Module 05

Network Security Controls - Technical Controls

Module Objectives

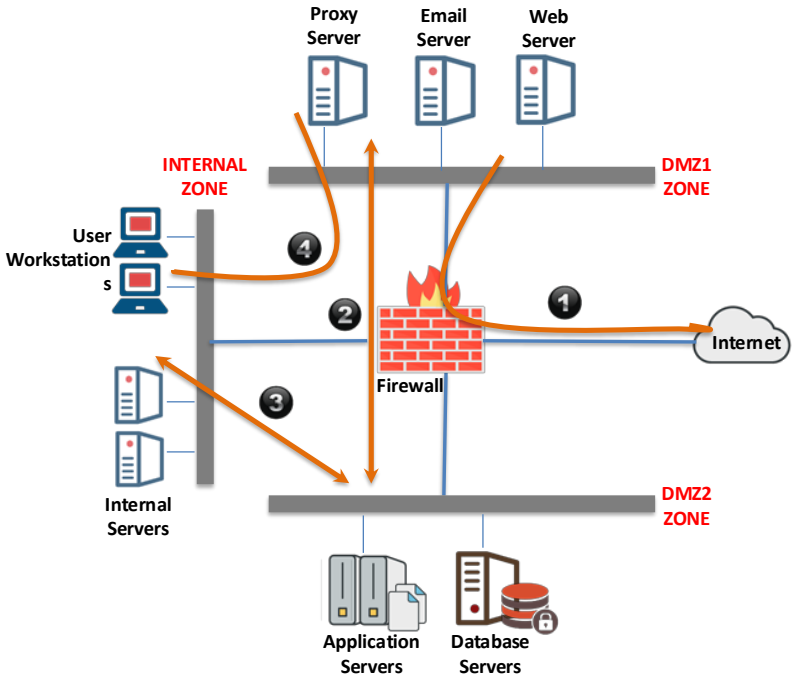
- Understanding Network Segmentation and its Types
- Understanding the Different Types of Firewalls and their Roles
- Understanding the Different Types of IDS/IPS and their Roles
- Overview of Different Types of Honeypots
- Understanding the Different Types of Proxy Servers and their Benefits
- Understanding the Fundamentals of Virtual Private Networks (VPNs) and their Importance in Network Security
- Overview of Security Incident and Event Management (SIEM) and User Behavior Analytics (UBA)
- Overview of Various Antivirus/Anti-malware Software

Module Flow

1. **Understand Different Types of Network Segmentation**
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

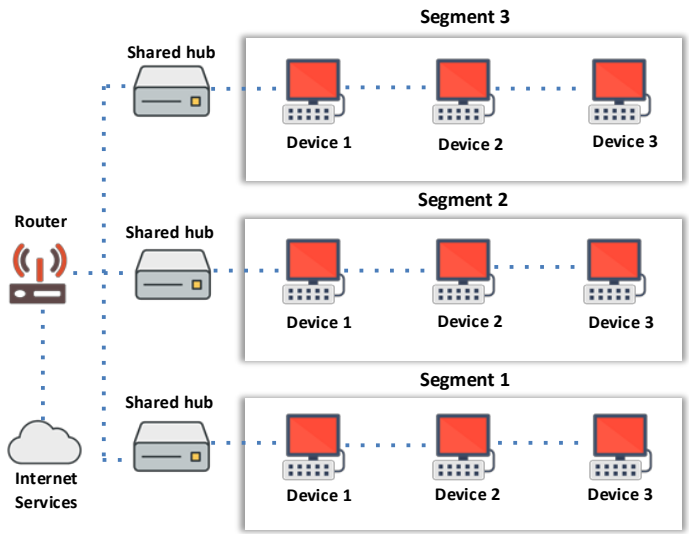
What is Network Segmentation?

- Network segmentation is the practice of **splitting** a network into smaller network segments and separating groups of systems or applications from each other
- In a segmented network, groups of systems or applications that have no interaction with each other will be placed in different network segment
- Security benefits of Network Segmentation
  - ✓ Improved Security
  - ✓ Better Access Control
  - ✓ Improved Monitoring
  - ✓ Improved Performance
  - ✓ Better Containment



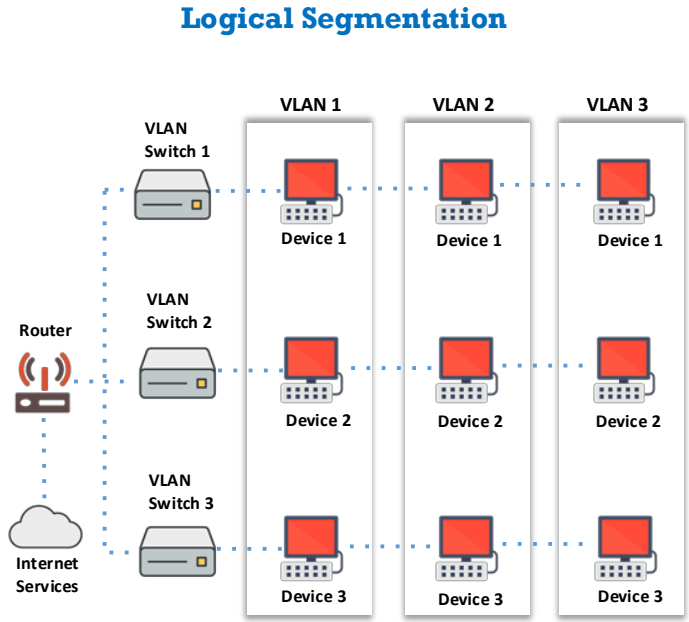
Types of Network Segmentation

- Physical segmentation is a process of splitting a larger network into **smaller physical components**
- These segments can communicate via **intermediary devices** such as switches, hubs, or routers
- Physical network segmentation can be an easy approach to divide a network, but it is **expensive** as it occupies more space



Types of Network Segmentation (Cont'd)

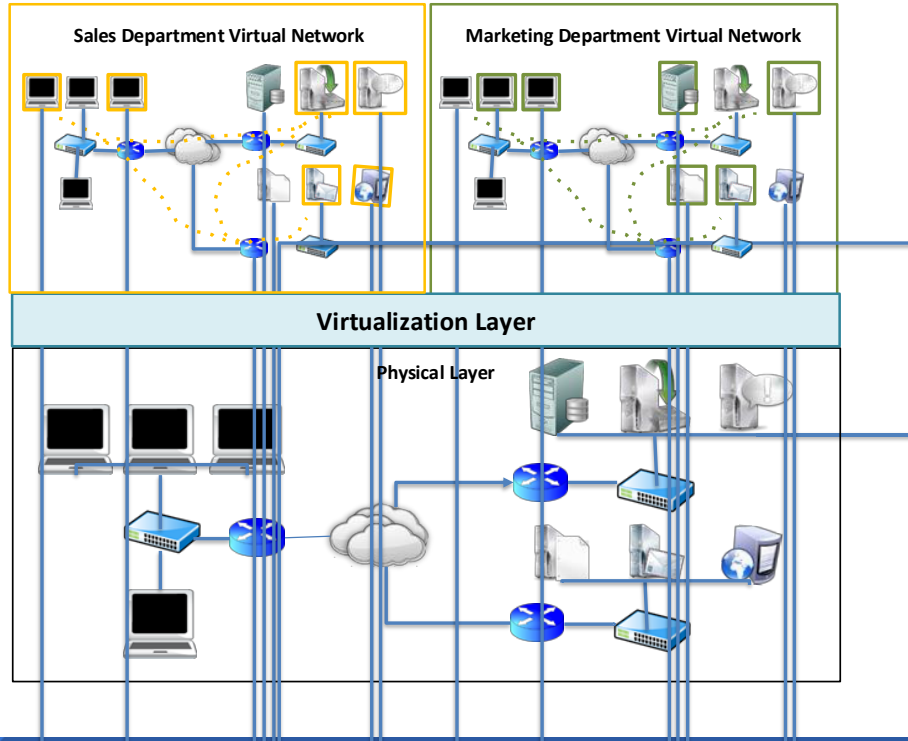
- Logical segmentation utilizes **VLANs**, which are **isolated logically** without considering the physical locations of devices
- Each VLAN is considered an **independent logical unit**, and the devices within a VLAN communicate as though they are in their own isolated network
- In this approach, **firewalls** are shared, and **switches** handle the VLAN infrastructure
- It is easier to implement and flexible to operate



Types of Network Segmentation (Cont'd)

Network Virtualization

- Network virtualization is a process of combining all the available network resources and enabling security professionals to share these resources amongst the network users using a **single administrative unit**
- Network virtualization enables each user to access available network resources such as files, folders, computers, printers, hard drives, etc. from their system



Introduction to Bastion Host

01 A bastion host is a computer system designed and configured to **protect network resources** from attacks

02 A bastion host is the only host computer on the Internet that can be **addressed directly** from the public network

03 It provides a **limited range of services** such as website hosting, and mail to ensure security

Need for Bastion Host

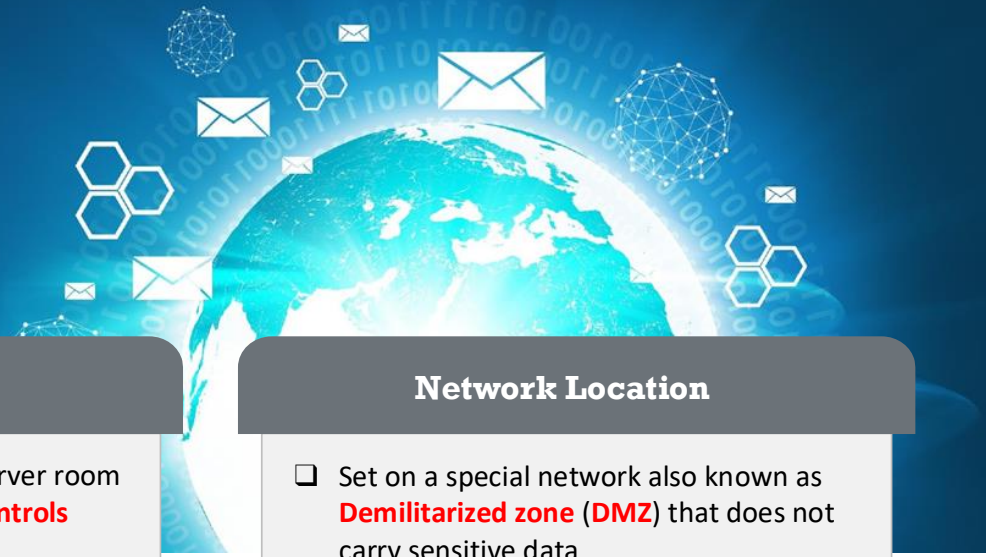
01 **Minimize the chances of penetration** by intruders

02 **Create all the logs**, which can be used to identify attack or attempts to attack

03 In case of an attack, bastion host acts as **scapegoat**

04 **Provide an additional level of security**

Positioning the Bastion Host



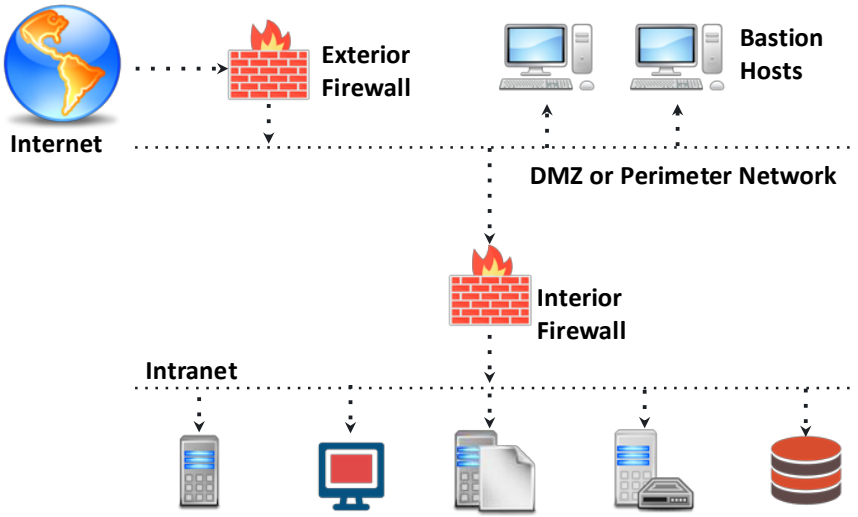
Physical Location

- Placed in a specially selected server room with suitable **environmental controls**
- Must be set up in a locked server cabinet with proper **ventilation**, cooling, and backup power

Network Location

- Set on a special network also known as **Demilitarized zone** (**DMZ**) that does not carry sensitive data
- Avoid placing the **bastion host** on internal networks
- Should be located on an additional layer known as a **perimeter network**
- Attach packet filtering router

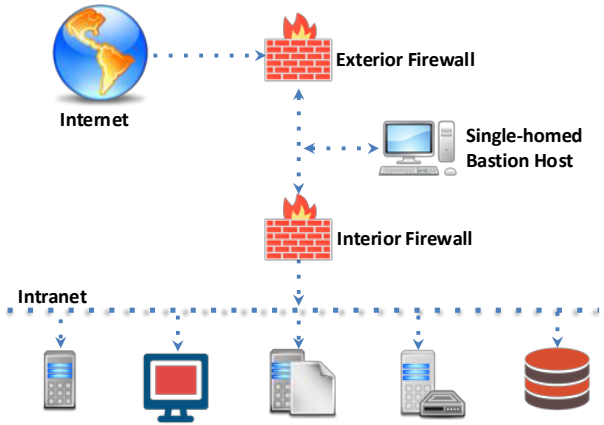
Positioning the Bastion Host (Cont'd)



Types of Bastion Hosts: Single-homed

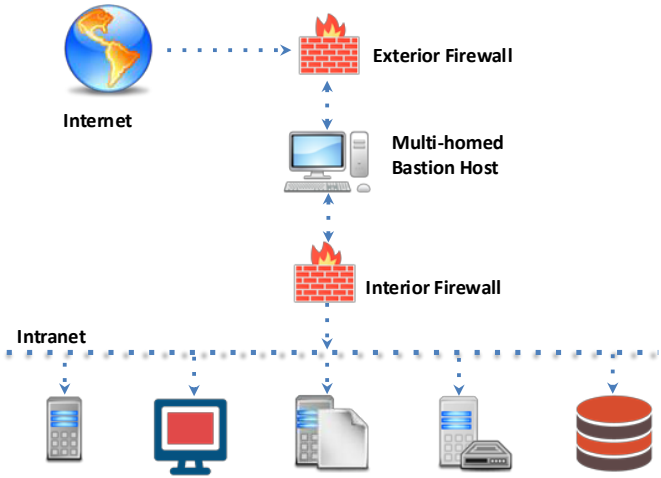
منفذ واحد

- A firewall device with only **one network interface**
- All the traffic, both incoming and outgoing, is **routed through** the bastion host
- It tests data against security guidelines and acts accordingly



Types of Bastion Hosts: Multi-homed

- A firewall device with at least **two network interfaces**
- This type of bastion host is capable of separating internal and external networks, thereby **improving security**

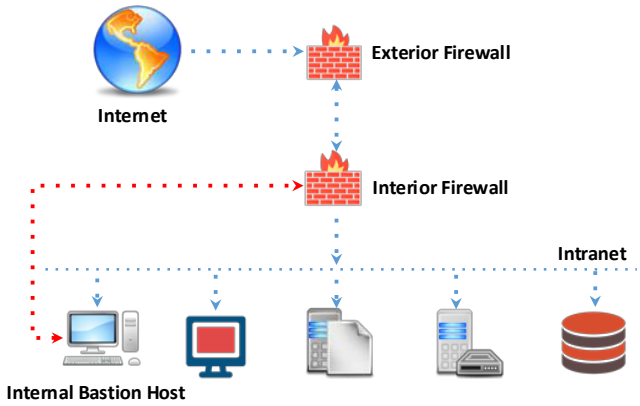


Types of Bastion Hosts: Internal Bastion Host

01 They reside **inside** the internal network of an organization

02 It can be **single-homed** or **multi-homed**

03 The internal network devices **communicate** with the internal bastion host



Types of Bastion Hosts (Cont'd)

Non-routing Dual-homed Hosts

- ✓ They operate with **multiple network connections**, but the network connections **don't interact** with each other

Victim Machines

- ✓ Victim machines allow any user to **login**
- ✓ They are useful in testing new applications whose security flaws are not yet known and to run services which are not secure

External Services Hosts

- ✓ Bastion hosts are visible to everyone, which makes them vulnerable to attack
- ✓ They require only **minimum access privileges** to the internal network, providing only a few services

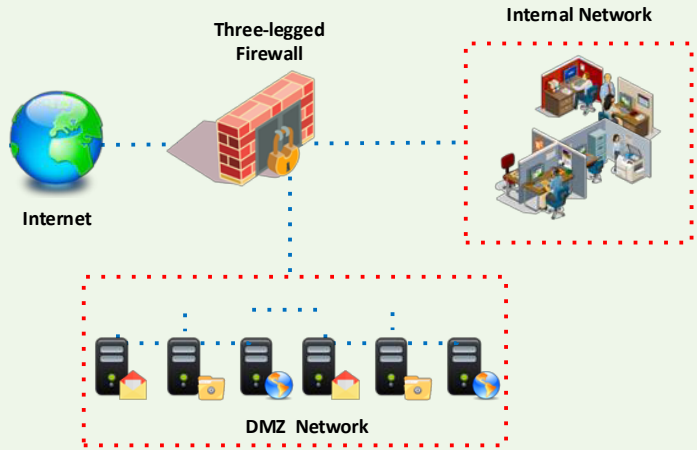
One-box Firewalls

- ✓ If a machine is constructed as a firewall, it is prone to more **attacks**
- ✓ The entire site's security relies on this single machine, so it is necessary to guarantee that this machine is absolutely secure

What is Demilitarized Zone (DMZ)?

- A computer subnetwork is placed between the organization's private network such as a **LAN**, and an outside public network such as the **Internet**, and acts as an additional security layer

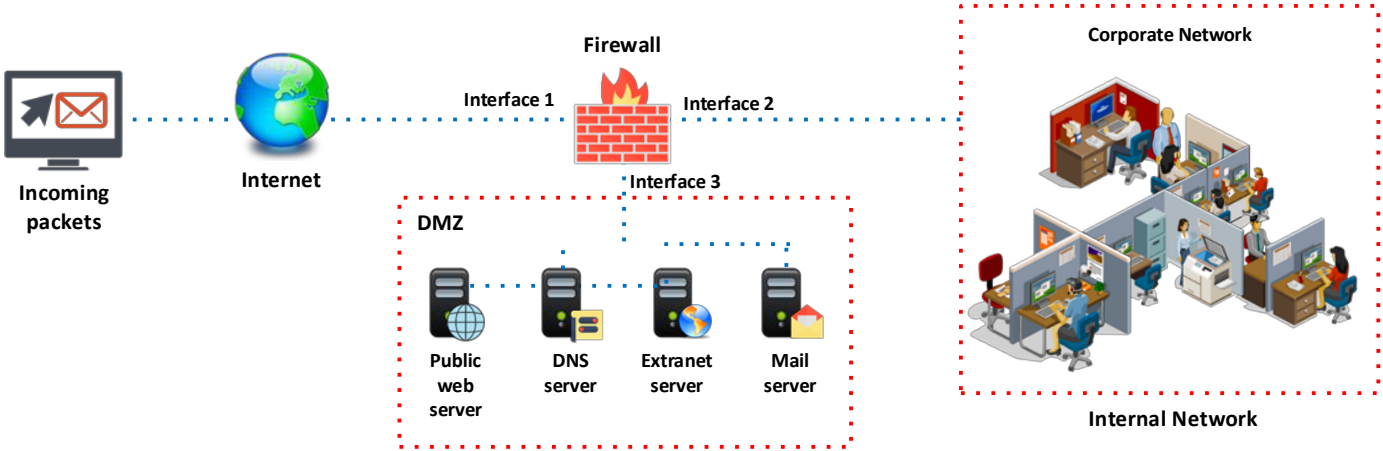
- Contains the servers that need to be accessed from an outside network
  - Web servers
  - Email servers
  - DNS servers
- DMZ configurations
  - Both **internal** and **external** networks can connect to the DMZ
  - **Hosts** in the DMZ can connect to external networks
  - But hosts in the DMZ can not connect to internal networks



Different Ways to Create a DMZ

Single Firewall DMZ

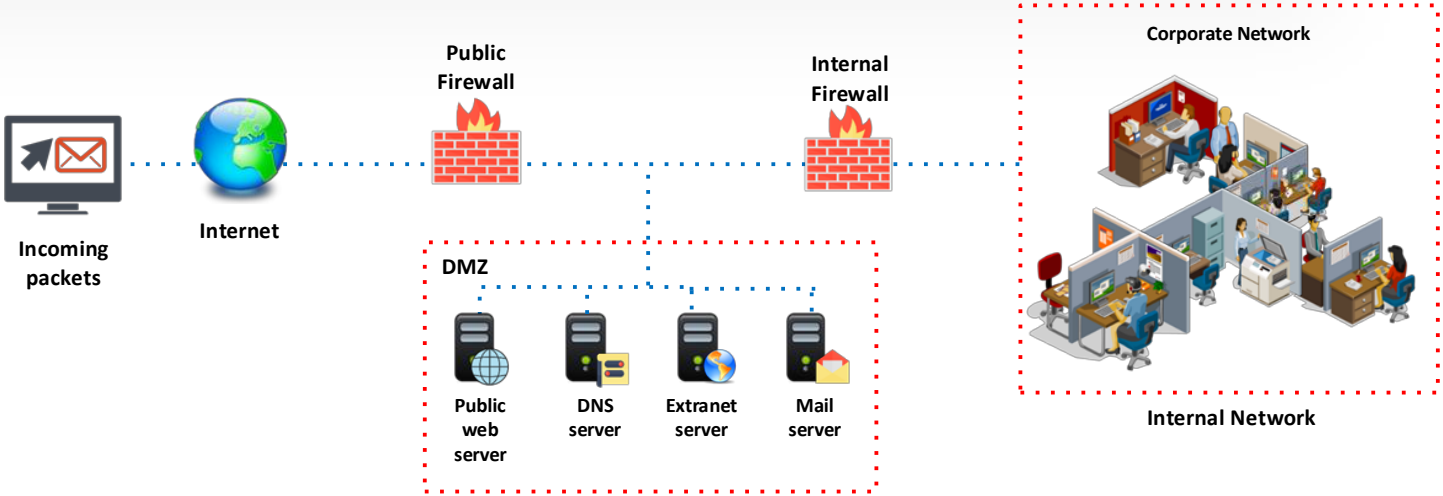
- In this model, the network architecture containing the DMZ consists of **three network interfaces**
- The first network interface connects the **ISP to the firewall**, forming the external network, whereas the second interface forms the **internal network**
- The third interface forms the **DMZ**



Different Ways to Create a DMZ (Cont'd)

Dual Firewall DMZ

- This approach uses **two firewalls** to create a DMZ
- The first firewall allows only **sanitized traffic** to enter the DMZ, whereas the second firewall conducts a double check on it
- It is the most **secure approach** in implementing a DMZ

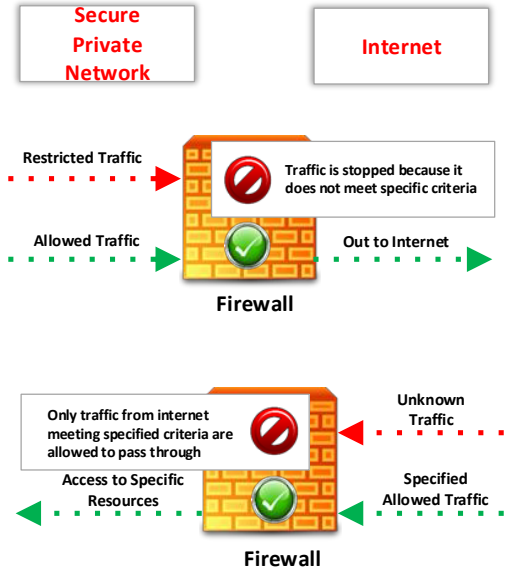


Module Flow

1. Understand Different Types of Network Segmentation
2. **Understand Different Types of Firewalls and their Role**
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

What is a Firewall?

- Firewall is a software or hardware, or a combination of both, **which is generally used to separate a protected network from an unprotected public network**
- It monitors and filters the incoming and outgoing **traffic** of the network and prevents unauthorized access to private networks

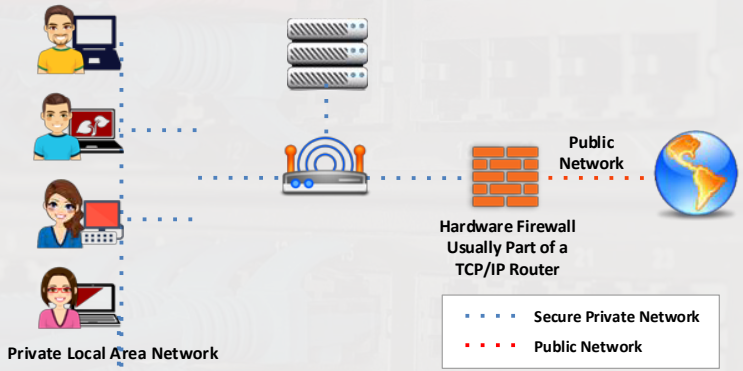


Types of Firewalls: Hardware Firewalls

01 A hardware firewall is either a dedicated **stand-alone hardware device** or it comes as part of a router

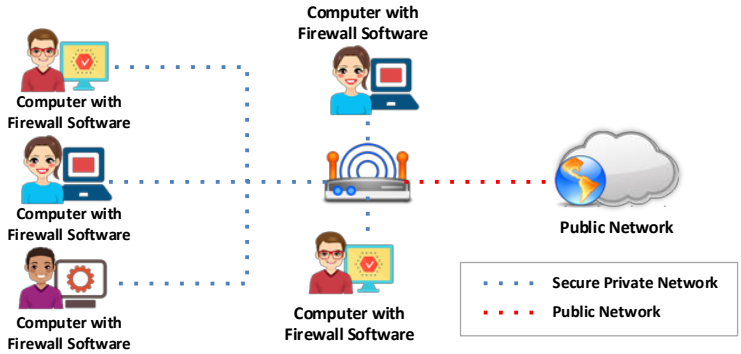
02 The network traffic is filtered using the **packet filtering** technique

03 It is used to **filter out** the network traffic for large business networks



Types of Firewalls: Software Firewalls

- A software firewall is a **software program** installed on a computer, just like normal software
- It is generally used to **filter traffic** for individual home users
- It only filters traffic for the computer on which it is **installed**, not for the entire network



Note: It is recommended that you configure both a software and a hardware firewall for best protection

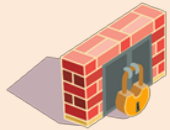
Types of Firewalls: Host-based and Network-based Firewalls

Host-based Firewalls

- The host-based firewall is used to filter inbound/outbound traffic of an **individual computer** on which it is installed
- It is a **software-based** firewall
- This firewall software comes as part of OS
- **Example**: Windows Firewall, Iptables, UFW etc.

Network-based Firewalls

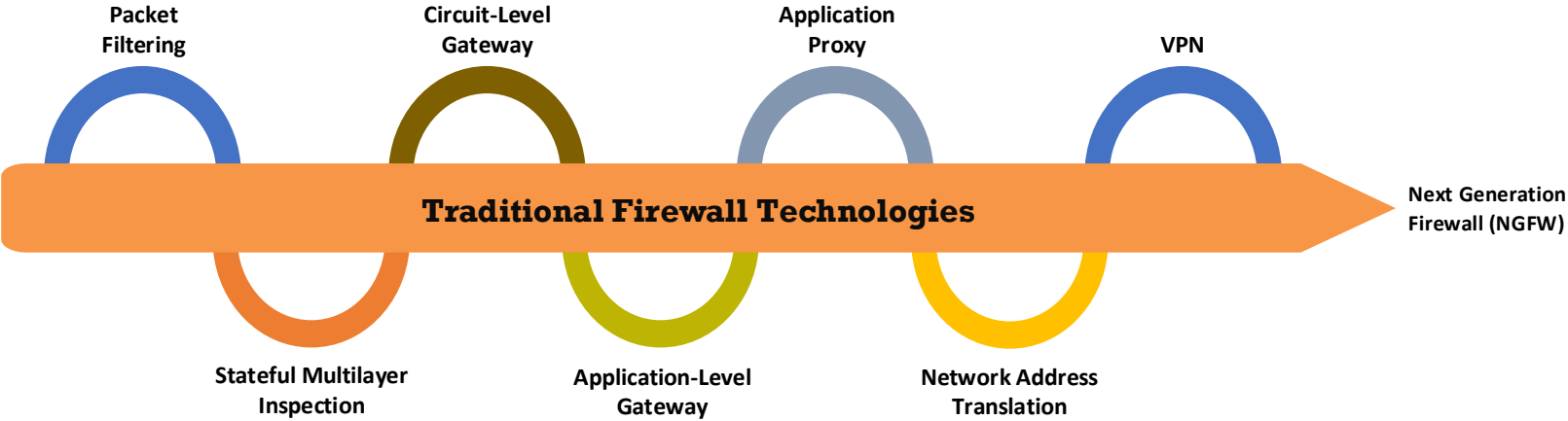
- The network-based firewall is used to filter inbound/outbound traffic from **Internal LAN**
- It is a **hardware-based** firewall
- **Example**: pfSense, Smoothwall, Cisco SonicWall, Netgear, ProSafe, D-Link, etc.



Note: It is recommended to configure both a host and network-based firewall for best protection

Firewall Technologies

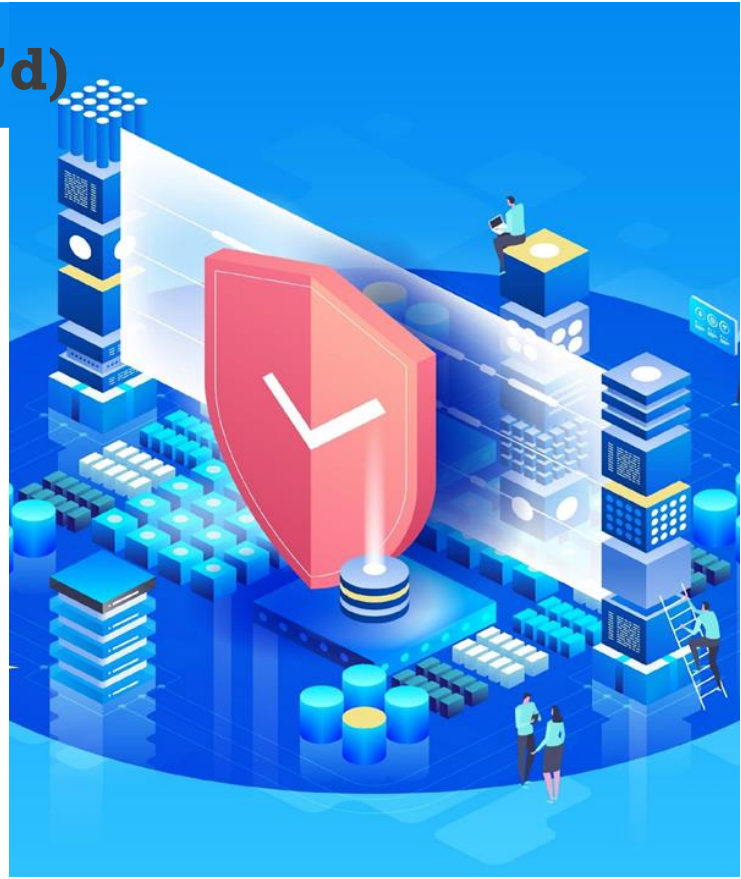
- Firewalls are designed and developed with the help of different **firewall services**
- Each firewall service provides security depending on their **efficiency** and **sophistication**



Firewall Technologies (Cont'd)

Firewall technologies operating at each OSI layer

OSI Layer	Firewall Technology
Application	✓ Virtual Private Network (VPN) ✓ Application Proxies
Presentation	✓ Virtual Private Network (VPN)
Session	✓ Virtual Private Network (VPN) ✓ Circuit-Level Gateways
Transport	✓ Virtual Private Network (VPN) ✓ Packet Filtering
Network	✓ Virtual Private Network (VPN) ✓ Network Address Translation (NAT) ✓ Packet Filtering ✓ Stateful Multilayer Inspection
Data Link	✓ Virtual Private Network (VPN) ✓ Packet Filtering
Physical	✓ Not Applicable

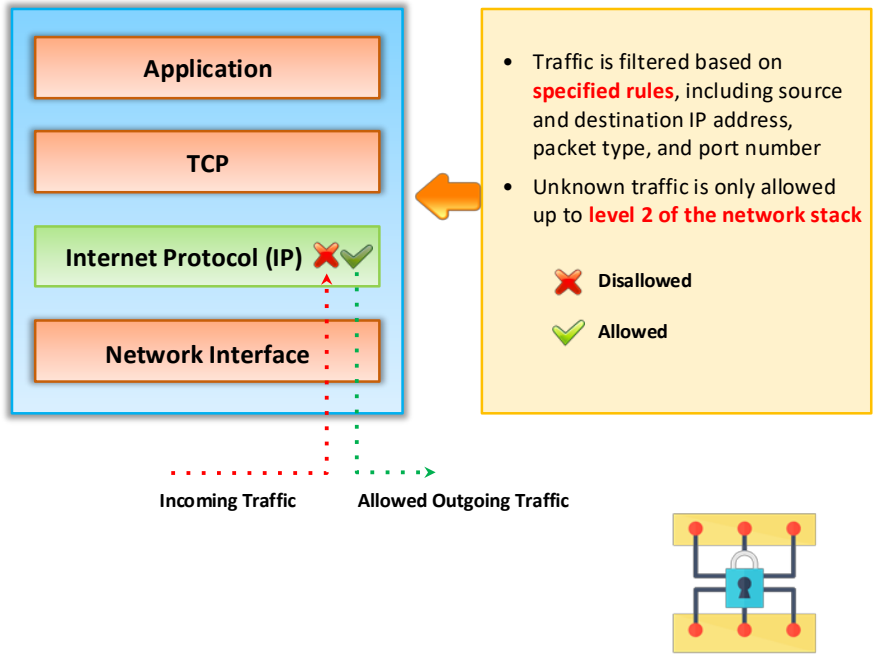


Packet Filtering Firewall

Packet filtering firewalls work at the network level of the **OSI model** (or the IP layer of TCP/IP)

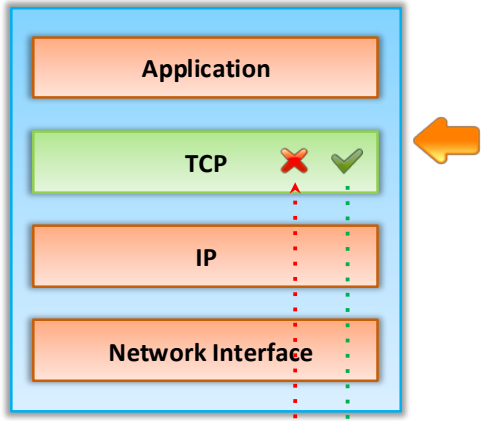
They are usually part of a **router**. Most routers support **packet filtering**

In a packet filtering firewall, each packet is compared to a **set of criteria** before it is forwarded



Circuit-Level Gateway

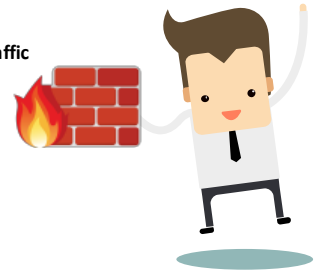
- Circuit level gateways work at the **session layer** of the OSI model, or the TCP layer of TCP/IP
- They monitor the TCP handshake between packets to determine whether a requested session is **legitimate or not**
- Information passed to a remote computer through a circuit-level gateway appears to have originated from the **gateway**



- Traffic is filtered based on **specified session rules**, such as when a session is initiated by a recognized computer
- Unknown traffic is only allowed up to **level 3 of the network stack**

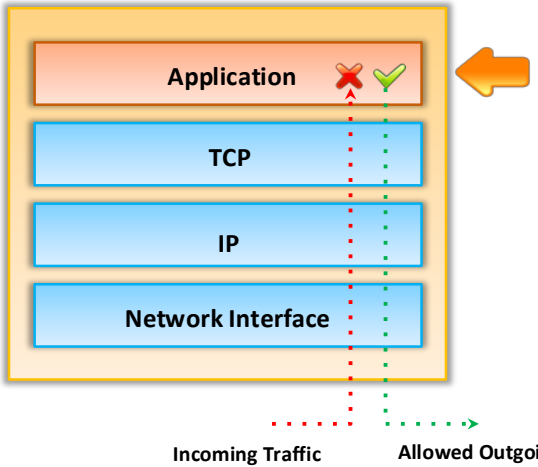
Disallowed

Allowed



Application Level Gateways

- Application level gateways can filter packets at the application layer of the **OSI model**
- Because they examine packets at the application layer, they can filter application-specific commands such as **http:post** and **get**
- In plain terms, an application level gateways can be configured to be a web proxy which will not allow any **FTP**, **gopher**, **Telnet**, or other traffic through



- Traffic is filtered based on specified application rules, applications (e.g. browser) and/or a protocol (e.g. FTP) or a combination of all of these
- Unknown traffic is only allowed up to the top of the network stack

Disallowed

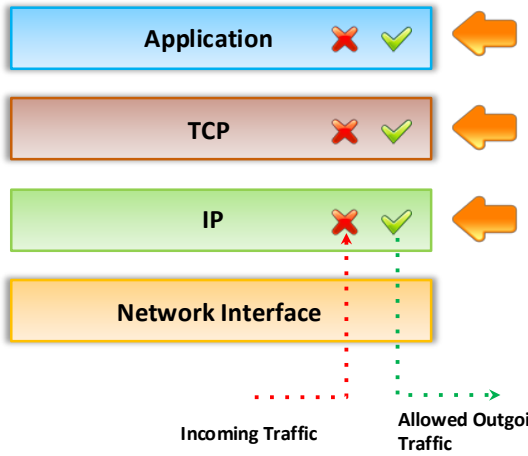
Allowed

Stateful Multilayer Inspection Firewall

A stateful multilayer inspection firewall **combines the aspects** of the other three types

They filter packets at the network layer, determine whether **session packets** are **legitimate** and evaluate the contents of packets at the **application layer**

They are **expensive** and require competent personnel to administer the device



Traffic is filtered at **three levels**, based on a wide range of specified application, session, and packet filtering rules

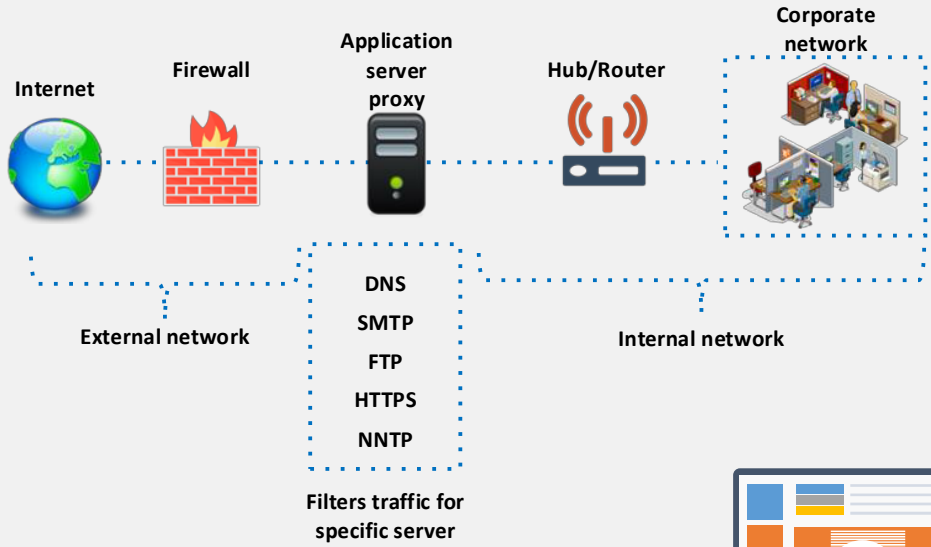
Unknown traffic is allowed up to **level 2 of the network stack**

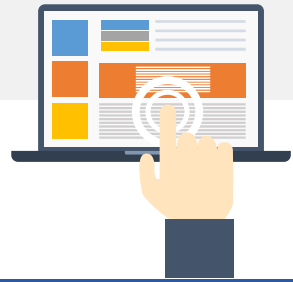
Disallowed

Allowed

Application Proxy

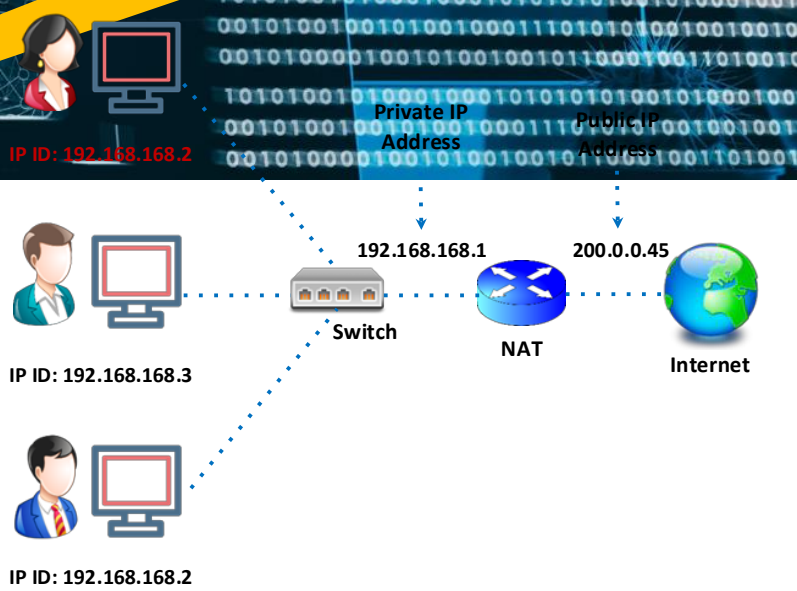
- An application-level proxy works as a proxy server and **filters connections** for specific services
- It filters connections based on the **services** and **protocols**
- **For example**, an FTP proxy will only allow FTP traffic to pass through, while all other services and protocols will be blocked





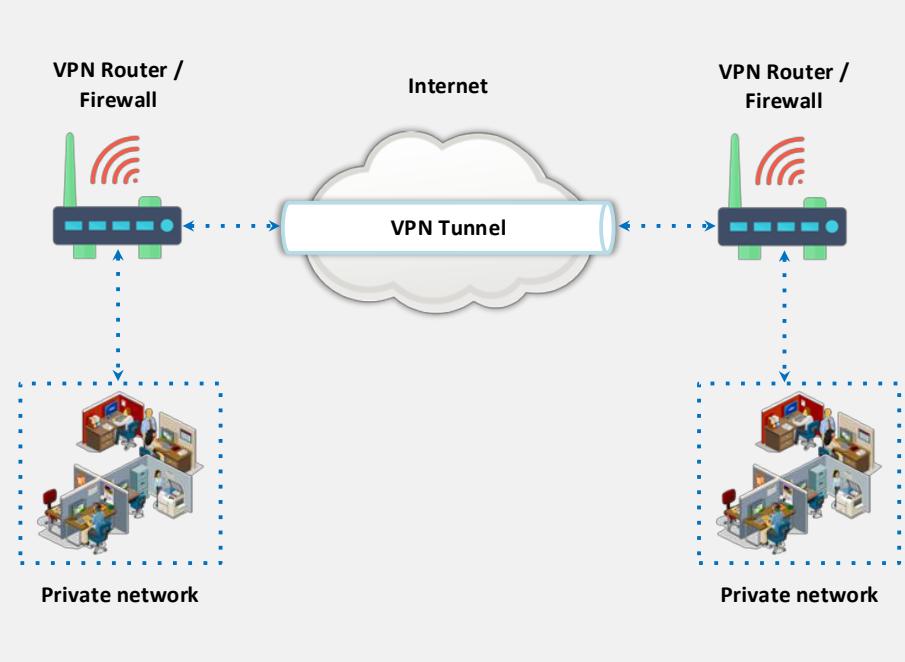
Network Address Translation (NAT)

- Network address translation separates IP addresses into two sets and enables the LAN to use these addresses for **internal** and **external traffic** respectively
- It also works with a router, the same as packet filtering does; NAT will also **modify** the packets the router sends at the same time
- It has the ability to **change** the **address** of the packet and make it appear to have arrived from a valid address
- It limits the number of **public IP addresses** an organization can use



Virtual Private Network

- A VPN is a **private network** constructed using public networks, such as the Internet
- It is used for the **secure transmission** of sensitive information over an untrusted network, using **encapsulation** and encryption
- It establishes a virtual point-to-point connection through the use of **dedicated connections**
- The **computing device** running the VPN software can only access the VPN

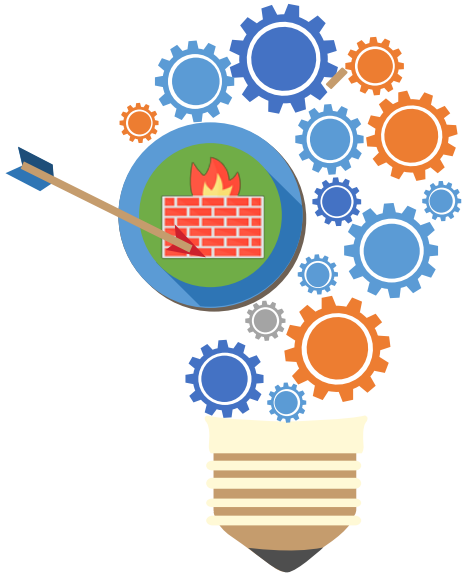


Next Generation Firewall (NGFW)

- Next generation firewall (NGFW) firewall technology is **third-generation firewall technology** that moves beyond port/protocol inspection
- In addition to traditional firewall capabilities, NGFW firewall technology has the capability to inspect traffic based on **packet content**
- Typical NGFW capabilities:
  - ✓ Deep packet inspection (DPI)
  - ✓ Encrypted traffic inspection
  - ✓ QoS/bandwidth management
  - ✓ Threat intelligence integration
  - ✓ Integrated intrusion prevention system
  - ✓ Advanced threat protection
  - ✓ Application control
  - ✓ Antivirus inspection

Firewall Capabilities

- Prevent network scanning
- Controls traffic
- Performs user authentication
- Filters packets, services, and protocols
- Performs traffic logging
- Performs network address Translation (NAT)
- Prevents malware attacks



Firewall Limitations

1

A firewall does not prevent the network from **backdoor attacks**

2

A firewall does not protect the network from **insider attacks**

3

A firewall cannot do anything if the network design and **configuration** is **faulty**

4

A firewall is not an alternative to **antivirus** or **antimalware**

5

A firewall does not prevent **new viruses**

6

A firewall cannot prevent **social engineering threats**

7

A firewall does not prevent **passwords misuse**

8

A firewall does not block attacks from a higher level of the **protocol stack**

Firewall Implementation and Deployment Process

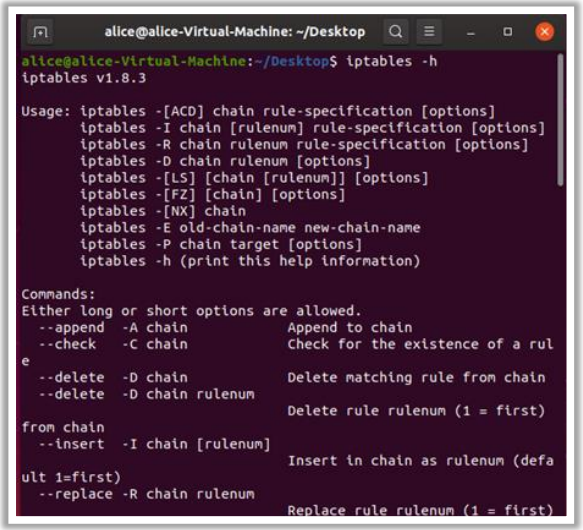
- Use a step-by-step process to ensure a **successful** firewall implementation and deployment
- The process helps to minimize any unforeseen **issues** and identify any potential **pitfalls** early on

Firewall Implementation and Deployment Process

Planning	When implementing a firewall for the network, organizations must **plan their positioning** in advance
Configuring	Involves configuring various components and features such as hardware, software, **policy configuration**, implementing **logging**, and **alerting** mechanisms
Testing	Mainly focuses on whether the **firewall rules** are set according to the actions performed by the firewall
Deploying	A phased approach to deploy multiple firewalls on a network helps detect and **resolve issues** regarding conflicting policies
Managing and Maintaining	Includes maintaining the **firewall architecture**, **policies**, software, and other components deployed on the network

Host-based Firewall Protection with Iptables

- Iptables is a **built-in firewall utility** for Linux OSes
- Iptables comes pre-installed on any Linux distribution. However, you can update/install it with `sudo apt-get install iptables` command



Task	Iptable Commands
Filtering non TCP packets	iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
Blocking XMAS scan Attack	iptables -A INPUT -p tcp --tcp-flags ALL -j DROP
Drop any NULL packets	iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
Drop any fragmented packets	iptables -A INPUT -f -j DROP

Host-based Firewall Protection with Iptables (Cont'd)

Existing rules can be checked using **`sudo iptables –L –n –v`** command

```
root@alice-Virtual-Machine: /home/alice
root@alice-Virtual-Machine:/home/alice# iptables -L -n -v
Chain INPUT (policy ACCEPT 97 packets, 7270 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 DROP       all  --  *      eth0    0.0.0.0/0            0.0.0.0/0
    owner UID match 1001
root@alice-Virtual-Machine:/home/alice#
```

Specific IP address can be block using **`Iptables Firewall`**

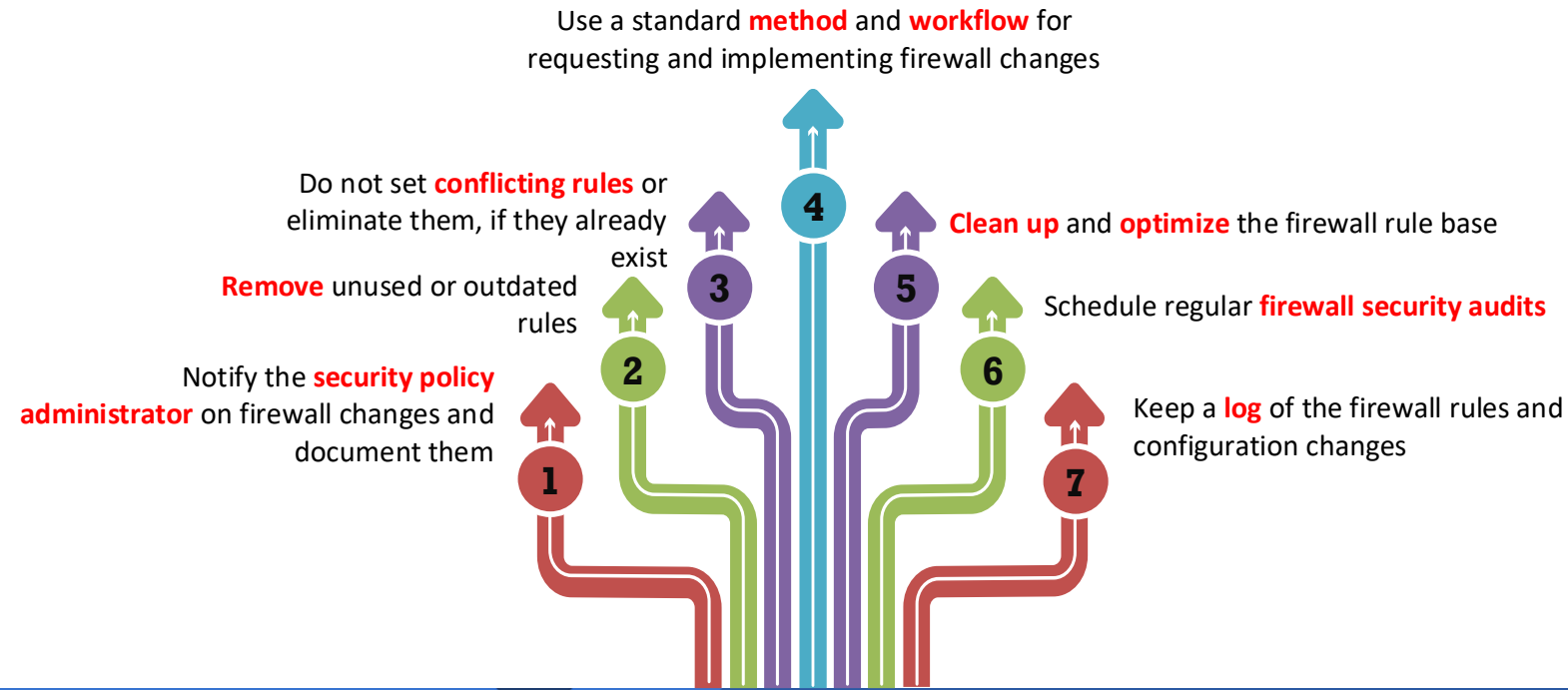
`iptables –A INUPT –s 10.10.10.55 –j DROP`

```
root@alice-Virtual-Machine: /home/alice
root@alice-Virtual-Machine:/home/alice# iptables -A INPUT -s 10.10.10.55 -j DROP
root@alice-Virtual-Machine:/home/alice#
```

Secure Firewall Implementation: Best Practices

- Filter unused and common **vulnerable** ports
- If possible, create a **unique user ID** to run the firewall services. Rather than running the services using the administrator or root IDs
- Set the firewall ruleset to deny all traffic and enable only the services required
- Change all the **default passwords** and create a strong password that is not found in any dictionary. A strong password to ensure brute-force attacks also fail.
- To enhance the **performance** of the firewall, limit the applications that are running
- Configure a **remote syslog server** and apply strict measures to protect it from malicious users
- Monitor **firewall logs** at regular intervals. Include them in your data retention policy
- Immediately investigate all **suspicious log** entries found

Secure Firewall Implementation: Recommendations



Secure Firewall Implementation: Do's and Don'ts

01 Implement a strong firewall

02 Limit the applications that run on a firewall

03 Control physical access to the firewall

04 Evaluate firewall capabilities

05 Consider workflow integration

06 Don't overlook scalability

07 Don't rely on packet filtering alone

08 Don't be unsympathetic to hardware needs

09 Don't cut back on additional security

10 Don't implement without SSL encryption