FIREWALL CONFIGURATION

ABSTRACT:

In this digital world Now a days personal computers and laptops usage are very high for every companies they have limited number of pc’s according to that the hackers also increasing to take the data from the company servers, so we decided to use Cisco Packet Tracer, to establish a firewall configuration for the systems. Here we will provide firewall security for the server and we will let the information access by the server from the computers

Several kinds of network devices like Firewalls are used to protect an institutional network against malicious attacks from the public Internet. This document enumerates and illustrates a selected set of grid scenarios that encounter some issues when dealing with firewall types of devices. The knowledge and experience gathered through these use-cases is utilized to classify the issues into homogeneous categories that can be used by grid application developers and management personnel as guidance. These categories will be used to propose new or recommend existing academic and/or standards based solutions to the grid community.

This research work investigated the firewall security and performance relationship for distributed systems. Internet connectivity is growing with most enterprises migrating to the use of web based services for services provision. As organizations grab the Internet as another business tool whether to sell, to team up or to communicate - web applications have turned into the new weakest connection in the organization's security technique. Firewalls provide a mechanism for protecting these enterprises from the less secure internet over which customers or collaborating partners transfer packets destined for the corporate network. The connection between the security and execution proficiency is exhibited through distinctive scenarios and the relationship between security and performance in firewalls is assessed. We demonstrated distinctive networks (with and without firewalls and diverse firewall functionality and simulated such systems with an eye on their performance). The simulation was done for 300 workstations and simulated in a way that all the 300 workstations access an email and web application under three different scenarios. Attention is on the relationship between system security and performance; the impacts of firewalls on system execution. Different scenarios were assessed through simulations utilizing OPNET IT Guru Academic Edition 9.1 to demonstrate the impacts of firewalls on system performance. The result shows that maintaining security which involves the utilization of numerous applications and the use of firewall has an effect on network performa

Methodology:- Firewall configuration consists of modules like pc’s, switches and servers. First the company pc’s are connected to the servers through the switch here switch is the intermediate act between the servers and pc’s . If the unknown ip address tries to login like hackers they can't login because the servers can’t recognize their ip address and data is blocked. The company devices also are able to login using the switches to access the data from the servers.If the unknown ip address is repeating again and again the server is blocked.

There are certain methods through which firewalls can be implemented. These are as follows:

Static packet filtering – Packet filtering is a firewall technique used to control access on the basis of source IP address, destination IP address, source port number, and destination port number. It works on layers 3 and 4 of the OSI model. Also, an ACL doesn't maintain the state of the session. A router with ACL applied to it is an example of static packet filtering.

Stateful packet filtering –

In stateful packet filtering, the state of the sessions is maintained i.e when a session is initiated within a trusted network, it's the source and destination IP address, source, and destination ports, and other layer information are recorded. By default, all the traffic from an untrusted network is denied.

The replies of this session will be allowed only when the IP addresses (source and destination IP address) and port numbers (source and destination)are swapped.

Proxy firewalls –

These are also known as application-layer firewalls. A proxy firewall acts as an intermediary between the original client and the server. No direct connection takes place between the original client and the server.

The client, who has to establish a connection directly to the server to communicate with it, now has to establish a connection with the proxy server. The proxy server then establishes a connection with the server on the behalf of the client. Now, the client sends the data to the proxy server and the proxy server forwards it to the server. A proxy server can operate up to layer 7 (application layer).

Application inspection –

These can analyze the packet up to layer 7 (deep inspection) but can't act as a proxy server. These can deeply analyze conversations between a client and server even when the server is assigning a dynamic port to the client therefore it doesn't fail in these cases (which can occur in a stateful firewall).

Transparent firewall –

By default, the firewall operates at layer 3 but the benefit of using a transparent firewall is that it can operate at layer 2. It has 2 interfaces that will act as a bridge so can be configured through a single management IP address. Also, users accessing the network will not even know that a firewall exists.

The main advantage of using a transparent firewall is that we don't need to re-address our networks while putting up a firewall in our network. Also, while operating at layer 2, it can still perform functions like building a stateful database, application inspection, etc

Network Address Translation (NAT) –

NAT is implemented on a router or firewall. NAT is used to translate a private IP address into a public IP address through which we can hide our source IP address.

And if we are using dynamic NAT or PAT, an attacker will not be able to know what devices are dynamically assigned which IP address from the pool. This makes it difficult to make a connection from the outside world to our private network.

Next-Generation Firewalls –

NGFWs are third-generation security firewalls that are implemented in either software or devices. It combines basic firewall properties like static packet filtering, application inspection with advanced security features like an integrated intrusion prevention system. Cisco ASA with firePOWER services is an example of a Next-Generation firewall.

Firewall Technologies

This section of the publication provides an overview of firewall technologies and basic information on the capabilities of several commonly used types. Firewalling is often combined with other technologies— most notably routing—and many technologies often associated with firewalls are more accurately part of these other technologies. For example, network address translation (NAT) is sometimes thought of as a firewall technology, but it is actually a routing technology. Many firewalls also include content filtering features to enforce organization policies not directly related to security. Some firewalls include intrusion prevention system (IPS) technologies, which can react to attacks that they detect to prevent damage to systems protected by the firewall.

Firewalls are often placed at the perimeter of a network. Such a firewall can be said to have an external and internal interface, with the external interface being the one on the outside of the network. These two interfaces are sometimes referred to as unprotected and protected, respectively. However, saying that something is or is not protected is often inappropriate because a firewall's policies can work in both directions; for example, there might be a policy to prevent executable code from being sent from inside the perimeter to sites outside the perimeter.

Packet Filtering The most basic feature of a firewall is the packet filter. Older firewalls that were only packet filters were essentially routing devices that provided access control functionality for host addresses and communication sessions. These devices, also known as stateless inspection firewalls, do not keep track of the state of each flow of traffic that passes though the firewall; this means, for example, that they cannot associate multiple requests within a single session to each other. Packet filtering is at the core of most modern firewalls, but there are few firewalls sold today that only do stateless packet filtering. Unlike more advanced filters, packet filters are not concerned about the content of packets. Their access control functionality is governed by a set of directives referred to as a ruleset. Packet filtering capabilities are built into most operating systems and devices capable of routing; the most common example of a pure packet filtering device is a network router that employs access control lists. In their most basic form, firewalls with packet filters operate at the network layer. This provides network access control based on several pieces of information contained in a packet, including: The packet's source IP address—the address of the host from which the packet originated (such as 192.168.1.1) The packet's destination address—the address of the host the packet is trying to reach (e.g., 192.168.2.1)

Application Firewalls

A newer trend in stateful inspection is the addition of a stateful protocol analysis capability, referred to by some vendors as deep packet inspection. Stateful protocol analysis improves upon standard stateful inspection by adding basic intrusion detection technology—an inspection engine that analyzes protocols at the application layer to compare vendor-developed profiles of benign protocol activity against observed events to identify deviations. This allows a firewall to allow or deny access based on how an application is running over the network. For instance, an application firewall can determine if an email message contains a type of attachment that the organization does not permit (such as an executable file), or if instant messaging (IM) is being used over port 80 (typically used for HTTP). Another feature is that it can block connections over which specific actions are being performed (e.g., users could be prevented from using the FTP "put" command, which allows users to write files to the FTP server). This feature can also be used to allow or deny web pages that contain particular types of active content, such as Java or ActiveX, or that have SSL certificates signed by a particular certificate authority (CA), such as a compromised or revoked CA

Major Result:- Created a firewall configurations for the systems by using Cisco packet tracer that considers one of the most important protection that majority of the companies data stored securely in the servers if the companies pc's also not detected that pc also can't login .

Majority of the companies use the firewall configuration because it is one of the latest ways of protecting the company's servers.And this implementation is done by using Cisco Packet Tracer.

Implications:-The servers will be directly connected to the client systems through the switches. The ICMP(Internet control message protocol) is been blocked at the server and we have allowed only IP address so that pcs can't send the messages to the server and they can only access through the website address

OBJECTIVE:-

The aim of this project is to come up with a simulation of firewall configurations for the systems That can be accessed by only clients and known IP addresses and show the concept of firewall configurations for the systems.Use of Cisco Packet Tracking Features simulated firewall configuration for the servers. This gives protection and safety to the company database. While the primary goal of a firewall is to keep attackers out, it also serves a valuable purpose by monitoring outgoing connections. Many types of malware will send out a signal once they take over a system, allowing the author to trigger specific actions or even control the computer remotely. A firewall can alert you when an unknown program attempts to "phone home," alerting you to a possible malware infection and allowing you to shut it down before it causes major damage to your network. Heading off a malware attack before it activates will keep your employees productive, protect vital company data and save you the cost of cleaning up the problem with other security software.

While the primary goal of a firewall is to **keep attackers out**, it also serves a valuable purpose by monitoring outgoing connections. Many types of malware will send out a

signal once they take over a system, allowing the author to trigger specific actions or even control the computer remotely.

A firewall is a vital piece of your business's defense against electronic threats. Serving as a gatekeeper between your company's servers and the outside world, a properly maintained firewall will not only keep external threats out, but it can also alert you to more subtle problems by intercepting outgoing data as well. Paired with a well-maintained anti-malware suite, a firewall can save your business from spending time and money dealing with virus infections or hacker attacks.

INTRODUCTION:-

The Cisco ASA 5505 Firewall is the smallest model in the new 5500 Cisco series of hardware appliances. Although this model is suitable for small businesses, branch offices or even home use, its firewall security capabilities are the same as the biggest models (5510, 5520, 5540
etc). The Adaptive Security technology of the ASA firewalls offers solid and reliable firewall protection, advanced application-aware security, denial of service attack protection and much more. Moreover, the performance of the ASA 5505 appliance supports 150Mbps firewall throughput and 4000 firewall connections per second, which is more than enough for small networks. In this article, I will explain the basic Cisco ASA 5505 configuration for connecting a small network to the Internet (here the complete guides).

We assume that our ISP has assigned us a static public IP address (e.g 200.200.200.1 as an example) and that our internal network range is 192.168.1.0/24. We will use Port Address Translation (PAT) to translate our internal IP addresses to the public address of the outside interface. The difference of the 5505 model from the bigger ASA models is that it has an 8-port 10/100 switch which acts as Layer 2 only. That is, you can not configure the physical ports as Layer 3 ports, rather you have to create interface VLANS(VLANs allow network administrators to automatically limit access to a specified group of users by dividing workstations into different isolated LAN segments. When users move their workstations, administrators don't need to reconfigure the network or change VLAN groups.)and assign the Layer 2 interfaces in each VLAN. By default, interface Ethernet0/0 is assigned to VLAN 2 and it’s the outside interface (the one which connects to the Internet), and the other 7 interfaces (Ethernet0/1 to 0/7) are assigned by default to VLAN 1 and are used for connecting to the internal network. Let’s see the basic configuration setup of the most important steps that you need to configure.

Firewalls have existed since the late 1980’s and started out as packet filters, which were networks set up to examine packets, or bytes, transferred between computers. Though packet filtering firewalls are still in use today, firewalls have come a long way as technology has developed throughout the decades.

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.

MODULES:-

SERVERS:-Server Is used to store the companies data and store every work related to usage of the companies .The role of a server is to share data as well as to share resources and distribute work. A server computer can serve its own computer programs as well; depending on the scenario, this could be part of a quid pro quo transaction, or simply a technical possibility.To protect the data from the unauthorized persons or unknown address the servers can be used. A physical server is simply a computer that is used to run server software. The differences between a server and a desktop computer will be discussed in detail in the next section. A virtual server is a virtual representation of a physical server. Like a physical server, a virtual server includes its own operating system and applications. These are kept separate from any other virtual servers that might be running on the physical server. The process of creating virtual machines involves installing a lightweight software component called a hypervisor onto a physical server. The supervisor's job is to enable the physical server to function as a virtualization host. The virtualization host makes the physical server's hardware resources -- such as CPU time, memory, storage and network bandwidth -- available to one or more virtual machines. An administrative console gives administrators the ability to allocate specific hardware resources to each virtual server. This helps dramatically drive down hardware costs because a single physical server can run multiple virtual servers, as opposed to each workload needing its own physical server.

Client–server systems are usually most frequently implemented by (and often identified with) the request response model: a client sends a request to the server, which performs some action and sends a response back to the client, typically with a result or acknowledgment. Designating a computer as "server-class hardware" implies that it is specialized for running servers on it. This often implies that it is more powerful and reliable than standard personal computers, but alternatively, large computing clusters may be composed of many relatively simple, replaceable server components.

SWITCHES:- The switches will be accessed in the Data link layer It takes in packets being sent by devices that are connected to its physical ports and sends them out again, but only through the ports that lead to the devices the packets are intended to reach Once a device is connected to a switch, the switch notes its media access control (MAC) address, a code that's baked into the device's network-interface card (NIC) that attaches to an ethernet cable that attaches to the switch. The switch uses the MAC address to identify which attached device outgoing packets are being sent from and where to deliver incoming packets. Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network. A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications.

Unmanaged Switch − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices need to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.

Managed Switch − These are costly switches that are used in organizations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.

LAN Switch − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred to as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
A network device that cross-connects clients, servers and network devices. Also known as a "frame switch,

LAN switches are common in Ethernet networks. A switch with four or more ports is also built into a wire

router for homes and small business

PoE Switch − Power over Ethernet (PoE) switches are used in PoE Gigabit Ethernets. PoE technology combines data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections

- A switch operates in the layer 2, i.e. data link layer of the OSI model.
- It is an intelligent network device that can be conceived as a multiport network bridge.
- It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
- It uses packet switching technique to receive and forward data packets from the source to the destination device.
- It supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
- Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.
- The number of ports is higher – 24/48.

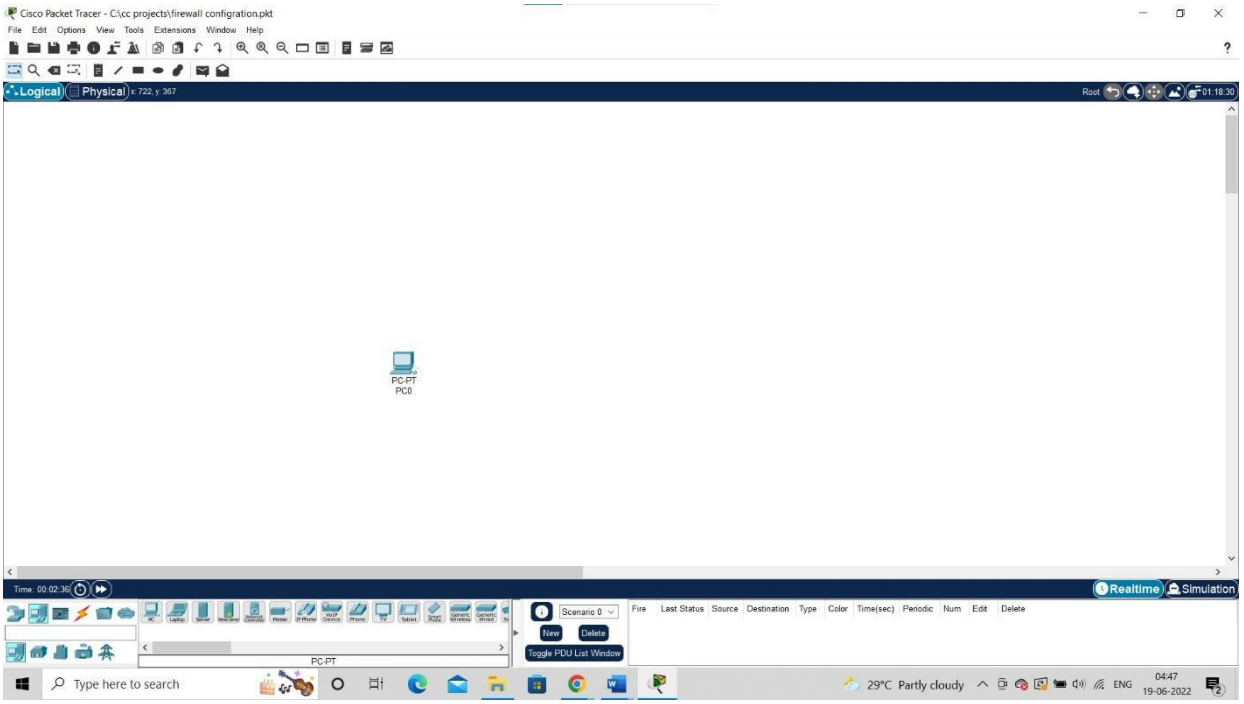
PC'S:- The use of the personal computers in the companies are to create any documents, projects reports according to the company needs. And the personal computers assigned to every employee in the company.Only the known ip address or mac address which connected to the switches based on the company needs. personal computer (PC)**,** a digital computer designed for use by only one person at a time. A typical personal computer assemblage consists of a central programing unit (CPU), which contains the computer's arithmetic, logic, and control circuitry on an integrated circuit two types of computer

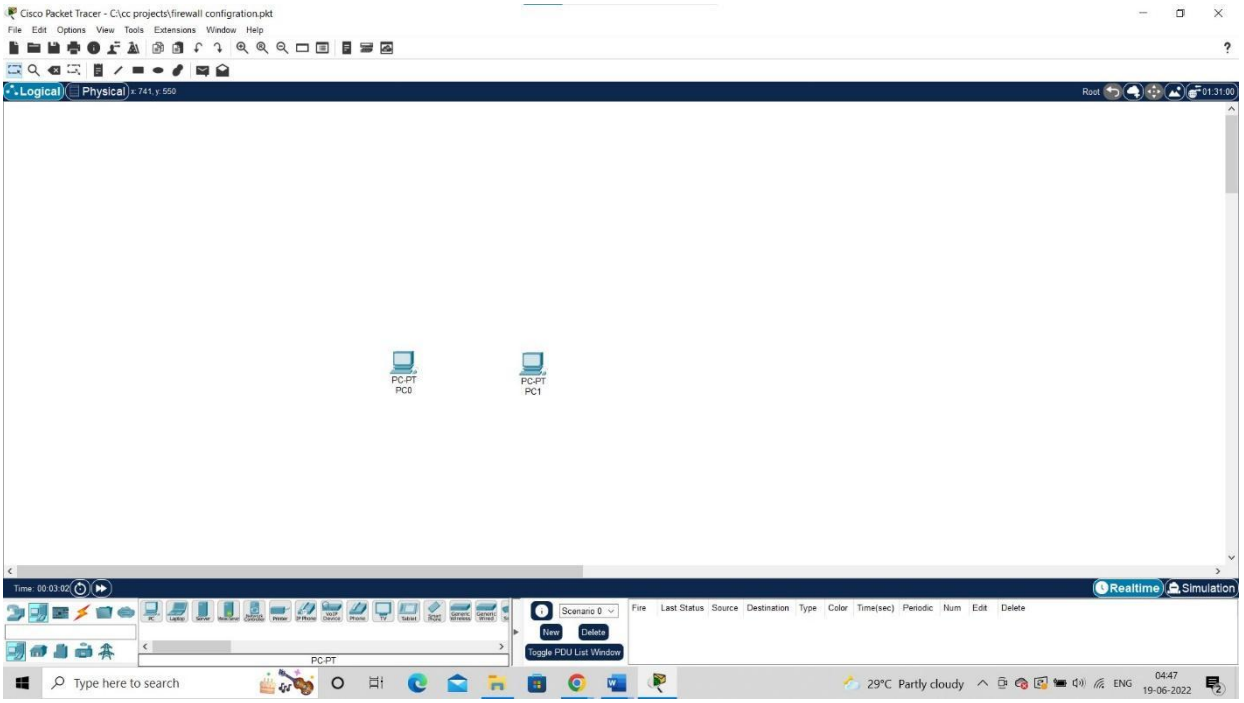
memory main memory, such as digital Random access memory (RAM),
and auxiliary memory, such as magnetic hard disks and special optical compact discs or read-only memory (ROM) discs (CD-ROMs and DVD-ROMs); and various secondary devices, including a display screen, keyboard and mouse, and printer.

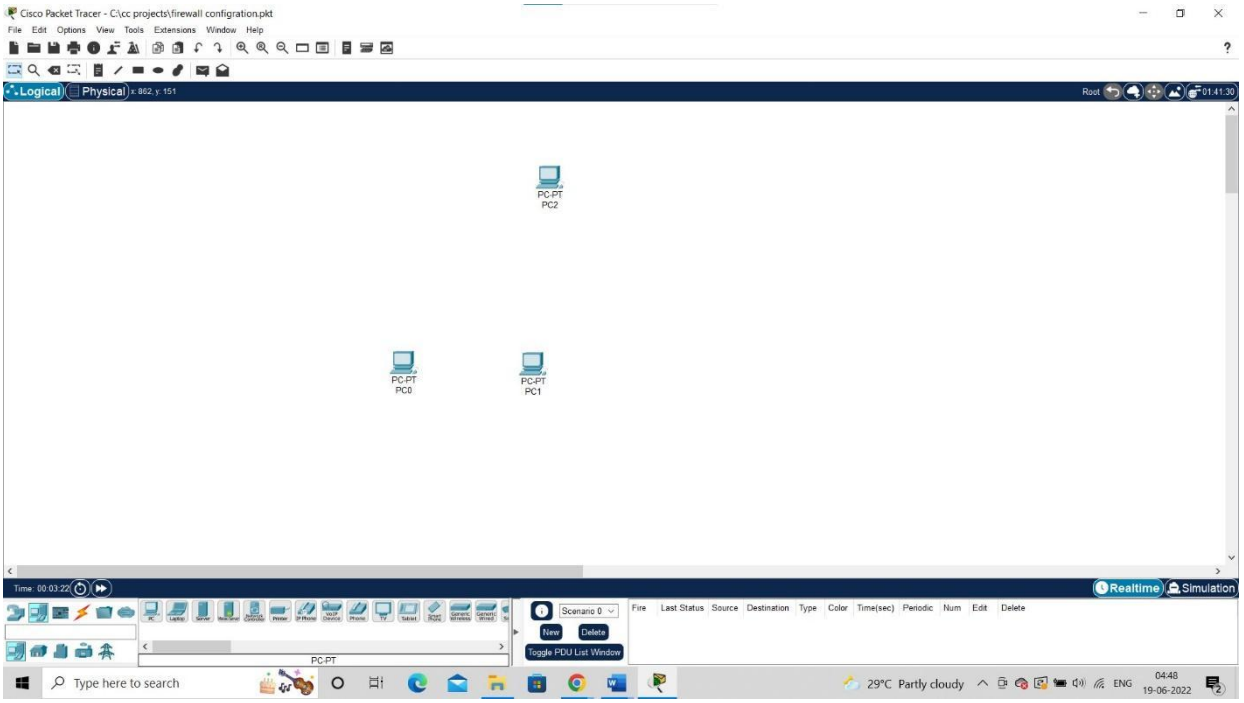
The personal computer industry truly began in 1977, with the introduction of three preassembled mass-produced personal computers: the Apple Computer, Inc. (now Apple Inc.), AppleII, the Tandy Radio Shack TRS-80, and the commodore business machines Personal Electronic Transactor (PET). These machines used eight-bit microprocessors (which process information in groups of eight bits, or binary digits, at a time) and possessed rather limited memory capacity—i.e., the ability to address a given quantity of data held in memory storage. But because personal computers were much less expensive than mainframe computers (the bigger computers typically deployed by large business, industry, and government organizations), they could be purchased by individuals, small and medium-sized businesses, and primary and secondary schools.

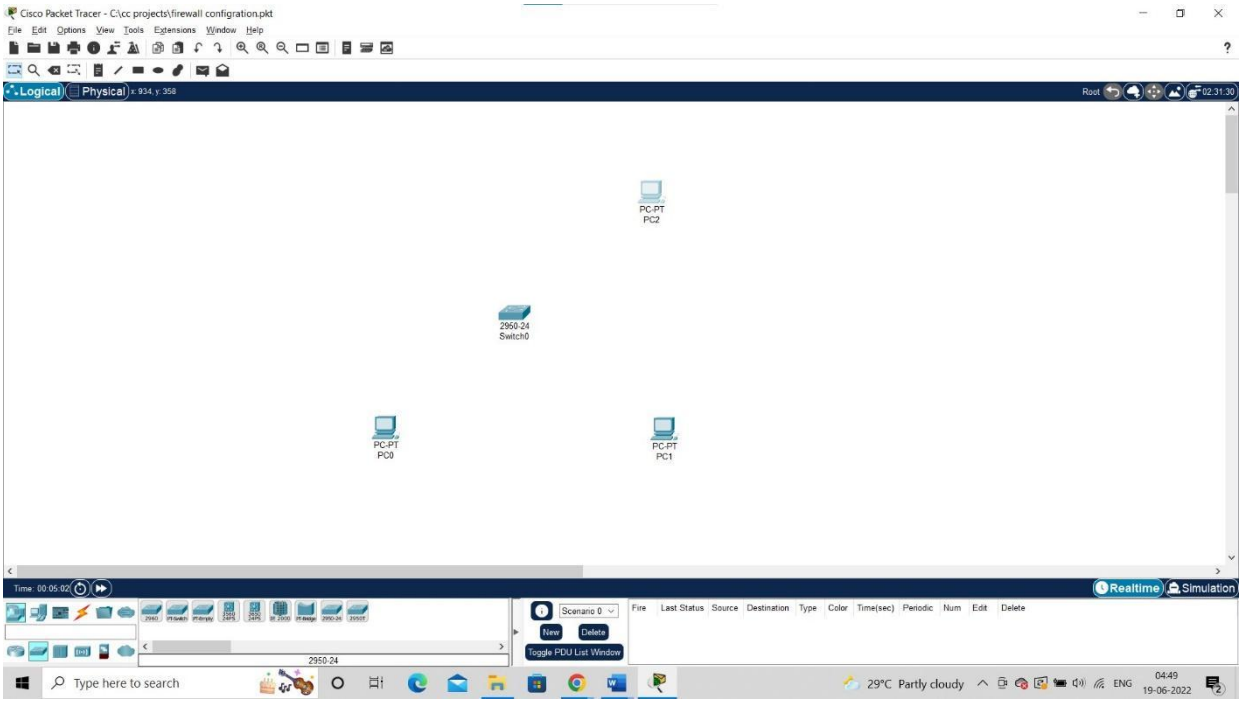
Of these computers, the TRS-80 dominated the market. The TRS-80 microcomputer came with four kilobytes of memory, a Z80 microprocessor, a BASIC programming language, and cassettes for data storage. To cut costs, the machine was built without the ability to type lowercase letters. Thanks to Tandy's chain of Radio Shack stores and the breakthrough price ($399 fully assembled and tested), the machine was successful enough to persuade the company to introduce a more powerful computer two years later, the TRS-80 Model II, which could reasonably be marketed as a small-business computer.

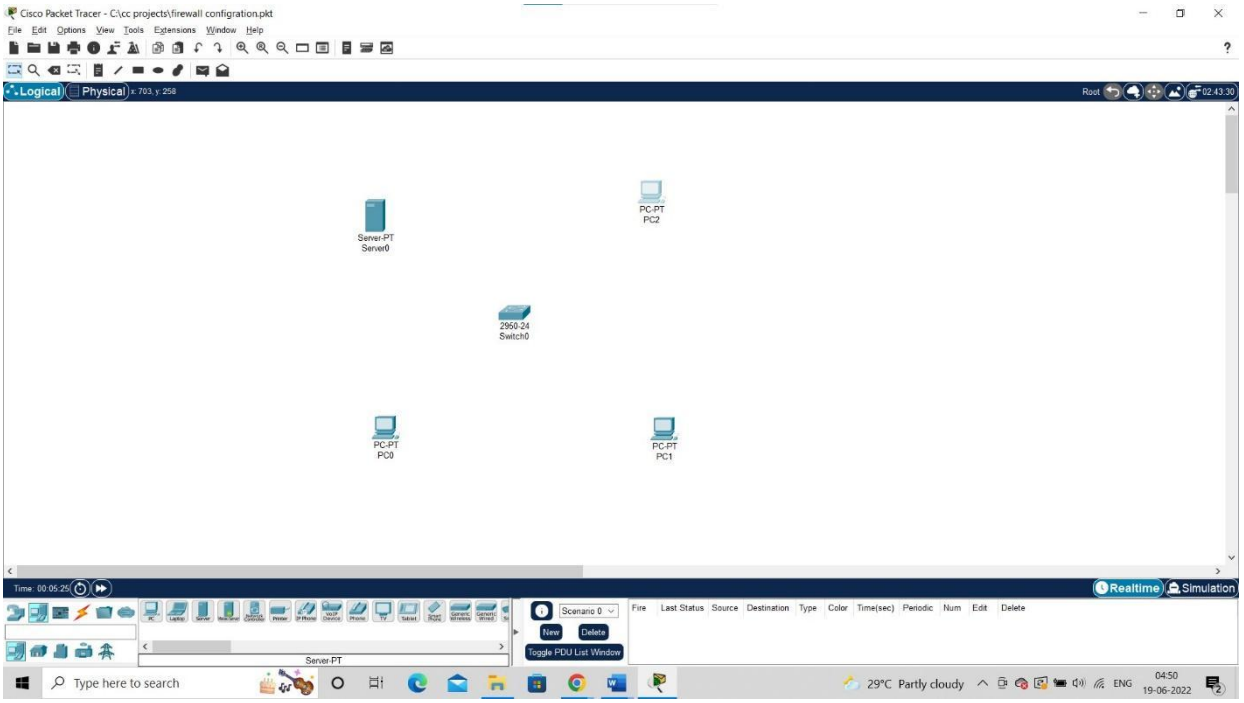
SIMULATION OF THE PROJECT:-

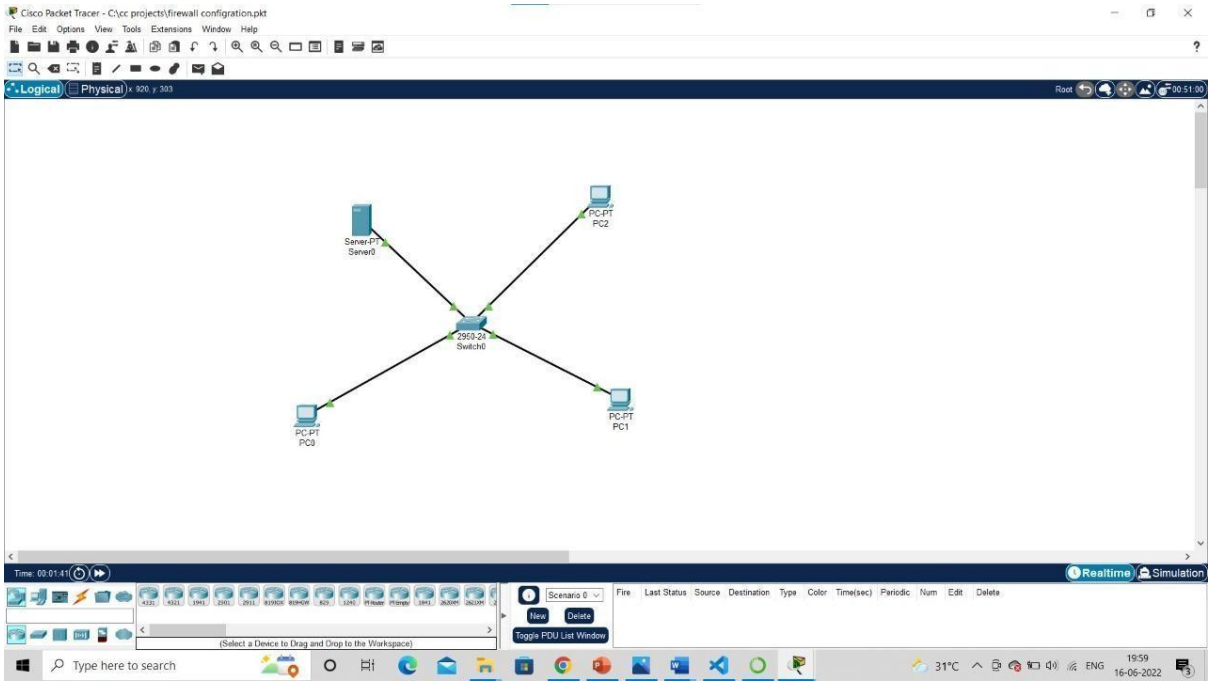


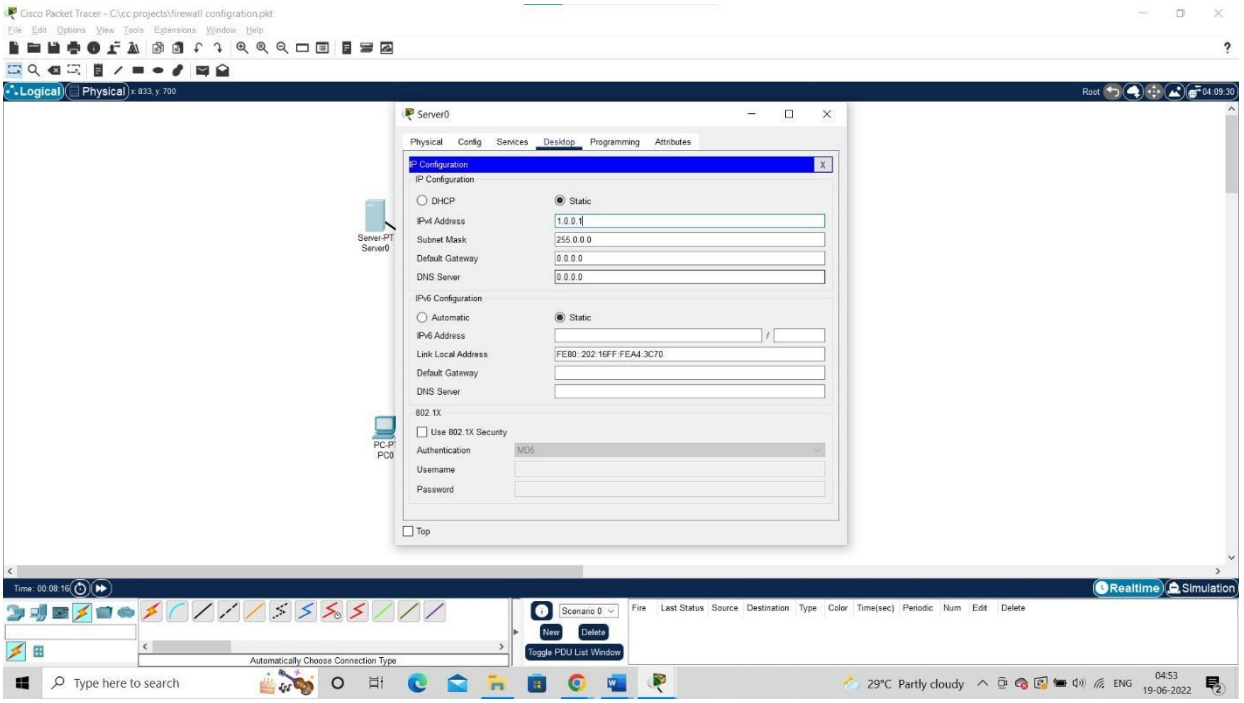


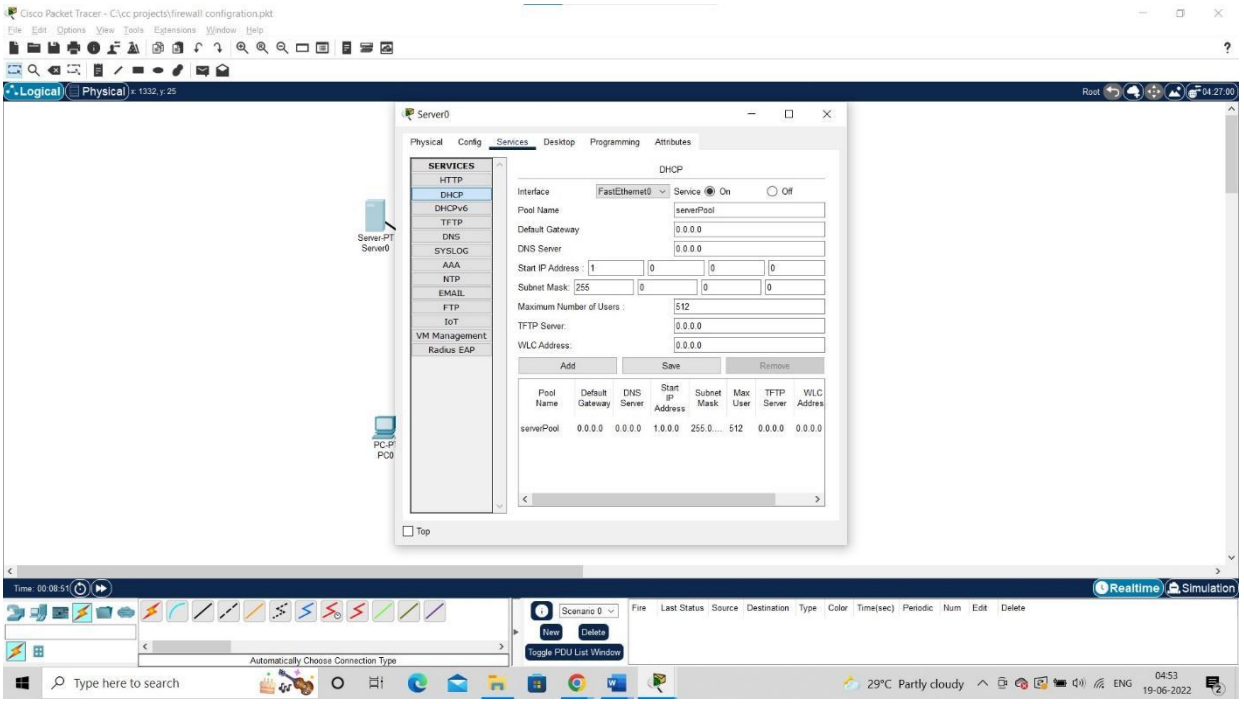

Cisco Packet Tracer - C:\cc projects\firewall configration.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 862, y: 151
Root 01:41:30
PC-PT PC2
PC-PT PC0
PC-PT PC1
Time: 00:03:22
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
PC-PT
Type here to search
29°C Partly cloudy
ENG
04:48
19-06-2022

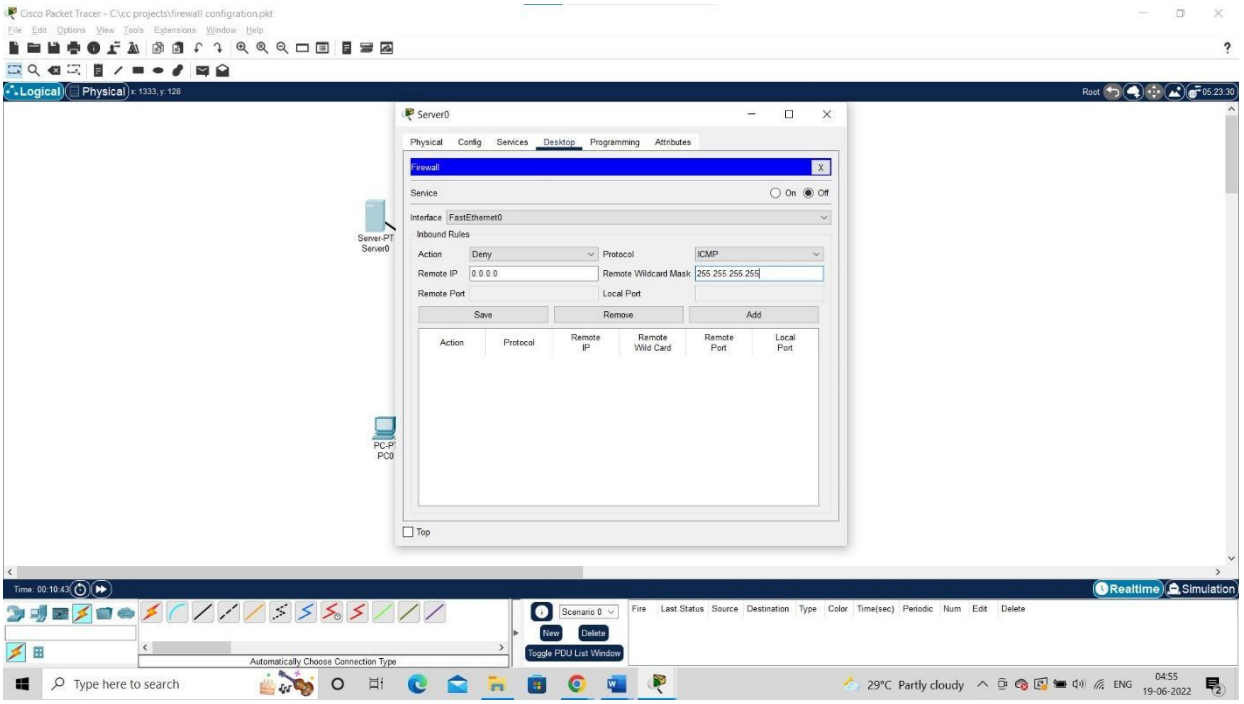

Cisco Packet Tracer - C:\cc projects\firewall configration.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 934, y: 358
Root 02:31:30
PC-PT PC2
2950-24 Switch0
PC-PT PC0
PC-PT PC1
Time: 00:05:02
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
2950-24
Type here to search
29°C Partly cloudy
ENG
04:49
19-06-2022

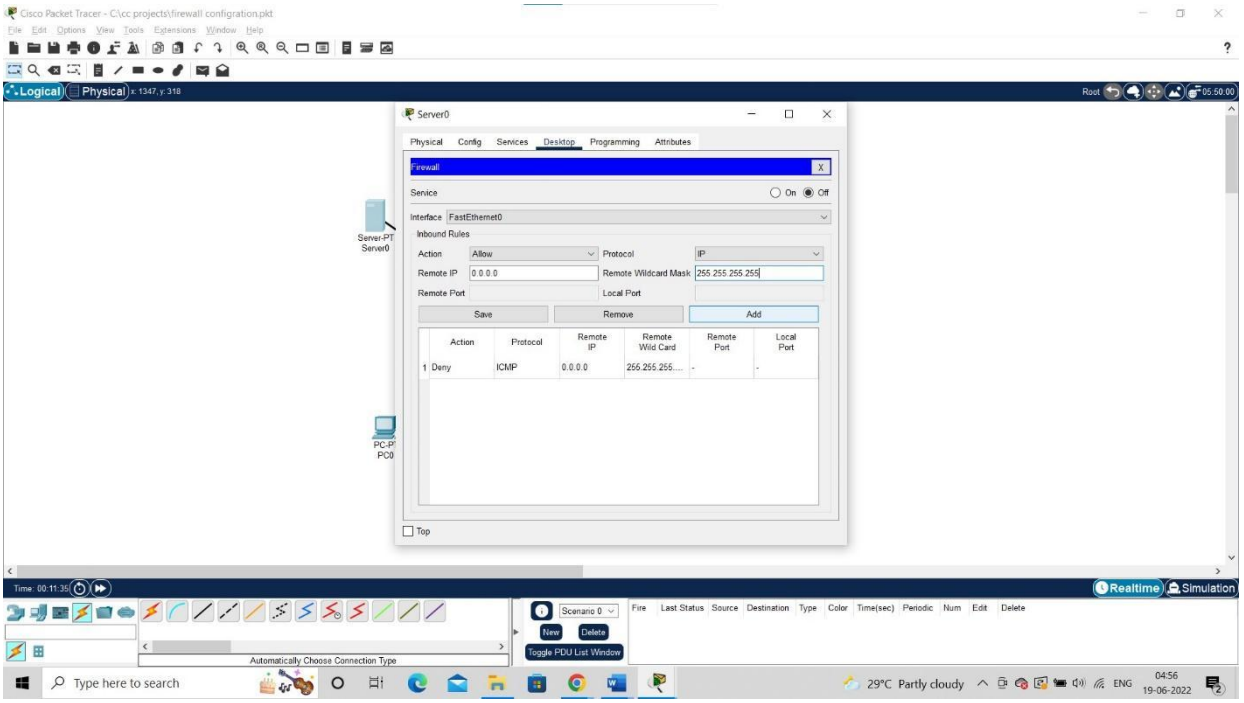

Cisco Packet Tracer - C:\cc projects\firewall configration.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x 703, y 258
Root 02:43:30
Server-PT Server0
PC-PT PC2
2950-24 Switch0
PC-PT PC0
PC-PT PC1
Time: 00:05:25
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Server-PT
Type here to search
29°C Partly cloudy
ENG
04:50
19-06-2022

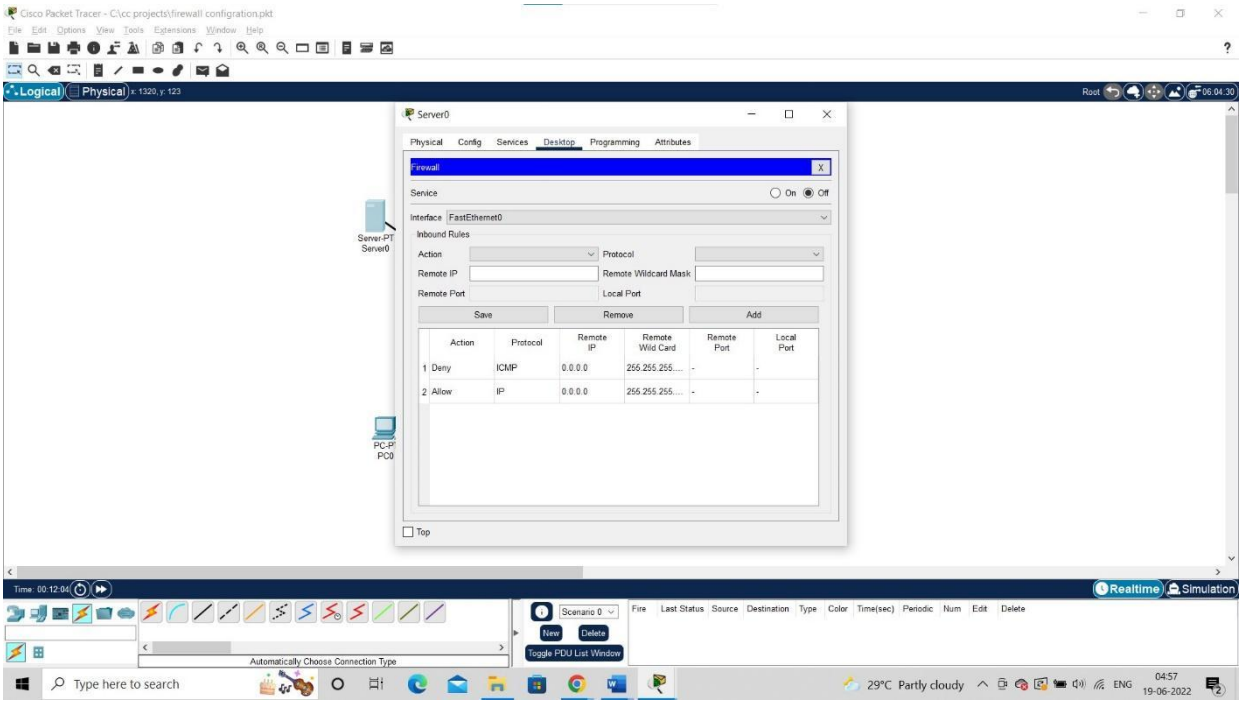

Cisco Packet Tracer - C:\cc projects\firewall configration.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x 920, y 303
Root 00:51:00
Server-PT Server0
PC-PT PC2
2950-24 Switch0
PC-PT PC0
PC-PT PC1
Time: 00:01:41
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
(Select a Device to Drag and Drop to the Workspace)
Type here to search
31°C
ENG
19:59
16-06-2022


Cisco Packet Tracer - C:\cc projects\firewall configration.pkt
Server0
Physical Config Services Desktop Programming Attributes
IP Configuration
DHCP
Static
IPv4 Address 1.0.0.1
Subnet Mask 255.0.0.0
Default Gateway 0.0.0.0
DNS Server 0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address FE80::202:16FF:FEA4:3C70
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication MD5
Username
Password
Top
Server-PT Server0
PC-PT PC0
Logical Physical
Realtime Simulation
Automatically Choose Connection Type
Type here to search
29°C Partly cloudy
ENG
04:53
19-06-2022

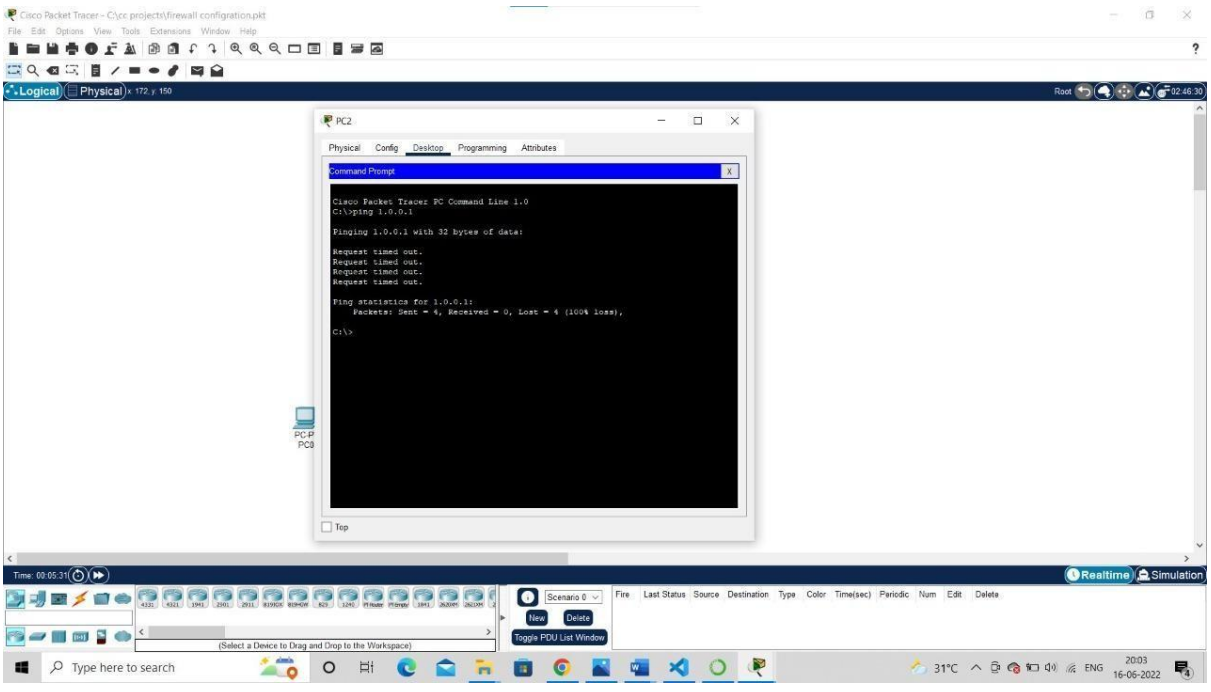

Cisco Packet Tracer - C:\cc projects\firewall configration.pkt
Server0
Physical Config Services Desktop Programming Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DHCP
Interface FastEthernet0 Service On Off
Pool Name serverPool
Default Gateway 0.0.0.0
DNS Server 0.0.0.0
Start IP Address : 1 0 0 0
Subnet Mask: 255 0 0 0
Maximum Number of Users : 512
TFTP Server: 0.0.0.0
WLC Address: 0.0.0.0
Add Save Remove
Pool Name Default Gateway DNS Server Start IP Address Subnet Mask Max User TFTP Server WLC Addres
serverPool 0.0.0.0 0.0.0.0 1.0.0.0 255.0.... 512 0.0.0.0 0.0.0.0
Top
Server-PT Server0
PC-PT PC0
Logical Physical
Realtime Simulation
Automatically Choose Connection Type
Type here to search
29°C Partly cloudy
ENG
04:53
19-06-2022

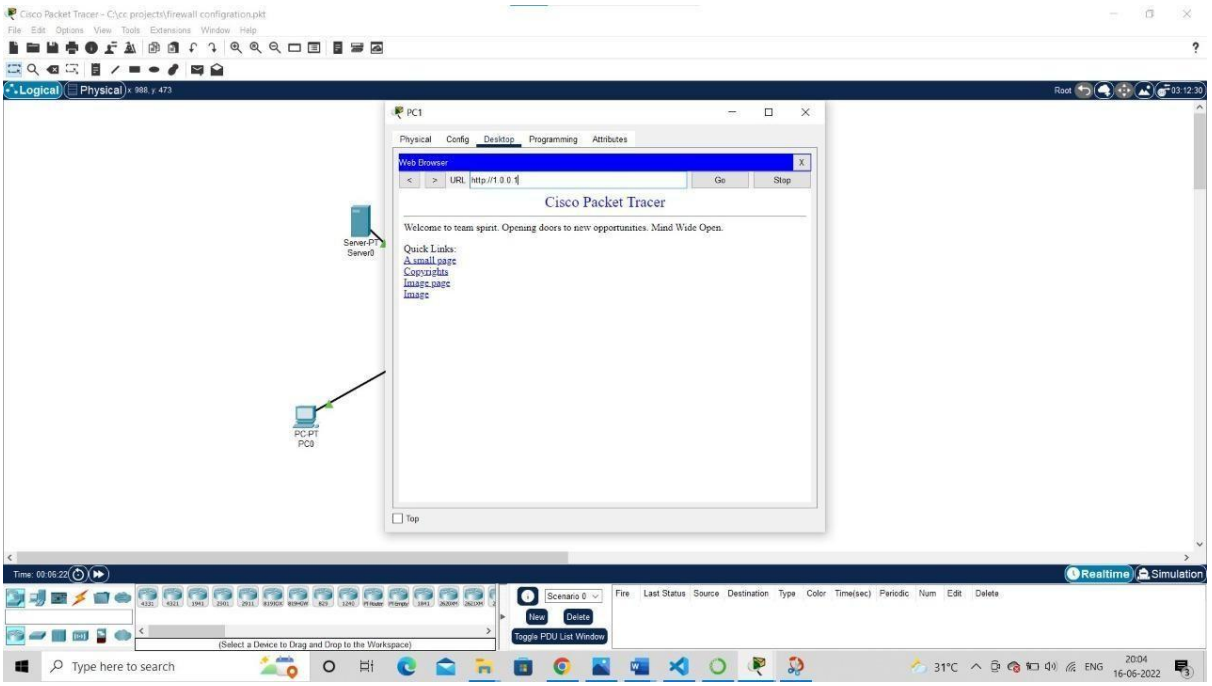

Cisco Packet Tracer - C:\cc projects\firewall configration.pkt
Server0
Physical
Config
Services
Desktop
Programming
Attributes
Firewall
Service
On
Off
Interface FastEthernet0
Inbound Rules
Action Deny
Protocol ICMP
Remote IP 0.0.0.0
Remote Wildcard Mask 255.255.255.255
Remote Port
Local Port
Save
Remove
Add
Action
Protocol
Remote IP
Remote Wild Card
Remote Port
Local Port
Top
Server-PT Server0
PC-PT PC0
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Type here to search
29°C Partly cloudy
ENG
04:55
19-06-2022


Cisco Packet Tracer - C:\cc projects\firewall configration.pkt
Server0
Physical
Config
Services
Desktop
Programming
Attributes
Firewall
Service
On
Off
Interface FastEthernet0
Inbound Rules
Action Allow
Protocol IP
Remote IP 0.0.0.0
Remote Wildcard Mask 255.255.255.255
Remote Port
Local Port
Save
Remove
Add
Action
Protocol
Remote IP
Remote Wild Card
Remote Port
Local Port
1 Deny ICMP 0.0.0.0 255.255.255.... - -
Top
Server-PT Server0
PC-PT PC0
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Type here to search
29°C Partly cloudy
ENG
04:56
19-06-2022


Cisco Packet Tracer - C:\cc projects\firewall configration.pkt
Server0
Physical
Config
Services
Desktop
Programming
Attributes
Firewall
Service
On
Off
Interface FastEthernet0
Inbound Rules
Action
Protocol
Remote IP
Remote Wildcard Mask
Remote Port
Local Port
Save
Remove
Add
Action
Protocol
Remote IP
Remote Wild Card
Remote Port
Local Port
1 Deny ICMP 0.0.0.0 255.255.255.... - -
2 Allow IP 0.0.0.0 255.255.255.... - -
Server-PT Server0
PC-PT PC0
Top
Logical
Physical
Realtime
Simulation
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Type here to search
29°C Partly cloudy
ENG
04:57
19-06-2022

OUTPUT:-


Cisco Packet Tracer - C:\cc projects\firewall configration.pkt
PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 1.0.0.1
Pinging 1.0.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 1.0.0.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
PC-PT PC0
Top
Logical
Physical
Realtime
Simulation
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New
Delete
Toggle PDU List Window
Type here to search
31°C
ENG
20:03
16-06-2022


Cisco Packet Tracer – C:\cc projects\firewall configration.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
PC1
Physical Config Desktop Programming Attributes
Web Browser
URL http://1.0.0.1
Go
Stop
Cisco Packet Tracer
Welcome to team spirit. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
Server-PT
Server0
PC-PT
PC0
Top
Time: 00:05:22
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
(Select a Device to Drag and Drop to the Workspace)
Type here to search
31°C
ENG
20:04
16-06-2022

CISCOPACKET TRACER:- we will first take four pcs namely pc0,pc1,pc2 and switch0 2950-24 and a server. We will change the mode of the server to DCPH protocol which provides the ip addresses for all the PCs connected to it. We will make use of the same server as a DHCP server and as a firewall and as well as web hosting. We will assign the ip address to the server as 1.0.0.1, and the IP address for the pc0 is 1.0.0.2 and the IP address for the pc1 is 1.0.0.3 and the IP address for the pc3 is 1.0.0.4 which will be automatically assigned by the server(DHCP/firewall/web host). We will note down all the IP addresses of the pc's. Our goal is to block the ICMP protocol(The ICMP stands for Internet Control Message Protocol. It is a network layer protocol. It is used for error handling in the network layer, and it is primarily used on network devices such as routers. As different types of errors can exist in the network layer, ICMP can be used to report these errors and to debug those errors.) so that no pc can access the server using the ping command. And we will allow the IP address for all the pc's. so that they can access the information through the website. And we will go to the server there, we will check for the DHCP address, and we will go to the index.html there will change some default things in the server. Now we will go to the main theme of our project, go to the firewall of IPv4(IPv4 stands for Internet Protocol version 4. It is the underlying technology that makes it possible for us to connect our devices to the web. Whenever a device accesses the Internet, it is assigned a unique, numerical IP address such as 99.48.227.227. To send data from one computer to another through the web, a data packet must be transferred across the network containing the IP addresses of both devices.) switch on the firewall and there, we will keep remote IP(Computers that connect to a TCP/IP network such as the Internet are assigned an IP address, a label consisting of 32-bits and represented in dotted-decimal notation, such as 192.168.0.1. PCs also have a host name, or computer name, composed of alphanumeric characters, which makes identification of a machine easier for users. If you need to perform maintenance on a workstation in your office but you don't remember the IP address of the PC, you can use the ping command to convert the PC's host name to an IP address.) as and we keep the action as **DENY** and the protocol you need to deny is **ICMP**, keep the remote subnet mask or remote wildcard mask (A **wildcard mask** is a mask of bits that indicates which parts of an IP address are available for examination. In the CISCO IOS they are used in several places) 255.255.255.255 . This is our first rule and the second rule is that we have to allow the IP address for the IP address 0.0.0.0 . actually 0.0.0.0 is to allow the IP address for all the pcs. Now all the things have been completed and now let's go and test it. Click on any pc[pc0,pc1,pc2] go to the desktop and click on command prompt and try to ping to the server using ping command 1.0.0.0.1 and check the output. We would not be able to ping to the server because the ICMP protocol is blocked which doesn't allow any pc to ping to the server. Now go to another pc and try ping to the server using the same technique yet you will not be able to ping to the server because of firewall and blocking of ICMP protocol. Now try connecting to the server using a web browser, open any pc[PC1,PC2,PC0]. And open web browser and type in search bar the address of the browser 1.0.0.1 you can able to see the outlay of the website which means that you can access to the server through the website as only the IP address is required to access the website, and as we have blocked the ping command so that we are not able to access the server directly.

INFERANCE:- thus we have a created server for whose firewall have been constructed by https://www.techtarget.com/searchsecurity/definition/firewallblocking ICMP protocol which doesn't allow the user or client or the customer to enter into the server and access the information but IP address is allowed in so we can able to access the information present inside the server.

REFERANCE:-

1) https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/#:~:text=A%20Firewall%20is%20a%20network,network%20and%20the%20public%20Internet.
2) https://www.kaspersky.co.in/resource-center/definitions/firewall
3) https://www.techtarget.com/searchsecurity/definition/firewall
4) https://www.routerfreak.com/basic-configuration-tutorial-cisco-asa-5505-firewall/
5) https://www.routerfreak.com/basic-configuration-tutorial-cisco-asa-5505-firewall/