## N/w security controls : Technical Controls

# Network Segmentation – Splitting Subnetmask(Prevent malware attcaks on other systems)

Once the Subnet mask is modified to make more logical networks then switches have ability to create multiple VLAN’s

Then we can create as many VLAN’s as per requirement

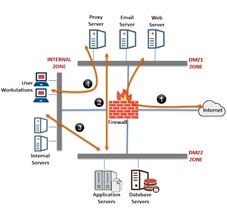
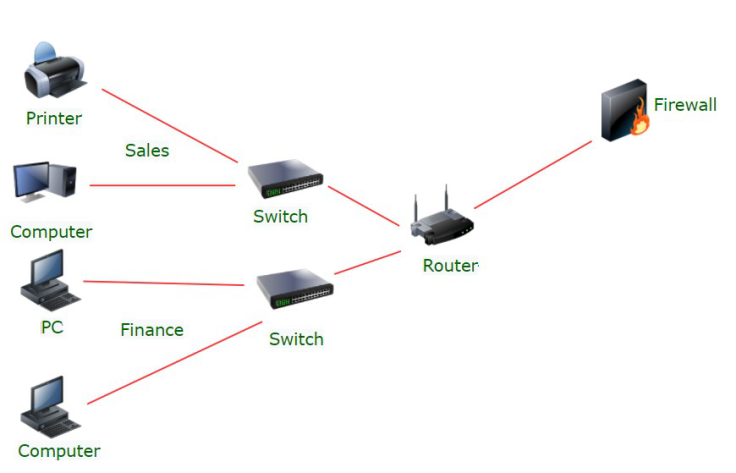
Flat network- Can be effected by equipment failure/Worm(Malware)

* Splitting a n/w into smaller n/w segments
* Seperating groups of systems /applications from each other
* If groups of systems or applications have no interaction with each other will be on different n/w sgment
* Security benefits: Improved security

Better access control

Improved monitoring & performance

Better containment



# Types:

* Physical segmentation – Expensive & occupies more space
* Logical segmentation –easy to implement & flexible to operate
* Network Virtualiazation

# Physical segmentation

Splitting larger n/w into small physical components

Segments Communicate via Hubs, switches or routers

This approach is easy to divide a n/w

If one hub /router malfunctions whole segment shuts down

# Logical segmentation – firewalls are shared & switches handle VLAN infrastructure

Segmented using VLANs – and are isolated using Ada 2.1Q logically

Physical locations of devices are not considered

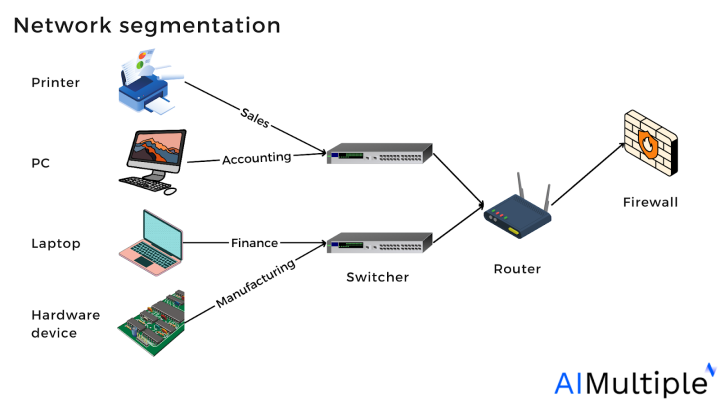
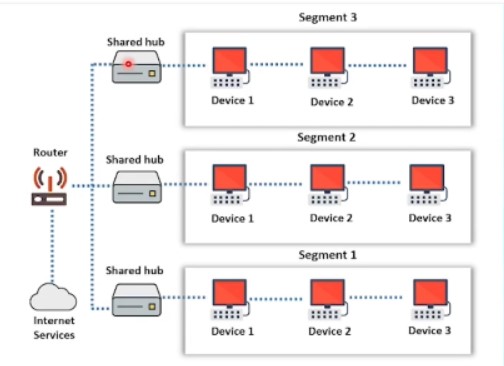
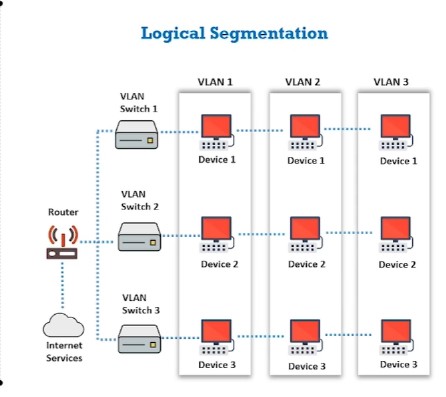
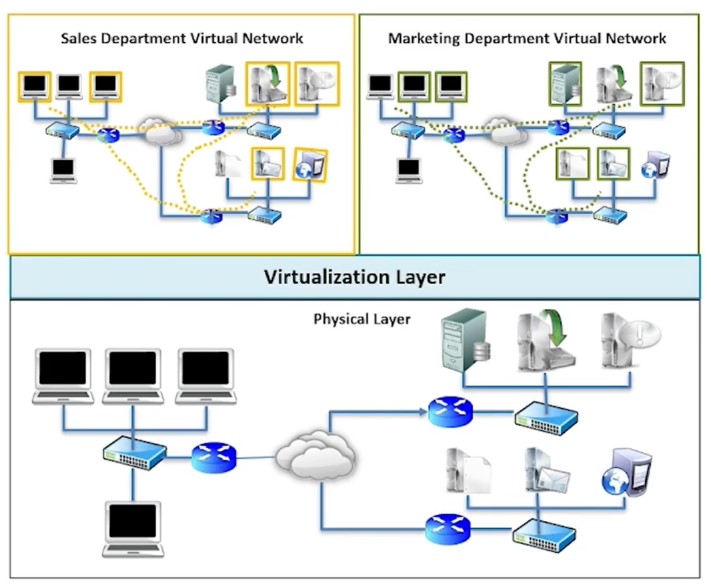
Each VLAN is independent logical unit

Devices within a VLAN communicates via their own isolated n/w

# Network Virtualization

Combines all available n/w resources enables security professionals to share these resources among n/w users using single administrative unit

This enables users to access files, folders, computers, printers, Hard drives etc from their system.

# 7 Different Types of Firewall

There are several types of firewalls that work on different layers of the OSI model. Depending on the kind of service and security you need for your network, you need to choose the right type of firewall. The following are the list of seven different types  firewalls that are widely used for network security.

Screened host firewalls

Screened subnet firewalls

Packet filter firewalls

Stateful inspection firewalls

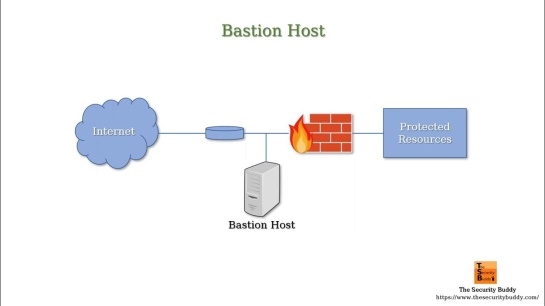
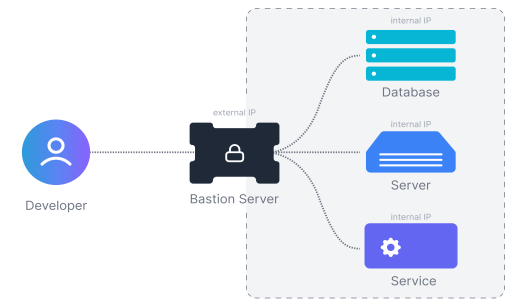
Hybrid firewalls

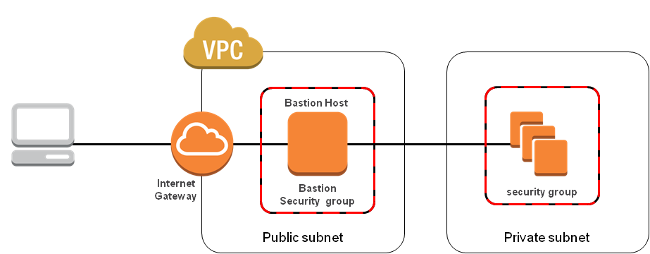
Proxy server firewalls

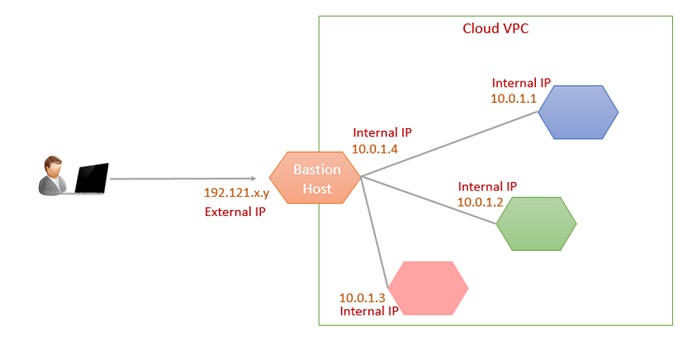
Application level (gateway) firewalls

# Bastion Host – (Firewall) Protect n/w resource from attacks

* A computer system designed & configured
* Only host on internet that can be addressed directly from the public n/w
* Provides limited range of services

* Ex: Website hosting & mail to ensure security 



Firewall allows or blocks – Protocols , Ports, programs, IP addresses

Windows Firewall is a Bastion Host

# Uses of Bastion Host:

* Min. Penetration attacks by intruders
* Creates all the logs –used to identify attack or attack attempts
* In case of attack, bastion host acts as scapegoat
* Provides additional level of security

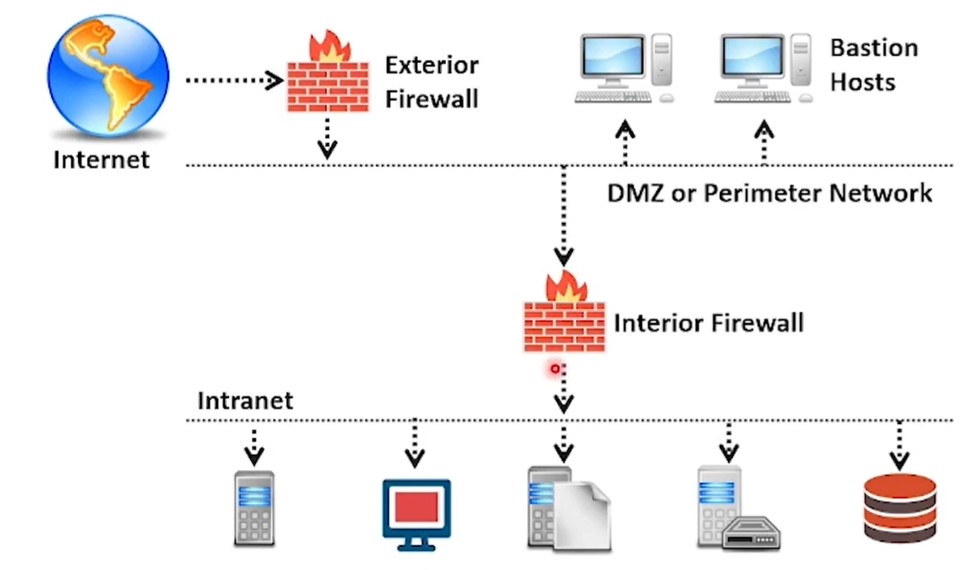
# Setting up Bastion Host:

## Physical location:

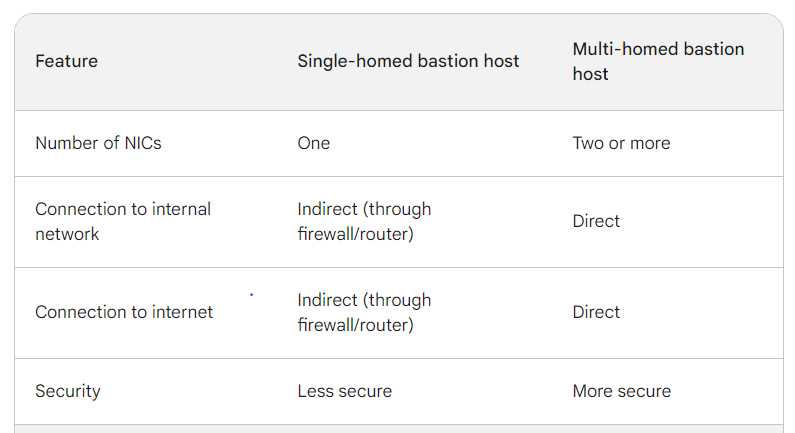
* In server room under environmental controls – proper ventilation, cooling, backup power
* Must be in locked server cabinet

## Network Location:

* Setup on n/w – Demilitarized zone (DMZ) that doesn’t carry sensitive data
* Avoid placing on internal n/w’s
* Should be kept on additional layer known as – perimeter n/w
* Attach packet filtering router

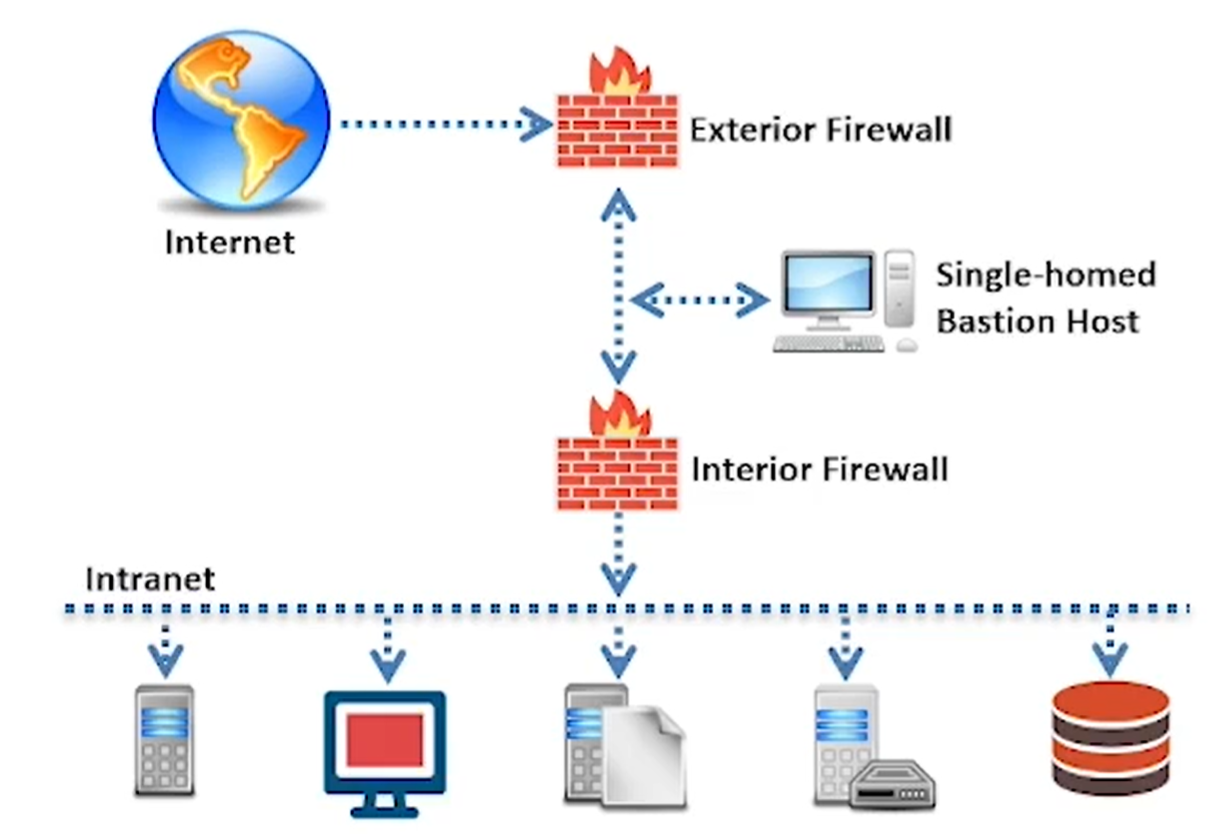
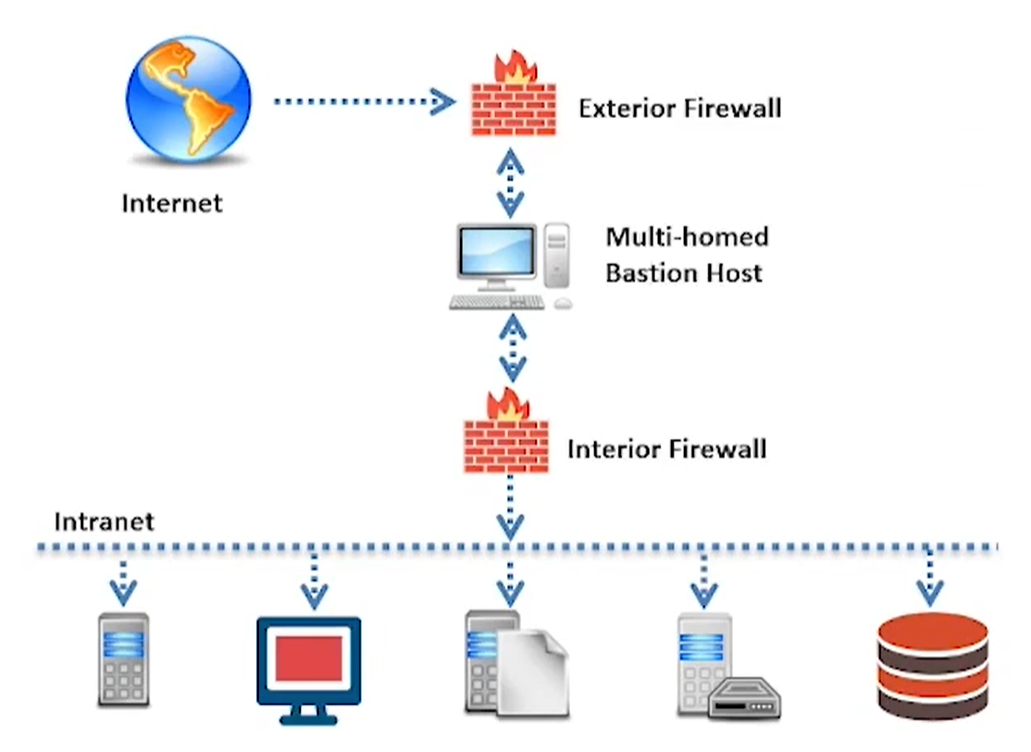


# Types of Bastion Host:



## Single Homed:

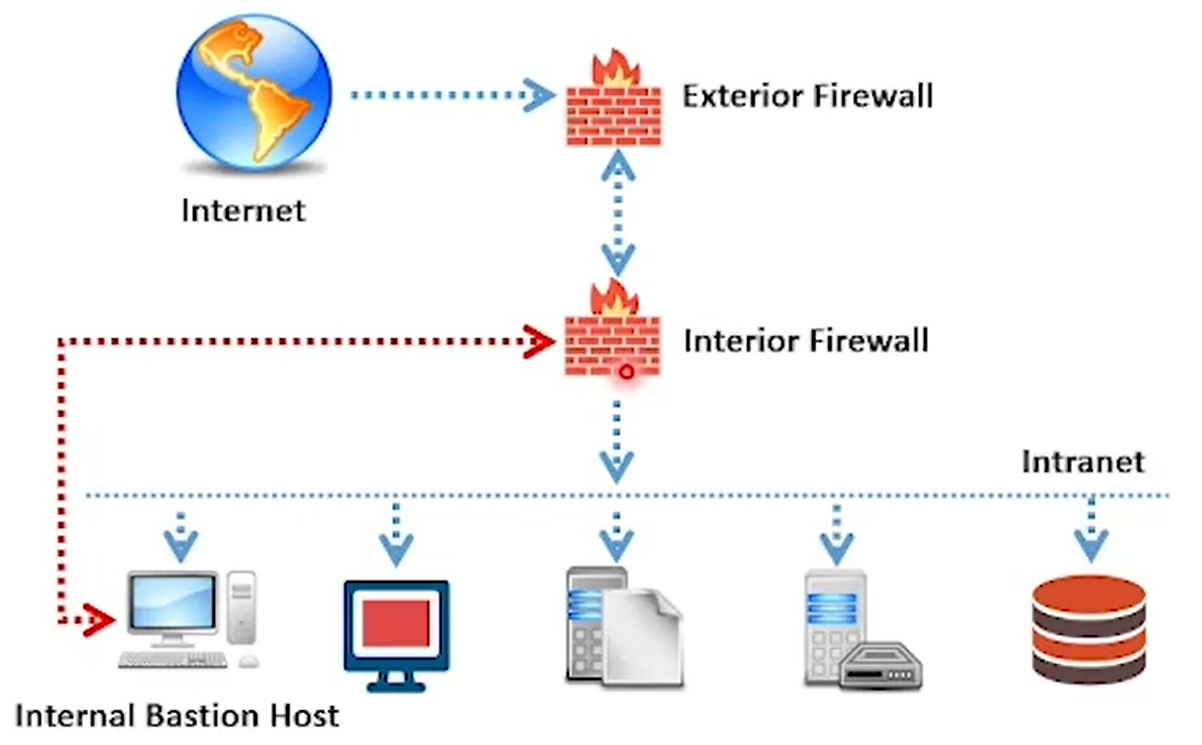
* Firewall device with one-n/w interface
* All traffic routed through bastion host
* Tests data against security guidelines and acts based on that

## Multi-homed:

* Atleast 2 n/w interfaces
* Can separate internal & external n/ws – improves security

## Internal Bastion Host:

* Inside the internal n/w of org.
* Can be single or multi-homed
* Internal n/w devices communicate with internal bastion host

## Non-routing Dual-home based Hosts

* Operate within n/w connections
* But n/w connections don’t interact with each other
* We can purchase physical connectors and can add them to firewall

## Victim Machines

* Allows any user to login
* Useful in testing new applications – whose security flaws are not yet known &

To run unsecured services

## External Services Hosts: vulnerable to attack

* Visible to everyone
* Easy to attack
* Require only min. access privileges to the internal n/w
* Provides only few services

## One-box firewalls: prone to more attacks

* Machine firewall
* Entire site’s security relies on this single box
* Necessary to guarantee that the machine is absolutely secure

# DMZ (Demilitarized Zone)

A computer subnetwork is placed between the org. private n/w like LAN , an outside n/w like Internet and acts as additional security layer.

## Contains

n/ws that need to be accessed from outside n/w – DNS, Web, Email servers

## DMZ Configuratuibs

* Internal and external n/ws can connect to DMZ
* Hosts in DMZ Can connect to external n/ws BUT blocked by Internal firewall
* i.e; can’t connect to internal networks

# Ways to create DMZ

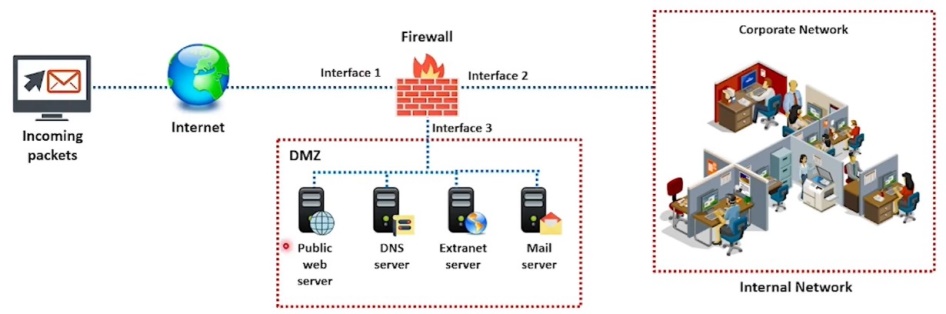
## Single Firewall DMZ

* N/w architecture containing DMZ consists of 3 N/w interfaces

Network 1 : Connects ISP to firewall (Forming external n/w)

Network 2: Forms internal network

Network 3: Forms the DMZ (it has public webserver, DN server, Extranet, mailserver)



## Dual Firewall DMZ – Most secure

* Uses 2 firewalls to create DMZ

Firewall 1: Public firewall

Allows only sanitized traffic to enter DMZ

Firewall 2: Internal Firewall

Conducts a double check on sanitized traffic

