

# Module-2

## **Security Device Management**

## **Module-2: Security Device Management**

- Different types of information security devices and their functions
- Technical and configuration specifications, architecture concepts
- Design patterns and how these contribute to the security of design and devices.

# **Module-2: Security Device Management**

**Different types of information security devices and their functions**

# **Information Security Management**

1. Access control
2. Antivirus and anti-malware software
3. Application security
4. Behavioral analytics
5. Data loss prevention
6. Distributed denial of service prevention
7. Email security
8. Firewalls
9. Mobile device security
10. Network segmentation
11. Security information and event management
12. Web security

# Types of information security devices

## 1. Access control

- This refers to **controlling which users have access to the network** or especially sensitive sections of the network.
- Using **security policies**, you can restrict network access to **only recognized users and devices** or **grant limited access to noncompliant devices or guest users**.

# Types of information security devices

## 2. Antivirus and anti-malware software

- Malware, or “malicious software,” is a common form of cyber attack that comes in **many different shapes and sizes**.
- Some variations work quickly to **delete files or corrupt data**, while others can lie dormant for **long periods of time** and **quietly allow hackers a back door into your systems**.
- The **best antivirus software will monitor network traffic** in real time for malware, scan activity log files for signs of suspicious behavior or long-term patterns, and offer threat remediation capabilities.

# Types of information security devices

## 3.Application security.

- Each device and software product used within your **networking environment** offers a potential way in for hackers.
- For this reason, it is important that **all programs be kept up-to-date** and patched to prevent cyber attackers from exploiting vulnerabilities to access sensitive data.
- Application security refers to the **combination of hardware, software, and best practices** you use to monitor issues and close gaps in your security coverage.

# Types of information security devices

## 4. Behavioral analytics

- In order to **identify abnormal behavior**, security support **personnel** need to establish a baseline of what constitutes **normal behavior for a given customer's users, applications, and network.**
- Behavioral analytics software is designed to help identify **common indicators of abnormal behavior**, which can often be a sign that a security breach has occurred.



# Types of information security devices

## 5.Data loss prevention

- Data loss prevention (DLP) technologies are those that **prevent an organization's employees from sharing valuable company information** or sensitive data
- DLP technologies can prevent actions that could potentially **expose data to bad actors outside** the networking environment, such as uploading and downloading files, forwarding messages, or printing.

# Types of information security devices

## 6. Distributed denial of service prevention

- Distributed denial of service (DDoS) attacks are becoming increasingly common.
- They function by **overloading a network with one-sided connection requests** that eventually cause the network to crash.
- A DDoS prevention tool scrubs incoming traffic to remove nonlegitimate traffic that could threaten your network, and may consist of a hardware appliance that works to filter out traffic before it reaches your firewalls.

# Types of information security devices

## 7. Email security

- Email is an especially important factor to consider when implementing networking security tools.
- Numerous threat vectors, like **scams, phishing, malware, and suspicious links**, can be attached to or incorporated into emails.
- Because so many of these threats will often use elements of personal information in order to appear more convincing, it is important to ensure an **organization's employees undergo sufficient security awareness training to detect when an email is suspicious.**
- Email security software works to filter out **incoming threats and can also be configured to prevent outgoing messages from sharing certain forms of data.**

# Types of information security devices

## 8. Firewalls

- Firewalls are another common element of a network security model.
- They essentially function as a **gatekeeper** between a **network and the wider internet**.
- Firewalls **filter incoming** and, in some cases, **outgoing traffic** by comparing data packets **against predefined rules** and policies, thereby preventing threats from accessing the network.

# Types of information security devices

## 9. Mobile device security

- The vast majority of us have mobile devices that **carry some form of personal or sensitive data** we would like to keep protected.
- This is a fact that hackers are aware of and can easily take advantage of. Implementing mobile device security measures can limit device access to a network, which is a necessary step to ensuring network traffic stays private and doesn't leak out through vulnerable mobile connections.

# Types of information security devices

## 10. Network segmentation

- **Dividing and sorting network traffic** based on certain **classifications** streamlines the job for security support personnel when it comes to applying policies.
- **Segmented networks** also make it easier **to assign or deny authorization credentials for employees**, ensuring no one is accessing information they should not be.
- Segmentation also helps to sequester potentially compromised devices or intrusions.

# Types of information security devices

## 11. Security information and event management

- These security systems (called SIEMs) combine host-based and network-based **intrusion detection systems** that combine **real-time network traffic monitoring** with **historical data** log file scanning to provide administrators with a comprehensive picture of all activity across the network.

# **Types of information security devices**

## **11.Security information and event management**

- An IPS can also **log security events** and send notifications to the necessary players in the interest of keeping network administrators informed.



# Types of information security devices

## 12.Web security

- Web security software serves a few purposes.
- First, it **limits internet access for employees**, with the intention of **preventing them from accessing sites that could contain malware**.
- It also blocks other web-based threats and works to protect a customer's web gateway.

# Module-2

## **Security Device Management**

# **Configuring Firewall**

- **What firewall software does?**
  - A firewall is simply a program or hardware device that filters the information coming through the internet connection into your private network or computer system.
  - If an incoming packet of information is flagged by the filters, it is not allowed through.

# Configuring Firewall

- Firewalls use one or more of **three methods** to control traffic flowing in and out of the network:
  - **Packet filtering**
  - **Proxy service**
  - **Stateful inspection**

# Configuring Firewall

- Packet Filtering
  - Packets (small chunks of data) are analyzed against a set of filters. Packets that make it through the filters are **sent to the requesting system** and **all others are discarded**.

# Configuring Firewall

- **Proxy service**

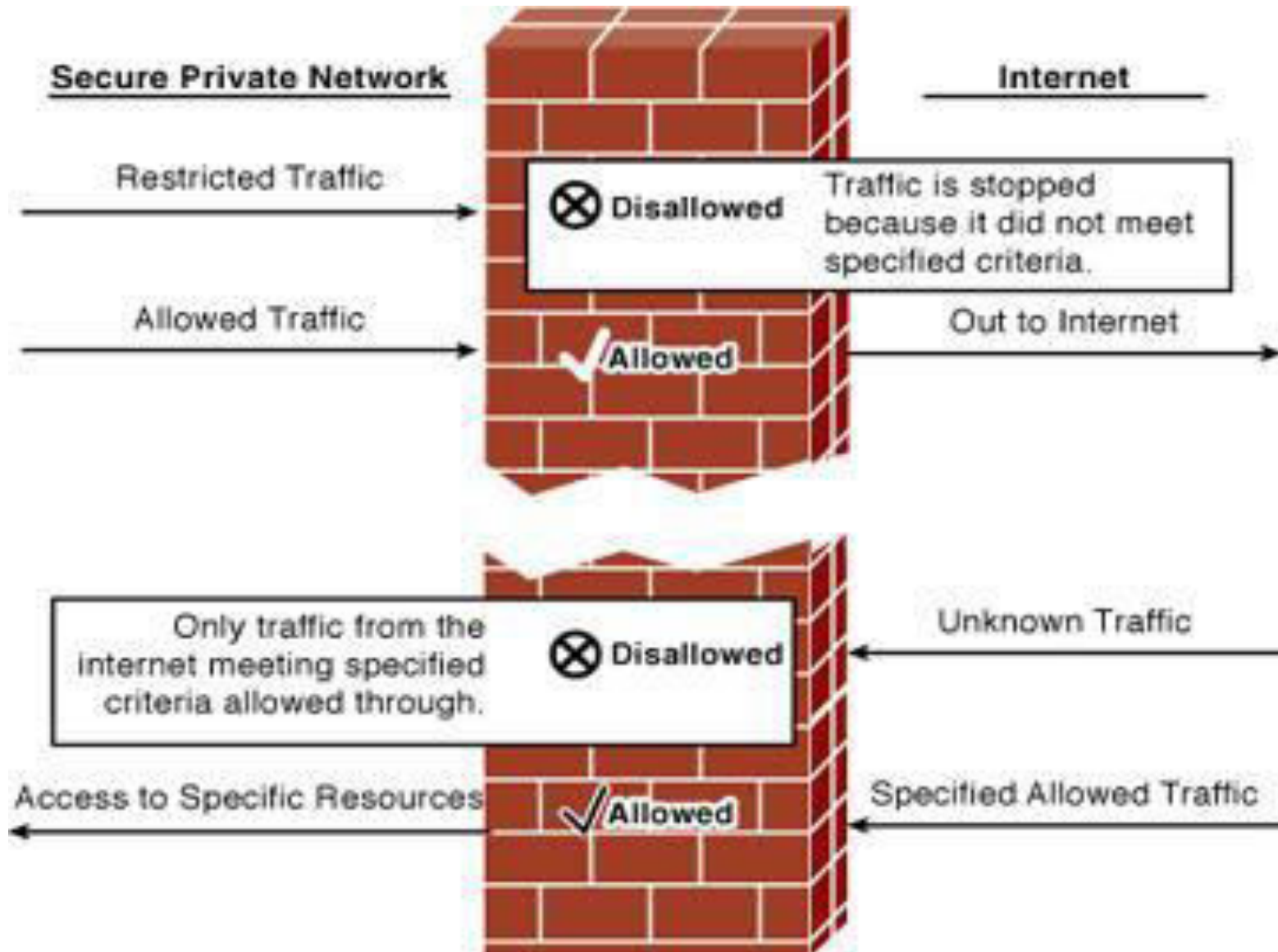
- Information from the internet is **retrieved by the firewall and then sent to the requestingsystem** and vice versa.

# Configuring Firewall

- **Stateful Inspection**

- A newer method that **doesn't examine the contents of each packet** but instead **compares certain key parts of the packet to a database of trusted information.**
- Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics.
- If the comparison yields a **reasonable match, the information is allowed through.** Otherwise it is discarded.

# Working of firewall





# **Firewall SOFTWARE CONFIGURATION**

- Firewalls are customizable. This means that you can add or remove filters based on several conditions. Some of these are:
  - **IP addresses**
  - **Domain names**
  - **Protocols**

# Firewall SOFTWARE CONFIGURATION

- **IP addresses**

- Each machine on the Internet is assigned a **unique address called an IP address.**
- IP addresses **are 32- bit numbers**, normally expressed as **four "octets" in a "dotted decimal number."**
- A typical IP address looks like this: 216.27.61.137. For example, if a certain IP address outside the company is reading too many files from a server, the **firewall can block all traffic to or from that IP address.**

# Firewall SOFTWARE CONFIGURATION

- **Domain names**

- As it is hard to remember the string of numbers that make up an IP address, and because IP addresses sometimes need to change, all servers on the Internet also have **human-readable names, called domain names**
- For example, it is easier for most of us to remember **www.howstuffworks.com** than it is to remember **216.27.61.137**.
- A company might block all access to certain domain names, or allow access only to specific domain names.

# Firewall SOFTWARE CONFIGURATION

- **Protocols**

- The protocol is the pre-defined way that someone who wants to use a service talks with that service.
- The "someone" could be a person, but more often it is a computer program like a Web browser.
- Protocols are often text, and simply describe how the client and server will have their conversation.
- Eg: **http** in the Web's protocol.
- A company might set up only one or two machines to handle a specific protocol and ban that protocol on all other machines.

# Firewall SOFTWARE CONFIGURATION

- **Protocols**

- Some common protocols that you can set firewall filters for include:

- **IP (Internet Protocol)**
    - **TCP (Transmission Control Protocol)**
    - **HTTP (Hyper Text Transfer Protocol)**
    - **FTP (File Transfer Protocol)**
    - **UDP (User Datagram Protocol)** teletype network
    - **ICMP (Internet Control Message Protocol)**
    - **SMTP (Simple Mail Transport Protocol)**
    - **SNMP (Simple Network Management Protocol)**
    - **Telnet (Teletype Network)**

# Why Firewall Security?

- **Access or abuse of unprotected computers**
  - There are many creative ways that unscrupulous people use to access or abuse unprotected computers:
    - **Remote login**
    - **Application backdoors**
    - **SMTP session hijacking**
    - **Operating system bugs**
    - **Denial of service**
    - **E-mail bombs**
    - **Macros**
    - **Viruses**
    - **Spam**
    - **Redirect bombs**
    - **Source routing**

# Why Firewall Security?

- **Remote Login**

- **When someone is able to connect to your computer and control it in some form.**
- **This can range from being able to view or access your files to actually running programs on your computer.**

# Why Firewall Security?

- **Application backdoors**

- Some programs have special features that allow for remote access.
- Others contain bugs that provide a backdoor, or hidden access that provides some level of control of the program.



# Why Firewall Security?

- **SMTP session hijacking**

- SMTP is the most common method of sending e-mail over the Internet.
- By gaining access to a list of e-mail addresses, a person can **send unsolicited junk e-mail** (spam) to thousands of users.
- This is done quite often by redirecting the e-mail through the SMTP server of an unsuspecting host, making the actual sender of the spam difficult to trace.

# Why Firewall Security?

- **Operating system bugs**
  - Like applications, **some operating systems have backdoors.**
  - Others provide remote access with insufficient security controls or have bugs that an experienced hacker can take advantage of.

# Why Firewall Security?

- **Denial of service**

- What happens is that the **hacker sends a request to the server to connect to it.**
- When the server responds with an acknowledgement and tries to establish a session, it cannot find the system that made the request. By inundating a server with these unanswerable session requests, a hacker causes the server to slow to a crawl or eventually crash.

# Why Firewall Security?

- **E-mail bombs**

- An **e-mail bomb** is usually a personal attack.
- Someone sends you the same e-mail hundreds or thousands of times until your e-mail system cannot accept any more messages.

# Why Firewall Security?

- **Macros**

- To simplify complicated procedures, many applications allow you to create a **script of commands that the application can run**. This script is known as a **macro**.
- Hackers have taken advantage of this to create their own macros that, depending on the application, can destroy your data or crash your computer.

# Why Firewall Security?

- **Viruses**

- Probably the most well-known threat is computer viruses.
- A virus is a small program that **can copy itself to other computers**. This way it can spread quickly from one system to the next. Viruses range from harmless messages to erasing all of your data.

# Why Firewall Security?

- **Spam**

- Typically, harmless but always annoying, **spam is the electronic equivalent of junk mail.**
- Spam can be dangerous though.
- Quite often it contains links to Web sites.
- Be careful of clicking on these because you may accidentally accept a cookie that provides a backdoor to your computer.

# Why Firewall Security?

- **Redirect bombs**

- Hackers can use ICMP to change (redirect) the path information takes by sending it to a different router.
- This is **one of the ways that a denial of service** attack is set up.



# Why Firewall Security?

- **Source routing**

- In most cases, the path a packet travels over the **Internet** (or any other network) is determined by **the routers along that path.**
- But the **source providing the packet can arbitrarily specify the route that the packet should travel.**
- Hackers sometimes take advantage of this to make information appear to come from a trusted source or even from inside the network! Most firewall products disable source routing by default.

# Why Firewall Security?

- **Security against unauthorized access or abuse**
  - Some of the items in the list above are hard, if not impossible, to filter using a firewall.
  - While **some firewalls offer virus protection**, it is worth the investment to install anti-virus software on each computer.
  - The **level of security you establish** will determine **how many of these threats can be stopped** by your firewall.
  - You can also **restrict traffic that travels** through the firewall so that only certain types of information, such as e-mail, can get through.
  - This is a good rule for businesses that have an **experienced network administrator that understands what the needs are and knows exactly** what traffic to allow through.
  - One of the best things about a firewall from a security standpoint is that it stops anyone on the outside from logging onto a computer in your private network.

## **Proxy Servers and DMZ**

- There are times that you may want remote users to have access to items on your network. Some examples are:
  - **Web site**
  - **Online business**
  - **FTP download and upload area**

# Proxy Servers and DMZ

- DMZ is just an area that is outside the firewall.
- Think of DMZ as the front yard of a house.
- It belongs to the owner, who may put some things there, but would put anything valuable inside the house where it can be properly secured.
- Setting up a DMZ is very easy.
- If you have multiple computers, you can choose to simply place **one of the computers between the Internet connection and the firewall**. Most of the software firewalls available will allow you to designate a directory on the gateway computer as a DMZ.

# Configuring a Simple Firewall

- Server Firewall

# Firewall Limitations

- A firewall cannot prevent users or attackers with modems from dialing into or out of the internal network, thus bypassing the firewall and its protection completely.
- Firewalls cannot enforce your password policy or prevent misuse of passwords. Your password policy is crucial in this area because it outlines acceptable conduct and sets the ramifications of noncompliance.
- Firewalls are ineffective against nontechnical security risks such as social engineering.
- Firewalls cannot stop internal users from accessing websites with malicious code, making user education critical.
- Firewalls cannot protect you from poor decisions.
- Firewalls cannot protect you when your security policy is too lax.

# Module-2

## **Security Device Management**

# Configuration Tasks

- Configure Access Lists
- Configure Inspection Rules
- Apply Access Lists and Inspection Rules to Interfaces



# Configuration Tasks

- Standard Access Control List

# Configuration Tasks

- [Extended Access Control List](#)

# Configure Access Lists

Perform these steps to create access lists for use by the firewall, beginning in global configuration mode:

## ➤ Step 1

### Command

**access-list** access-list-number {**deny** | **permit**} protocol  
source source-wildcard [ **operator** [port]] destination

### Example

```
Router(config)# access-list 103 permit host 200.1.1.1 eq  
isakmp any  
Router(config)#
```

### Purpose

Creates an access list which prevents Internet-initiated traffic from reaching the local (inside) network of the router, and which compares source and destination ports.

# Configure Access Lists

## ➤ Step 2

### Command

```
access-list access-list-number {deny | permit} protocol  
source source-wildcard destination destination-wildcard
```

### Example

```
Router(config)# access-list 105 permit ip 10.1.1.0 0.  
0.0.255 192.168.0.0 0.0.255.255  
Router(config)#
```

### Purpose

Creates an access list to control network traffic to and from the corporate network between the corporate network and the local network. This is used to control the configured VPN traffic.

# Configure Inspection Rules

Perform these steps to configure firewall inspection rules for all TCP and UDP traffic, as well as specific application protocols as defined by the security policy, beginning in global configuration mode:

## ➤ Step 1

### Command

```
ip inspect name inspection-name protocol
```

### Example

```
Router(config)# ip inspect  
name firewall tcp  
Router(config)#
```

### Purpose

Defines an inspection rule for particular protocol.

# Apply Access Lists and Inspection Rules to Interfaces

Perform these steps to apply the ACLs and inspection rules to the network interfaces, beginning in global configuration mode:

## Step 1

### Command

**interface** type number

### Example

Router(config)# interface vlan 1

Router(config-if)#

### Purpose

Enters interface configuration mode for the inside network interface on your router.

# Apply Access Lists and Inspection Rules to Interfaces

## ➤ Step 2

### Command

```
ip inspect inspection-name { in | out }
```

### Example

```
Router(config-if)# ip inspect firewall in  
Router(config-if)#
```

### Purpose

Assigns the set of firewall inspection rules to the inside interface on the router.

# Apply Access Lists and Inspection Rules to Interfaces

## Step 3

### Command

**Exit**

### Example

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

```
Router(config)#
```

### Purpose

Returns to global configuration mode.



# Apply Access Lists and Inspection Rules to Interfaces

## ➤ Step 4

### Command

**interface** type number

### Example

Router(config)# interface fastethernet 0

Router(config-if)#

### Purpose

Enters interface configuration mode for the outside network interface on your router.

# Apply Access Lists and Inspection Rules to Interfaces

## Step 5

### Command

```
ip access-group { access-list-number  
| access-list-name } { in | out }
```

### Example

```
Router(config-if)# ip access-group 103  
in  
Router(config-if)#
```

### Purpose

Assigns the defined ACLs to the outside interface on the router..

# Apply Access Lists and Inspection Rules to Interfaces

## ➤ Step 6

### Command

**exit**

### Example

Router(config-if)# exit

Router(config)#

### Purpose

Returns to global configuration mode.

# Configure Inspection Rules

## ➤ Step 2

### Command

**ip inspect name** inspection-name protocol

### Example

```
Router(config)# ip inspect  
name firewall rtsp
```

```
Router(config)# ip inspect  
name firewall h323
```

```
Router(config)# ip inspect  
name firewall netshow
```

```
Router(config)# ip inspect  
name firewall ftp
```

```
Router(config)# ip inspect  
name firewall sqlnet
```

```
Router(config)#
```

### Purpose

Repeat this command for each inspection rule that you wish to use.

## Access Control Lists

### Standard ACL

#### Procedure:

Step 1. Choose three pcs and configure IP's with 192.168.10.1, 192.168.10.2, 192.168.10.3

Step 2: Connect the switch with these pcs

Step 3: connect the router with the switch and server

Step 4. Gateway for router from switch as 192.168.10.10 and from server 10.10.10.10

Open the router CLI and configure gateway as

-- System Configuration Dialog ---

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

Press RETURN to get started!

```
Router>enable
```

```
Router#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#interface gigabitethernet 0/0
```

```
Router(config-if)#ip address 192.168.10.10 255.255.255.0
```

```
Router(config-if)#no shutdown
```

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

```
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

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

```
Router(config)#interface gigabitethernet 0/1
```

```
Router(config-if)#ip address 10.10.10.10 255.0.0.0
```

```
Router(config-if)#no shutdown
```

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

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Step 5: Give this gateway address 192.168.10.10 in PCs and 10.10.10.10 in Server. Keep the server IP as 10.10.10.11

Step 6. Now ping the server from the pc's and check the packets sent from pc's to server

### Now create the ACL

```
Router(config-if)#exit
Router(config)#ip access-list ?
extended Extended Access List
standard Standard Access List
Router(config)#ip access-list standard?
standard
Router(config)#ip access-list standard ?
<1-99> Standard IP access-list number
WORD Access-list name
Router(config)#ip access-list standard 11
Router(config-std-nacl)#?
<1-2147483647> Sequence Number
default Set a command to its defaults
deny Specify packets to reject
exit Exit from access-list configuration mode
no Negate a command or set its defaults
permit Specify packets to forward
remark Access list entry comment
Router(config-std-nacl)#deny ?
A.B.C.D Address to match
any Any source host
host A single host address
Router(config-std-nacl)#deny host?
host
Router(config-std-nacl)#deny host ?
A.B.C.D Host address
Router(config-std-nacl)#deny host 192.168.10.1
Router(config-std-nacl)#permit ?
A.B.C.D Address to match
any Any source host
host A single host address
Router(config-std-nacl)#permit host ?
A.B.C.D Host address
Router(config-std-nacl)#permit host 192.168.10.2
Router(config-std-nacl)#exit
Router(config)#interface gigabitethernet 0/0
Router(config-if)#ip access-group 11
```

% Incomplete command.

Router(config-if)#ip access-group 11 in

Router(config-if)#exit

Router(config)#exit

Router#

%SYS-5-CONFIG\_I: Configured from console by console

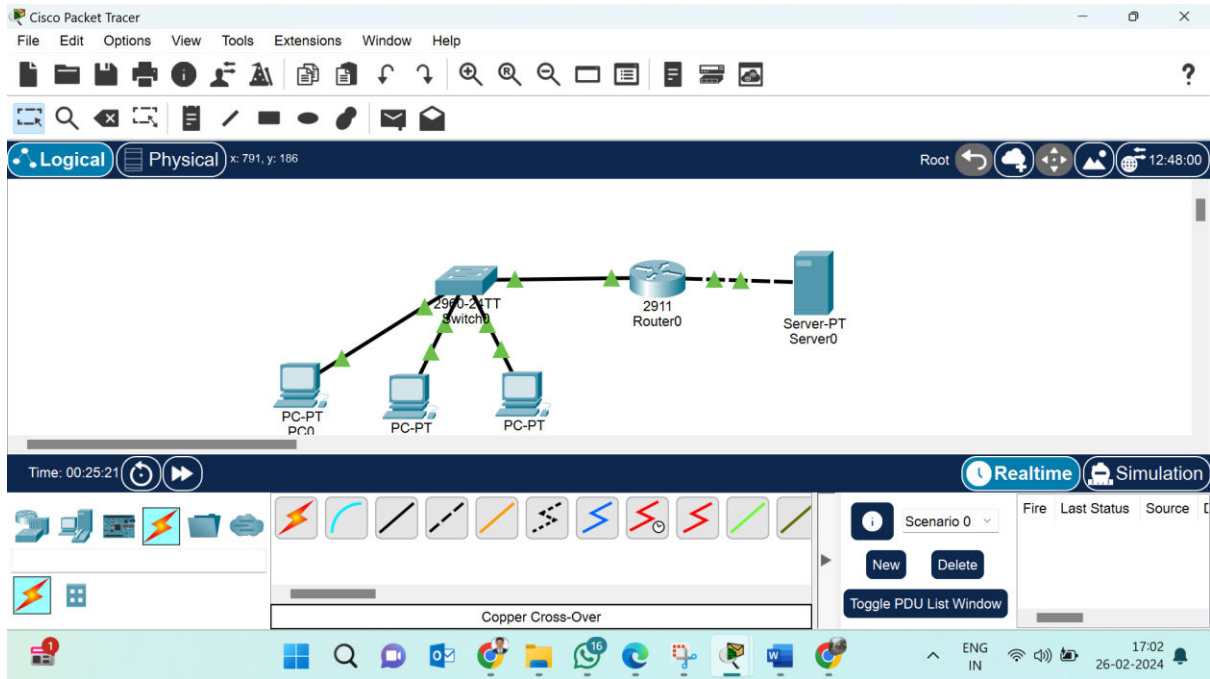
Router#show access-lists 11

Standard IP access list 11

deny host 192.168.10.1

permit host 192.168.10.2

Router#





## EXPERIMENT NO.5

### Extended ACL

#### PROBLEM STATEMENT:

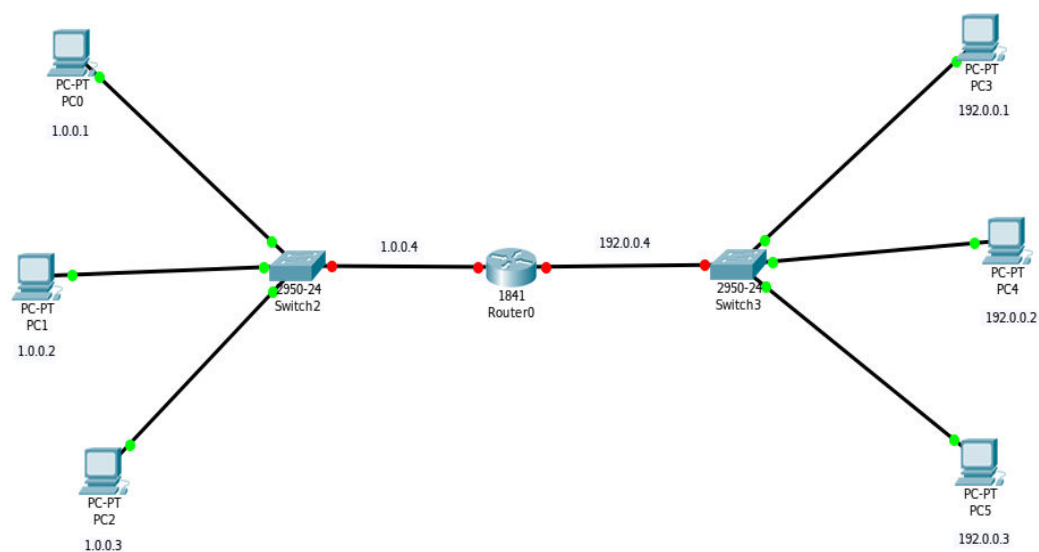
Configure the below network with Extended ACL in packet tracer.

#### CONCEPT TO BE APPLIED:

Use CISCO Packet tracer simulation tool and create the necessary topology with required PCs, Switch and a Router along with a server PT for implementing extended ACL

Implementing Extended **ACL** in packet tracer

#### Network Connection:



#### Steps:

- 1) Establish a topology

of network as above. (Routers are connected with Serial DCE wire)

2) Setup Extended Access-List in Router.

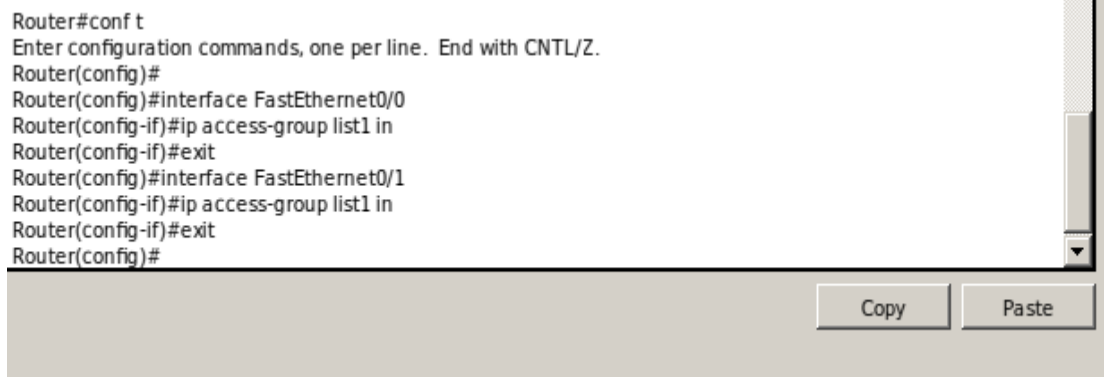
**Commands:**

```
Router(config)#ip access-list extended list1
Router(config-ext-nacl)#deny tcp 192.0.0.2 255.255.255.0 host 1.0.0.1
Router(config-ext-nacl)#permit ip 10.0.0.0 0.255.255.255 20.0.0.0 0.255.255.255
Router(config-ext-nacl)#deny tcp 192.0.0.2 255.255.255.0 host 1.0.0.1
Router(config-ext-nacl)#exit
```

3) Set the Commands up, in Router.

**Commands:**

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group list1 in
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group list1 in
Router(config-if)#exit
Router(config)#exit
```



```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group list1 in
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group list1 in
Router(config-if)#exit
Router(config)#
```

Copy

Paste

## Result:

Ping from PC-0 to PC-3 (before Extended-ACL implementation):

```
PC>ping 192.0.0.1

Pinging 192.0.0.1 with 32 bytes of data:

Reply from 192.0.0.1: bytes=32 time=0ms TTL=127
Reply from 192.0.0.1: bytes=32 time=0ms TTL=127
Reply from 192.0.0.1: bytes=32 time=0ms TTL=127
Reply from 192.0.0.1: bytes=32 time=0ms TTL=127

Ping statistics for 192.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping from PC-0 to PC-3 (after Extended-ACL implementation):

```
PC>ping 192.0.0.1

Pinging 192.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```



## 12.Firewall

Firewall is a network security device that monitors all incoming and outgoing traffic based on a defined set of security rules.

**PROBLEM STATEMENT:** Basic Firewall Configuration in Cisco Packet Tracer

### CONCEPT TO BE APPLIED:

Use CISCO Packet tracer simulation tool and create the necessary topology with required PCs, Switch and Server.

### PROCEDURE:

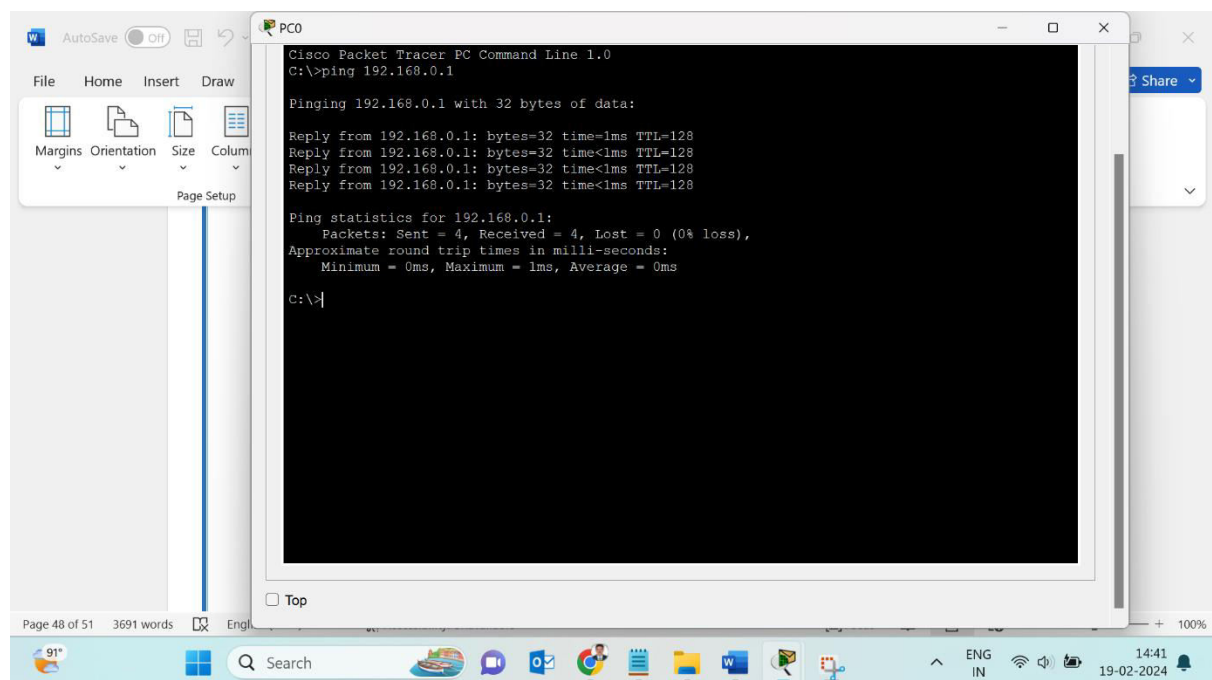
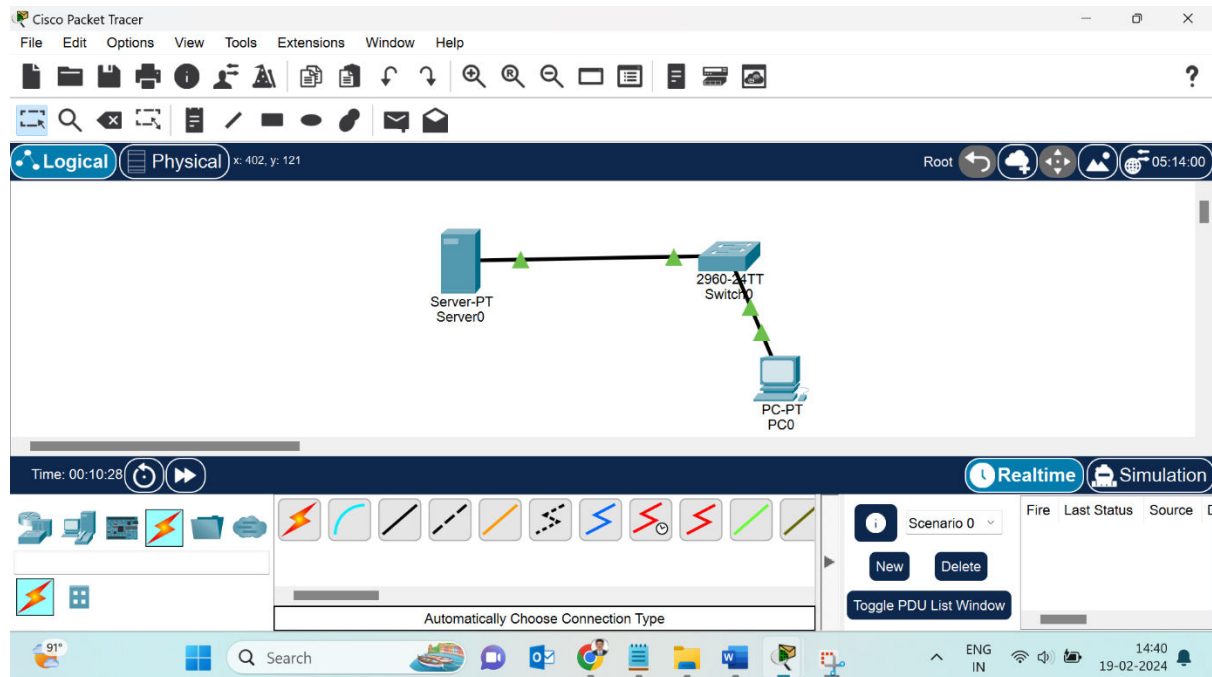
1. First, open the Cisco packet tracer desktop and select the devices given below: • PC - 1 • PT-Server - 1 • PT-Switch – 1
2. Create a network topology
3. Configure the PCs and server with IPv4 address and Subnet Mask according to the IP address
4. Assign an IP address in PC0, PC1, PC2, server
5. Then, go to desktop and then IP configuration.
6. Fill IPv4 address and subnet mask.
7. Repeat the same procedure with the server.
8. Click on server0 then go to the desktop.
9. Then click on firewall IPv4, Turn on the services.
10. First, **Deny** the **ICMP** protocol and set remote IP to 0.0.0.0 and Remote wildcard mask to 255.255.255.255.
11. Then, **allow** the **IP protocol** and set remote IP to 0.0.0.0 and Remote wildcard mask to 255.255.255.255, And add them.
12. We will use the ping command to do so.

13. First, click on PC2 then Go to the command prompt.

14. Then type ping .

15. We will ping the IP address of the server0.

16. As we can see in the below image we are getting no replies which means the packets are blocked. 17. Click on PC2 and go to desktop then web browser



SERVER 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	255.255.255.255	-	-
2	Allow	IP	0.0.0.0	255.255.255.255	-	-

RESULT:

ICMP PROTOCOL DENIED:

```
PC0
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

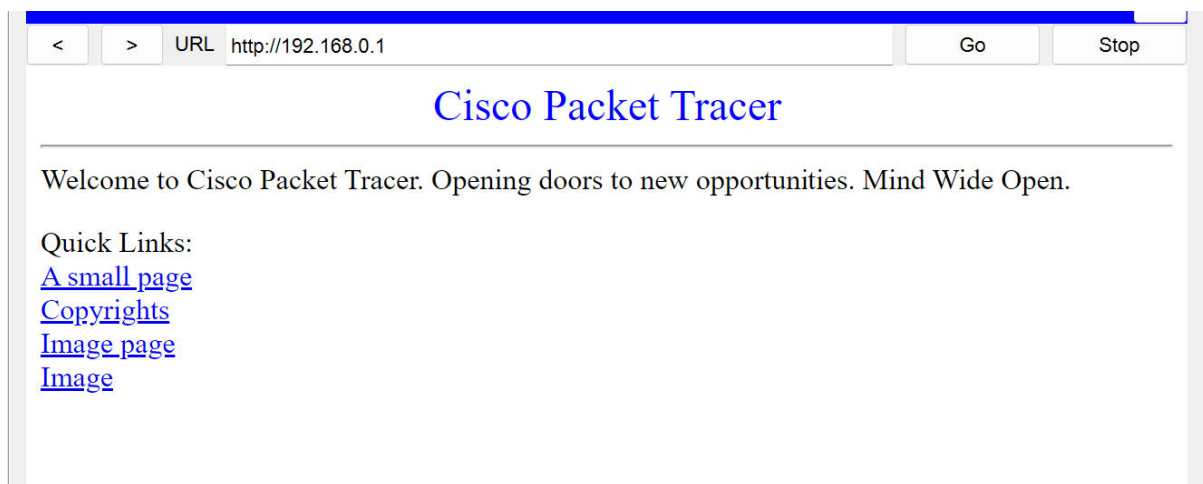
Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
```

#### IP PROTOCOL ALLOWED:





For the above implemented network design, ICMP protocols are denied when the server is pinged and the IP protocols are allowed while PC2 with IP address opens a web browser. Thus, firewall plays its role with accepting, denying or by dropping that specific traffic.