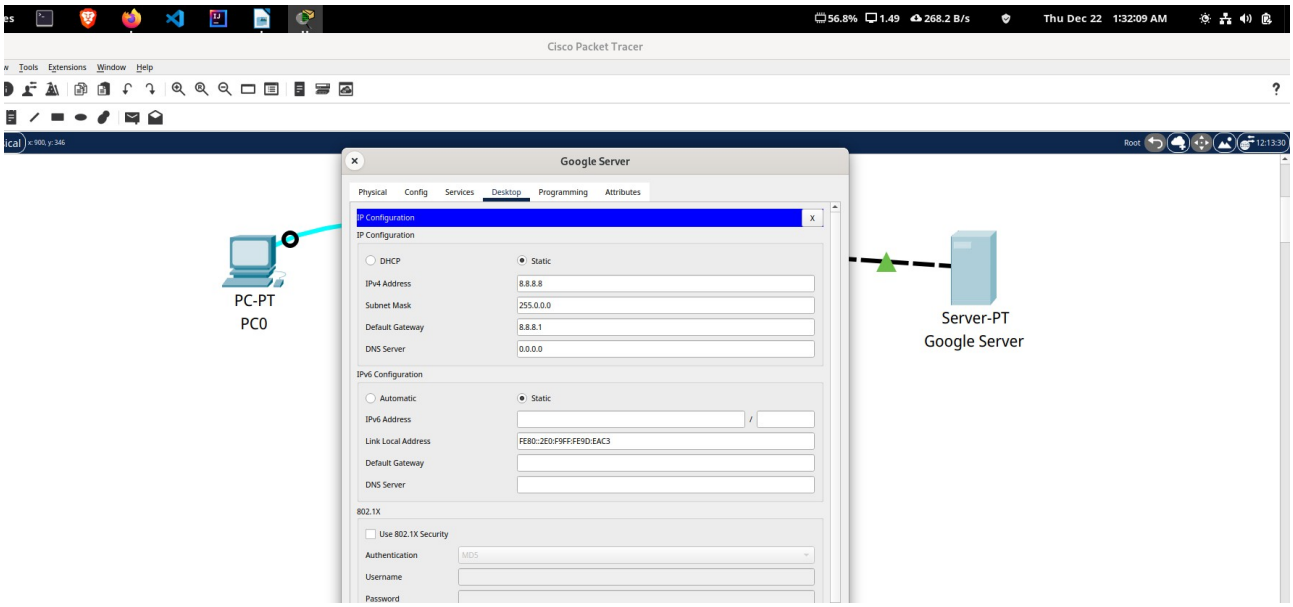


Enable the configuration and then set the IP Address by configuring the FA0/1 interface of the ISP Router.

int f0/1
ip add 8.8.8.1 255.0.0.0
no shut
exit

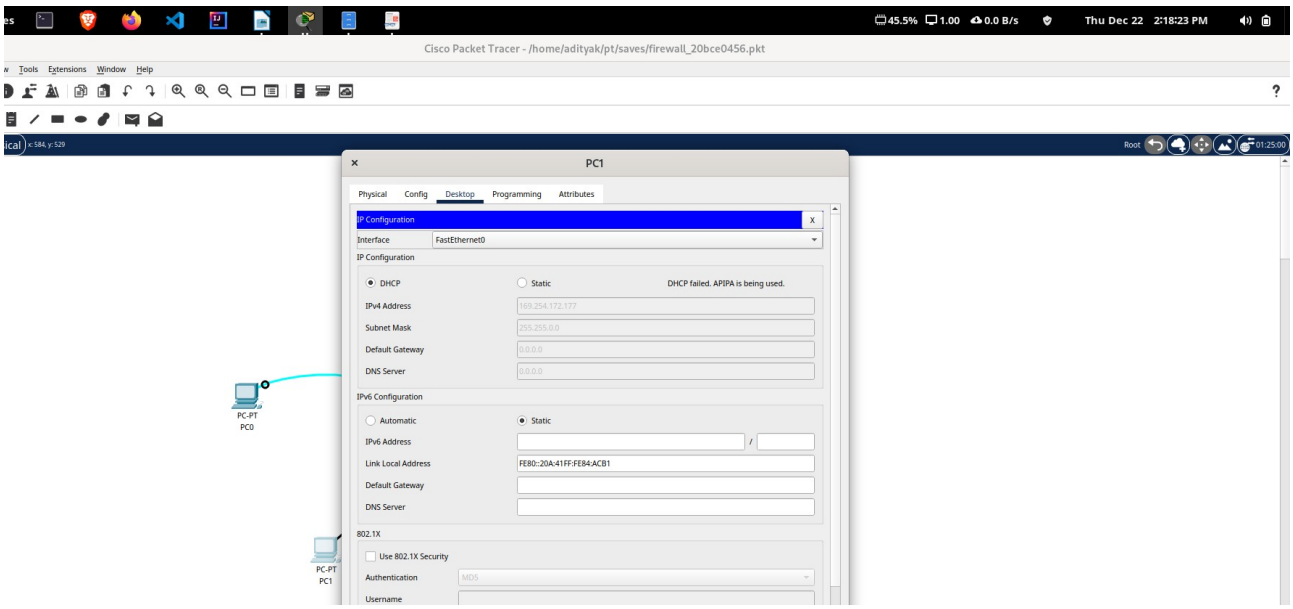


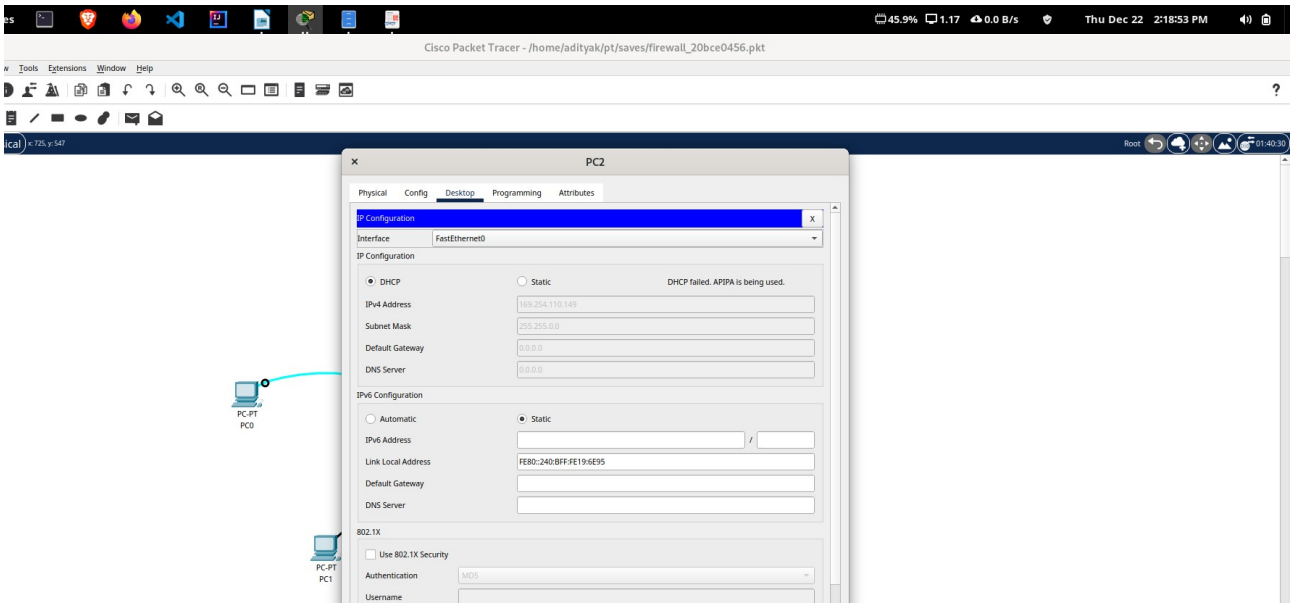
Set the IP Address by configuring the FA0 interface of the Google Server



Step 4 : Configuration of DHCPServer and DNS IP on ASA

Set IP Configuration of PC1 & PC2 from Static to DHCP



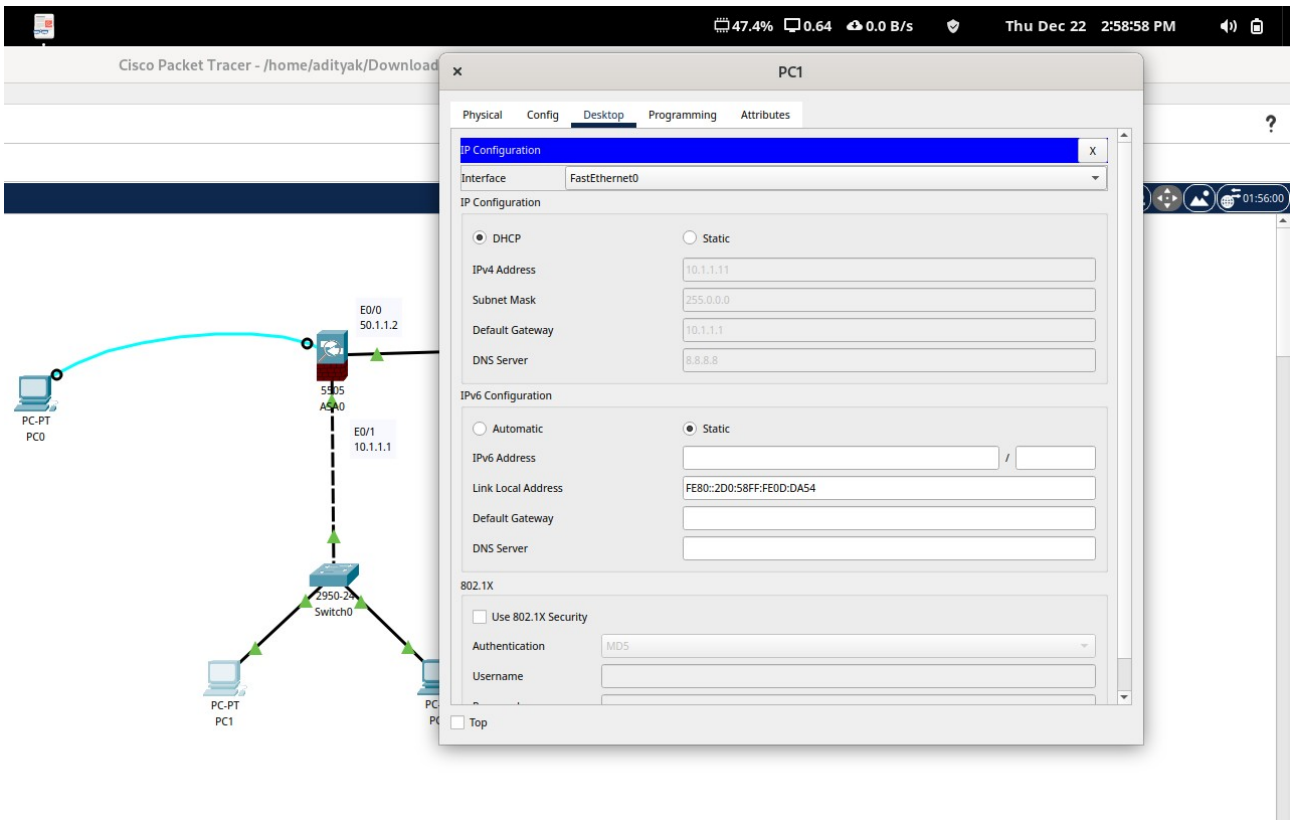


The DHCP addresses won't be provided as of now.

Setting DHCP Server and the DNS IP of firewall using cli of PC0

Using global configuration mode:

dhcpd address 10.1.1.10-10.1.1.30 inside
dhcpd dns 8.8.8.8 interface inside



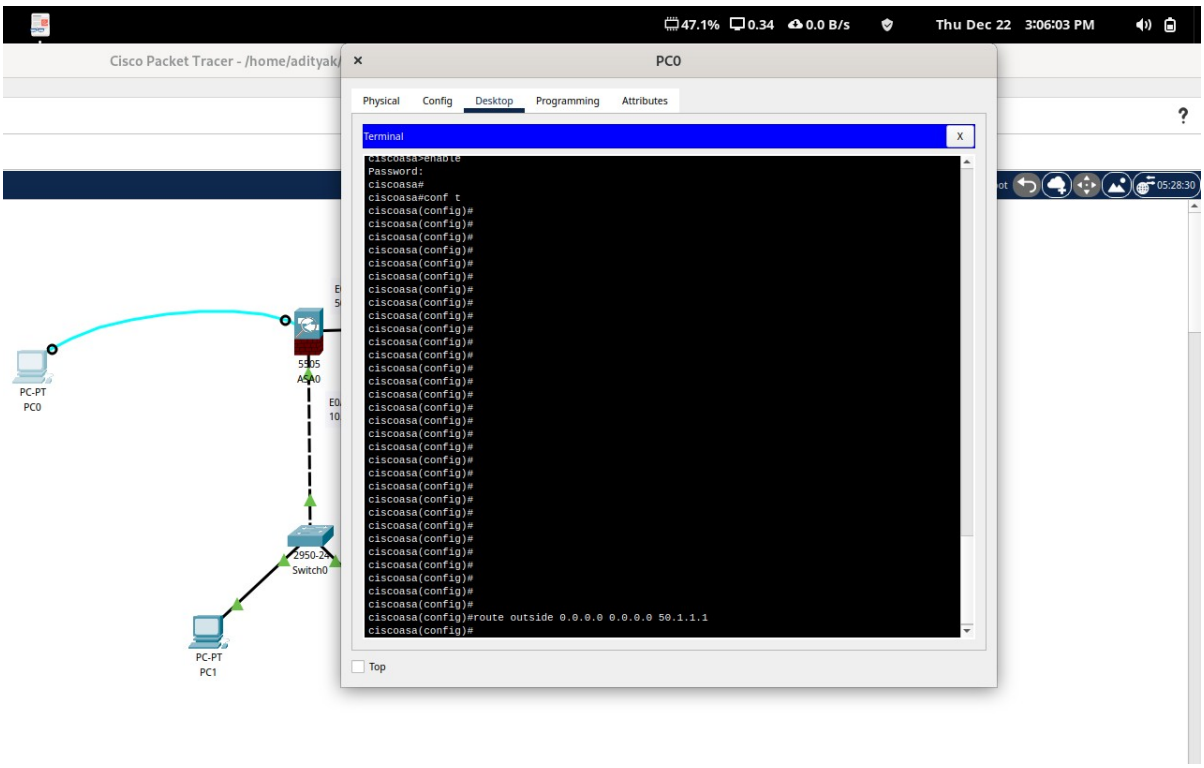
DHCP Server providing IP Address to PC1

DHCP Server providing IP Address to PC2

Step 5 : Configuration of Default Route on ASA

To configure the default route on ASA using CLI Terminal of PC0

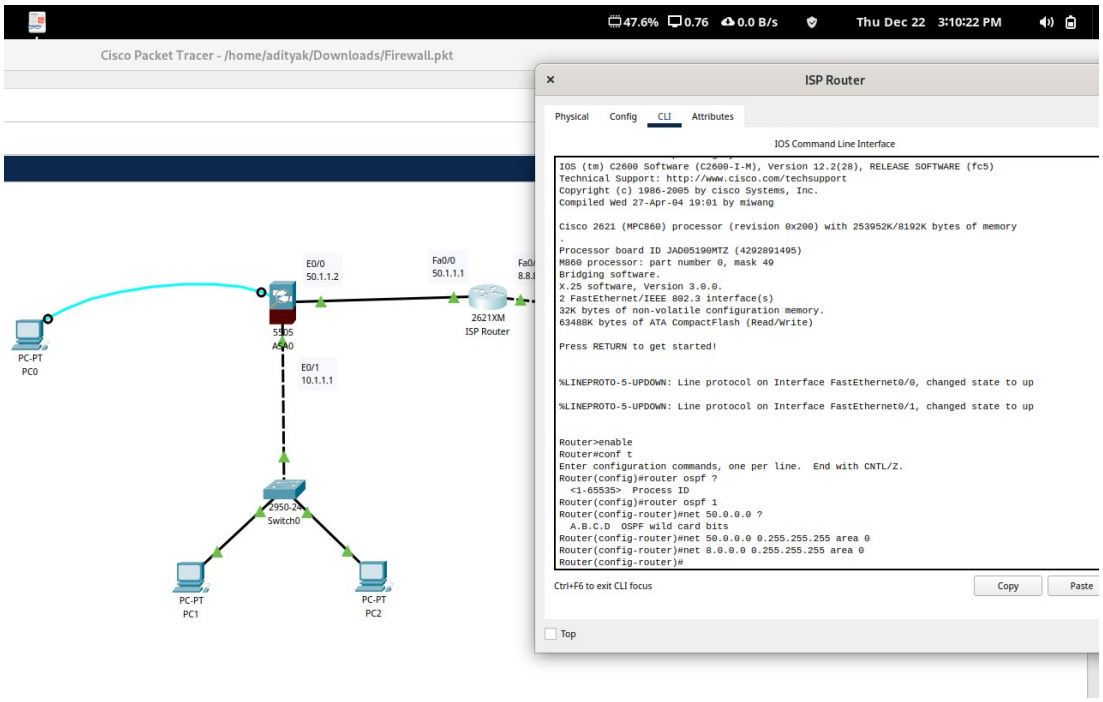
route outside 0.0.0.0 0.0.0.0 50.1.1.1



Step 6 : Configuration of OSPF on ISP Router

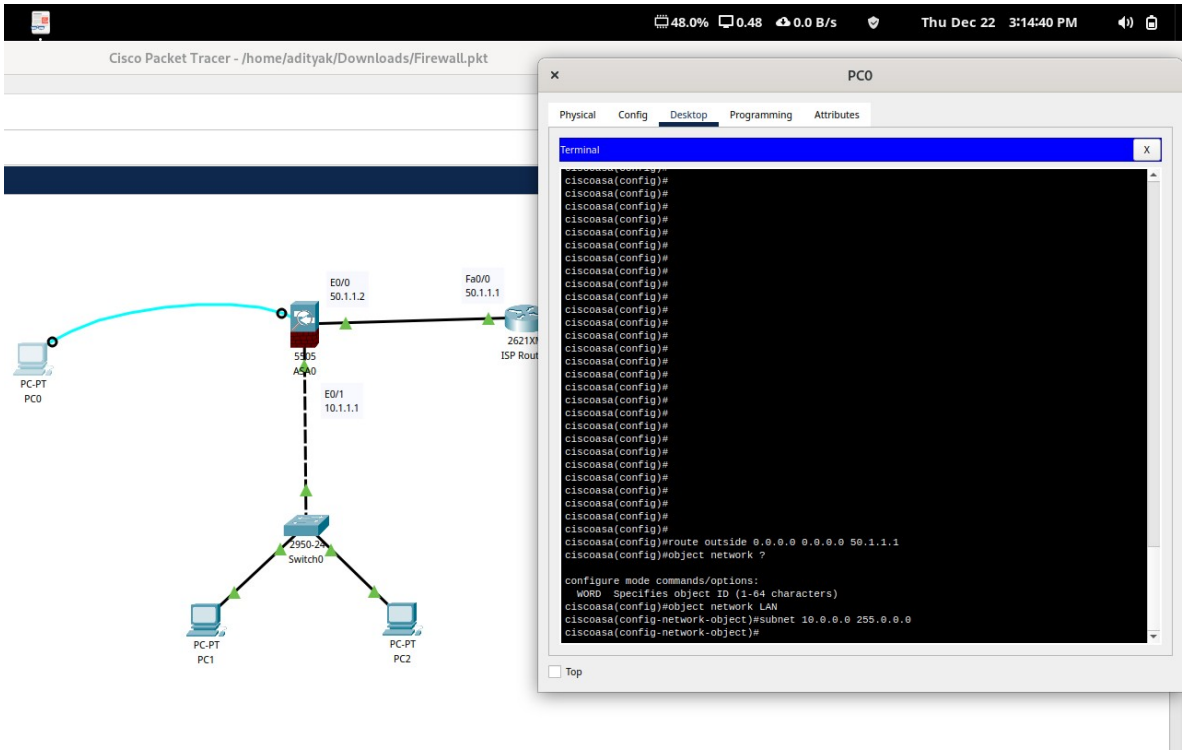
Configure OSPF or any dynamic routing protocol by enabling global configuration mode

en
conf t
router ospf ?
router ospf 1
net 50.0.0.0 ?
net 50.0.0.0 0.255.255.255 area 0
net 8.0.0.0 0.255.255.255 area 0

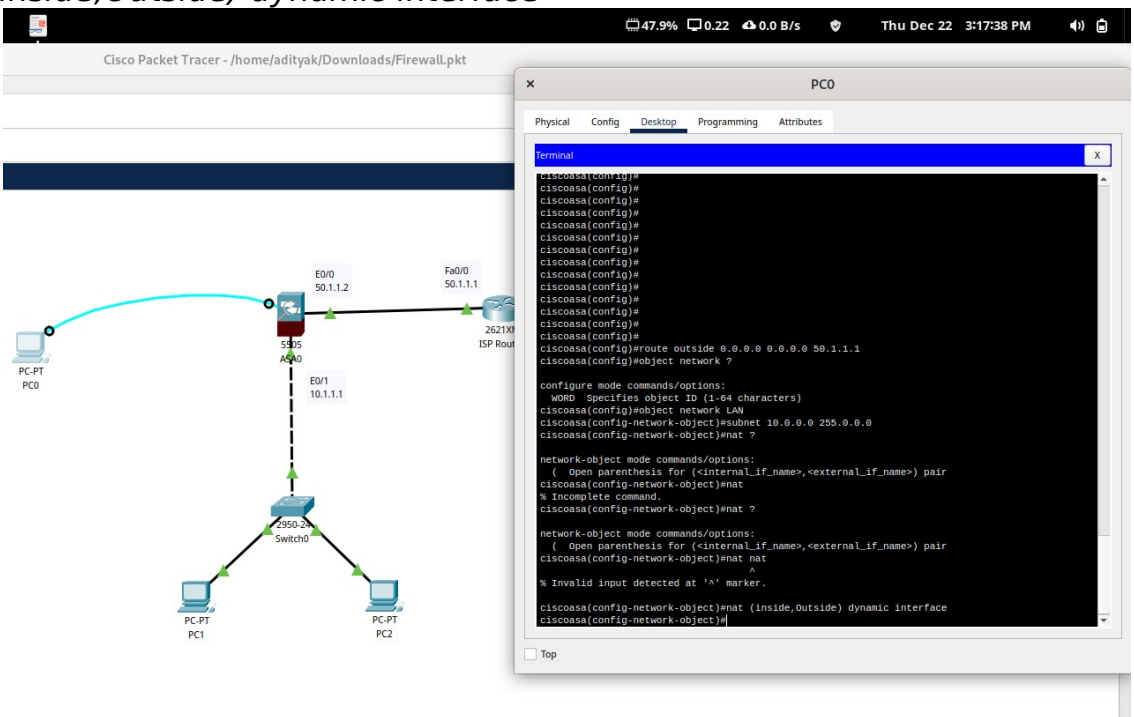


Step 7 : Creation of Object Network and Enable NAT on ASA
Create object network using CLI Terminal of PC0

object network ?
object network LAN
subnet 10.0.0.0 255.0.0.0



Enabling NAT on ASA
nat ?
nat (inside,Outside) dynamic interface



Step 8 : Create ACL on ASA

Using CLI Terminal of PC0 and enabling global configuration

conf t

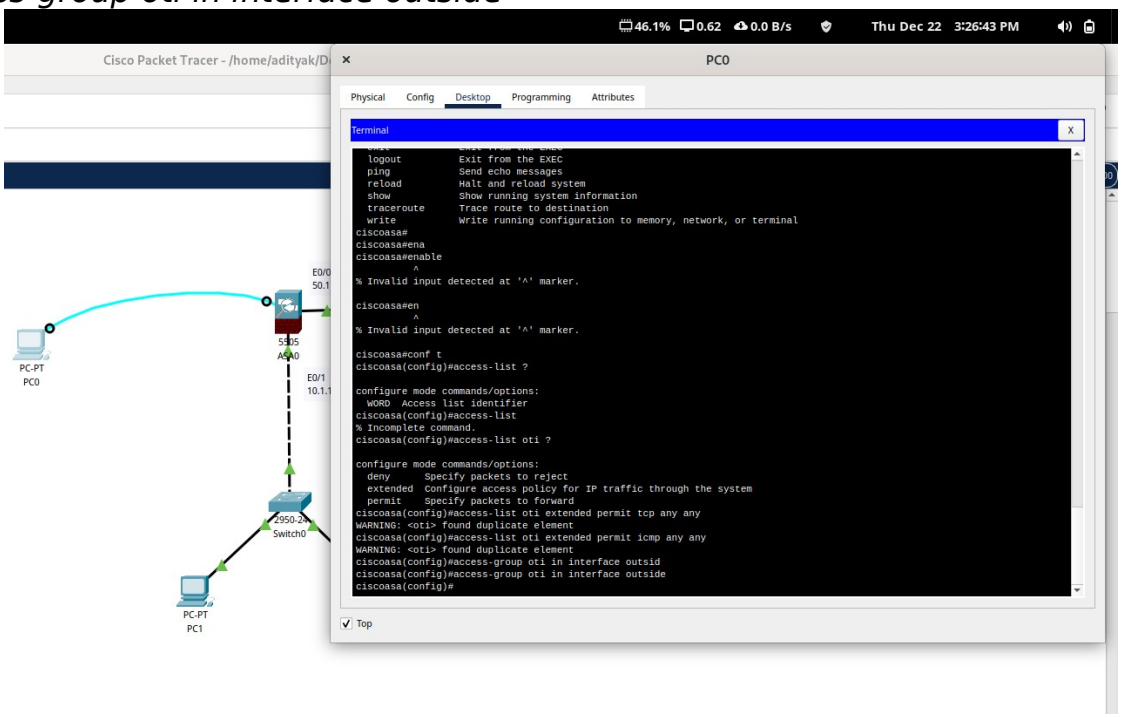
access-list ?

access-list oti ?

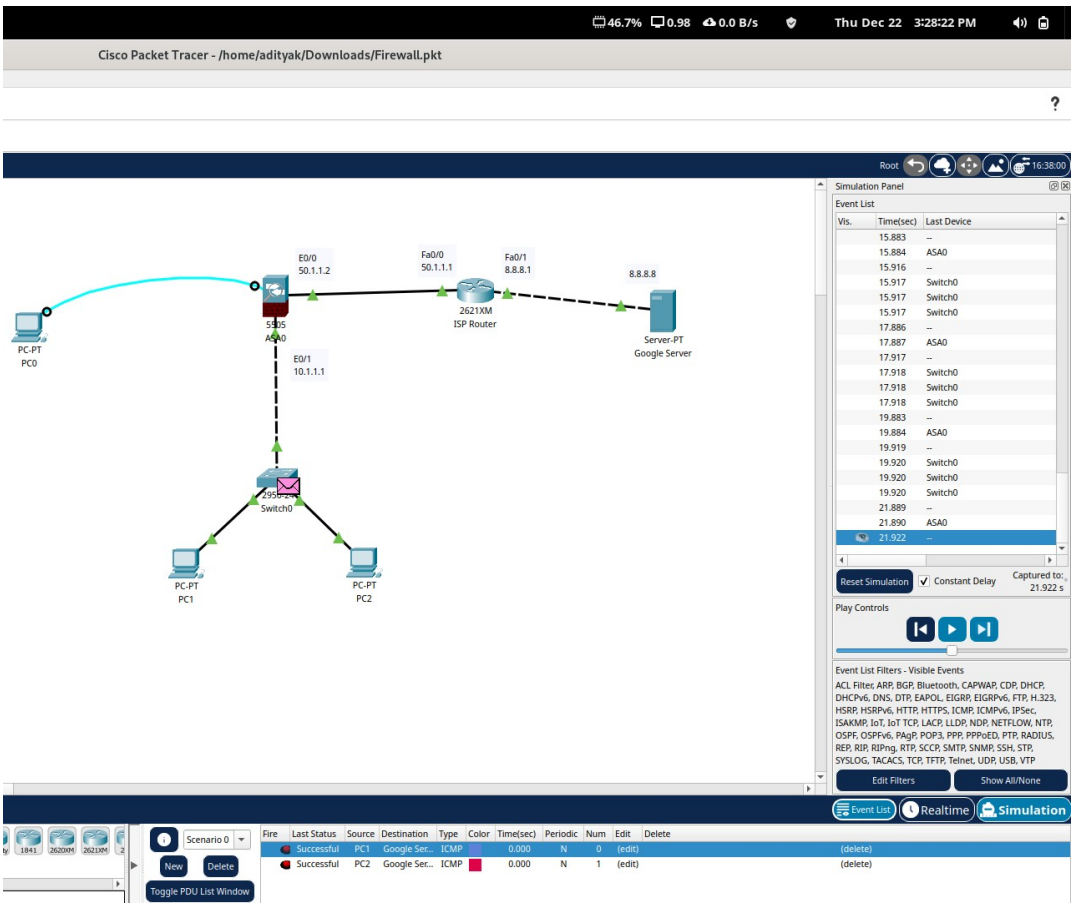
access-list oti extended permit tcp any any (From any source to any destination)

access-list oti extended permit icmp any any

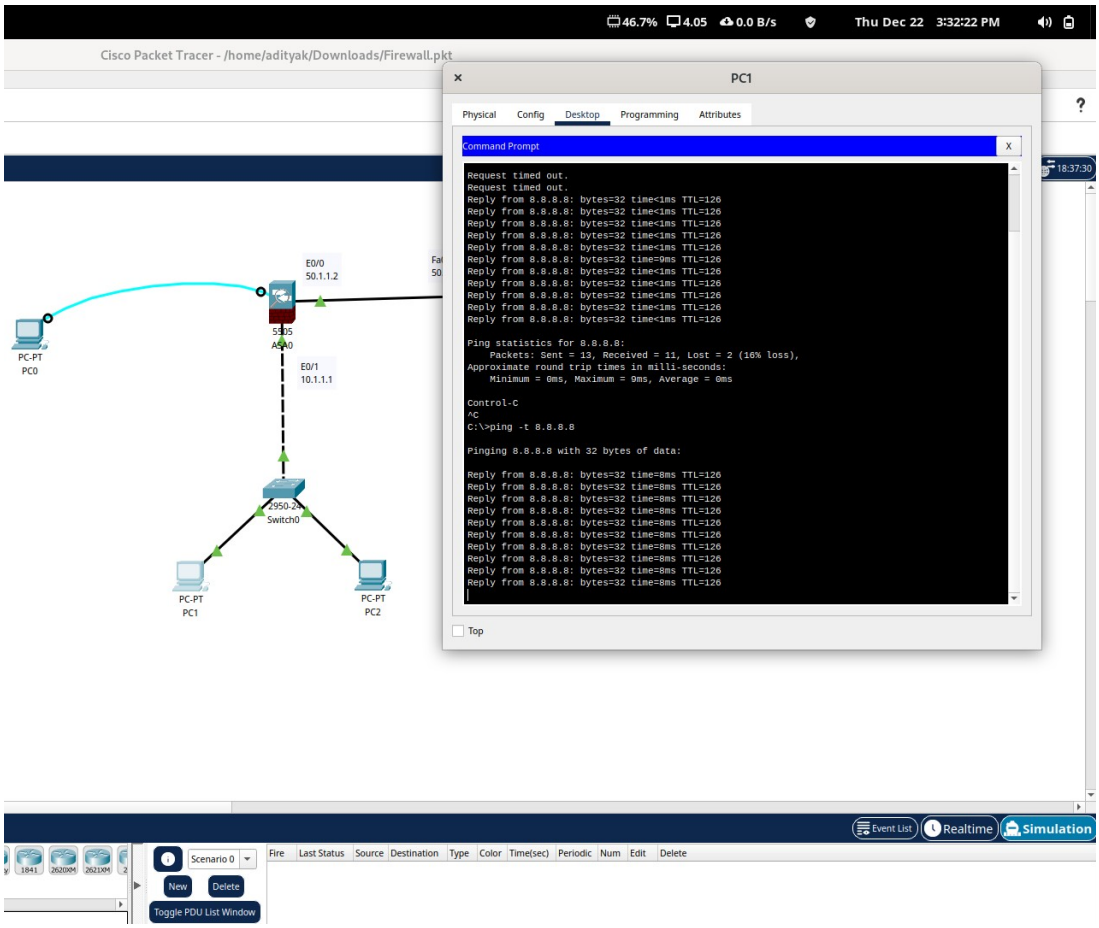
access-group oti in interface outside



Simple PDUs successfully sent from PC1 and PC2 to Google Server.

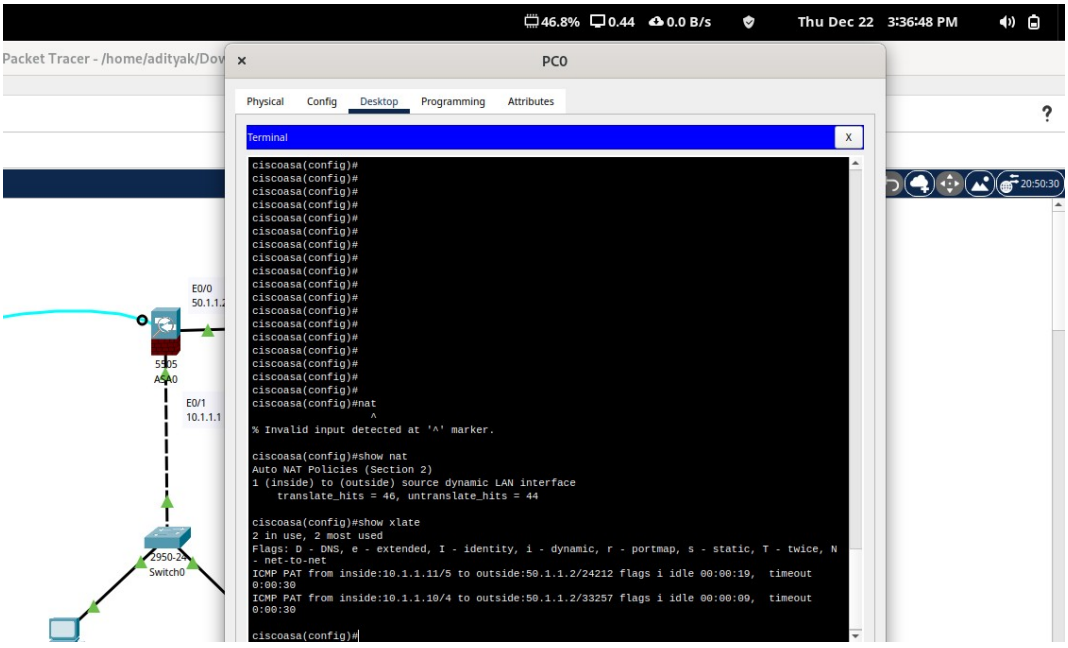


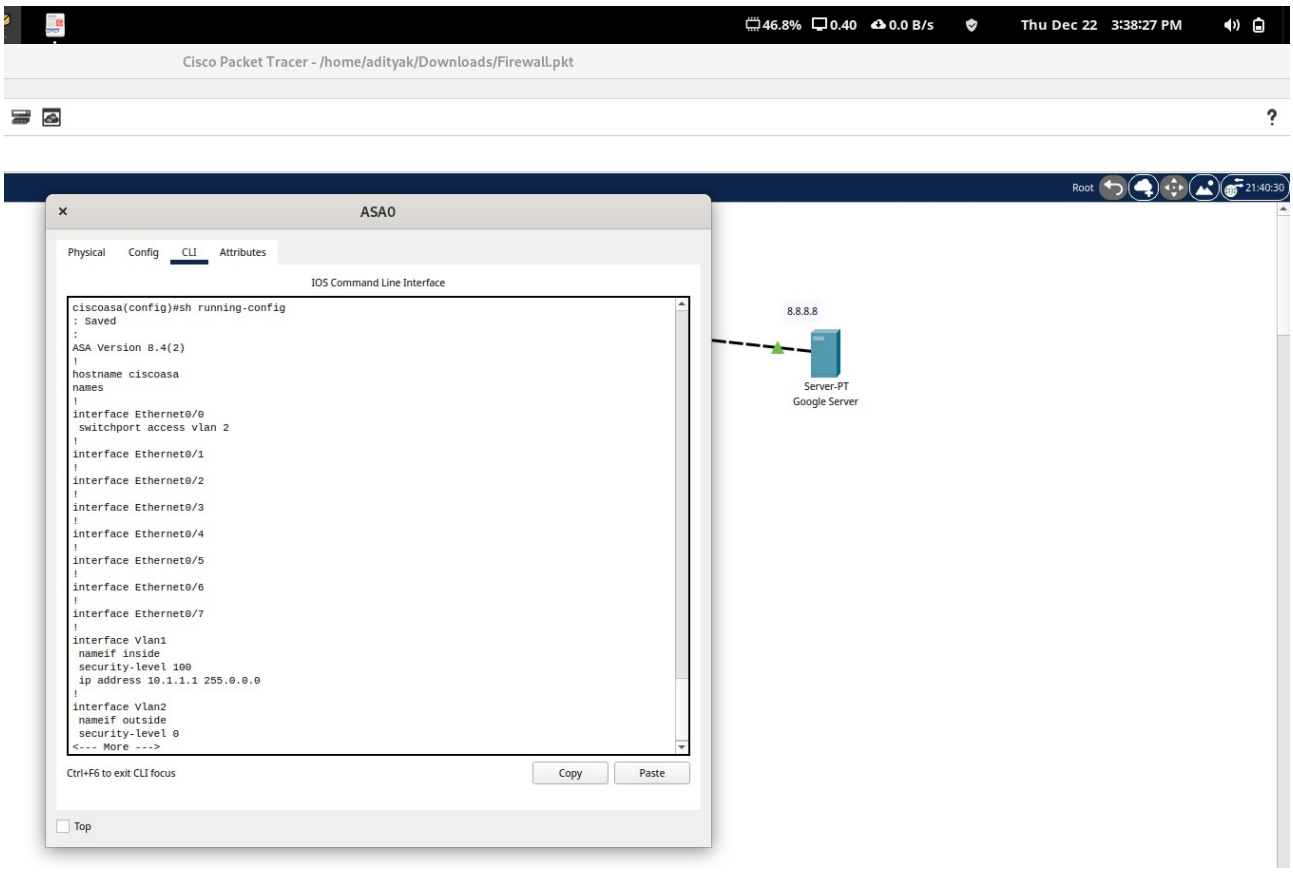
The request-response mechanism is now perfectly working between the Google Server and the PCs 1 & 2 as the firewall allows the communication.



Step 9 : Verification

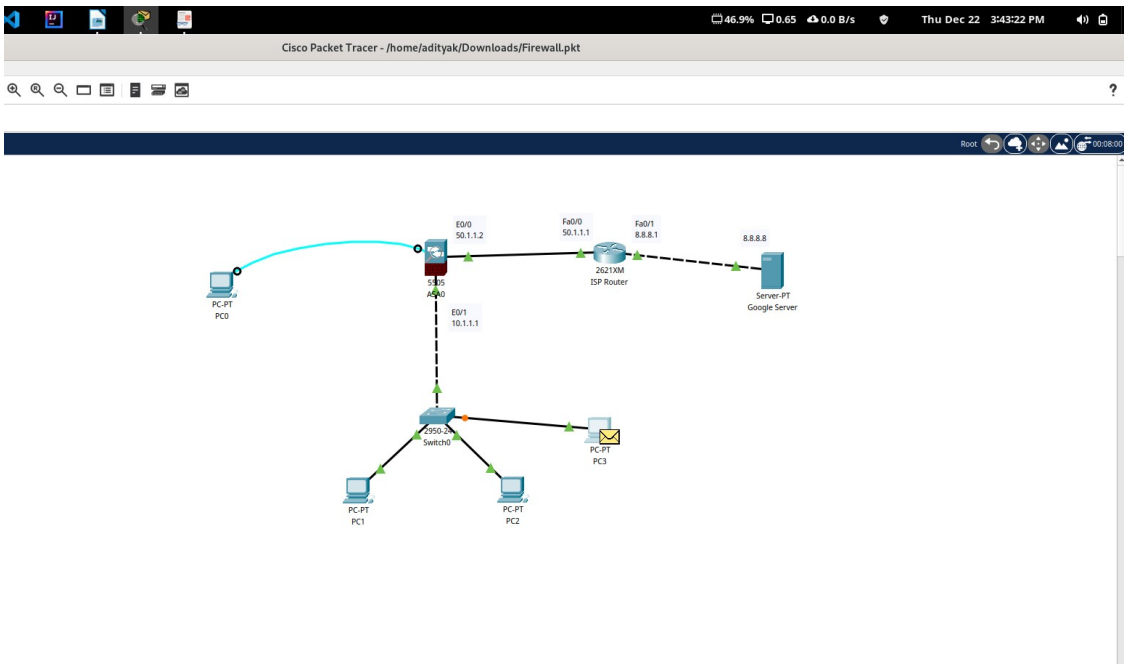
Using privilege mode of the firewall
show nat
show xlate



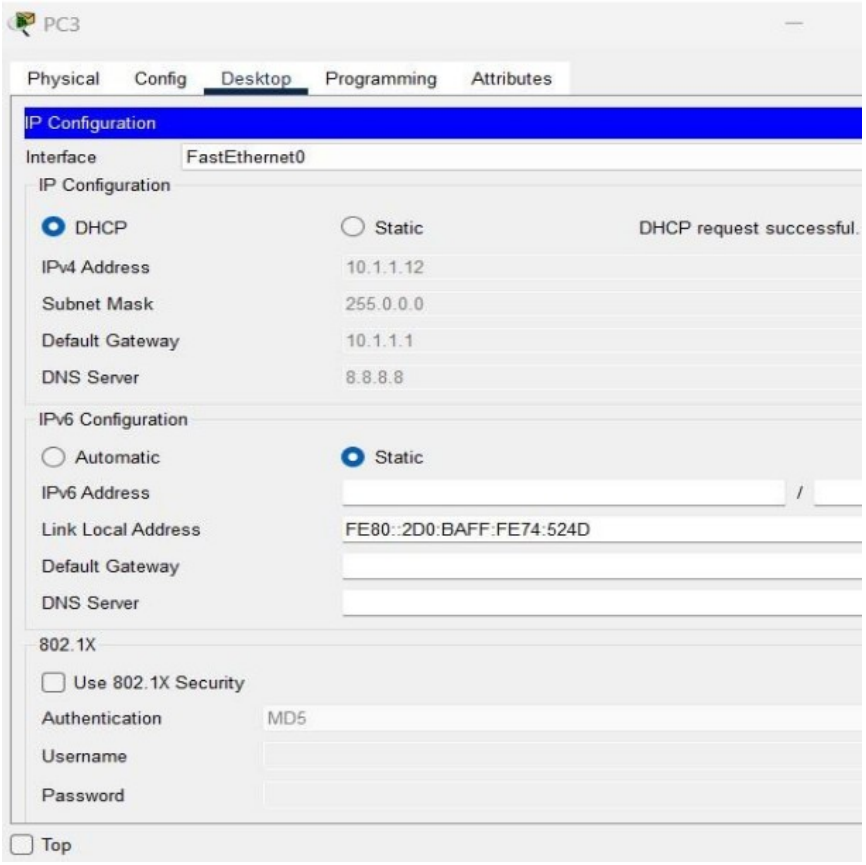


Using running configuration on CLI Terminal of ASA firewall

By adding third PC to inside network and initiating communication between that PC and the Google Server



IP Address successfully allocated to the added PC by the DHCP Server



Conclusion :

We have therefore configured ASA firewall using CISCO Packet Tracer. We can add as many PCs and end-devices in the network and all will have access to the internet, in our case Google Server, via the firewall.

Note: The IP address range in the DHCP Server must be adjusted accordingly.