# Firewalls

## Types:

## Hardware –part of TCP/IP router (Usually)

* Either dedicated stand alone h/w device or a part of a router
* Packet filtering Technique – filters Network traffic
* It’s used to filter out the n/w traffic for large business n/ws

### Netwrok Based Firewalls –Hardware based

* Filter inbound/outbound traffic from Internal LAN
* Ex: pfSense, Smoothwall, Cisco SonicWall, Netgear, ProSafe, D-Link etc

## Software

* It’s a software program
* Filter traffic for individual home users
* It filters traffic only for the computer
* doesn’t filter traffic for the entire network

### Host Based Firewalls- sotware based

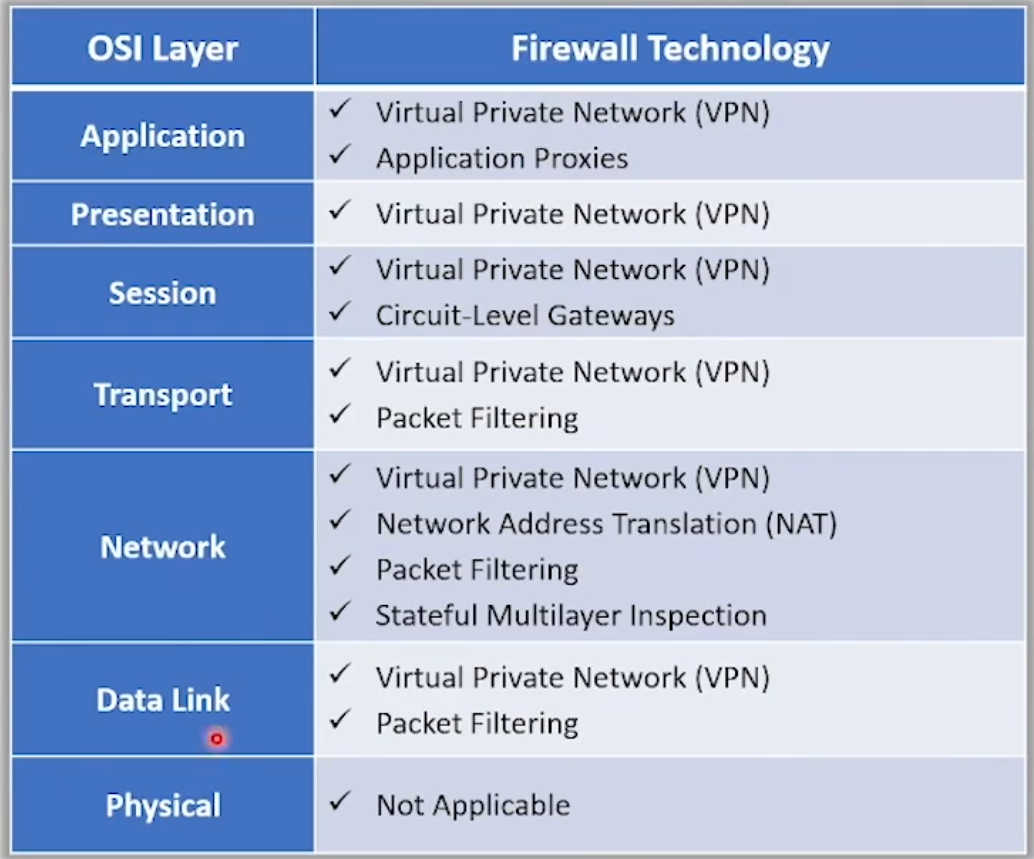
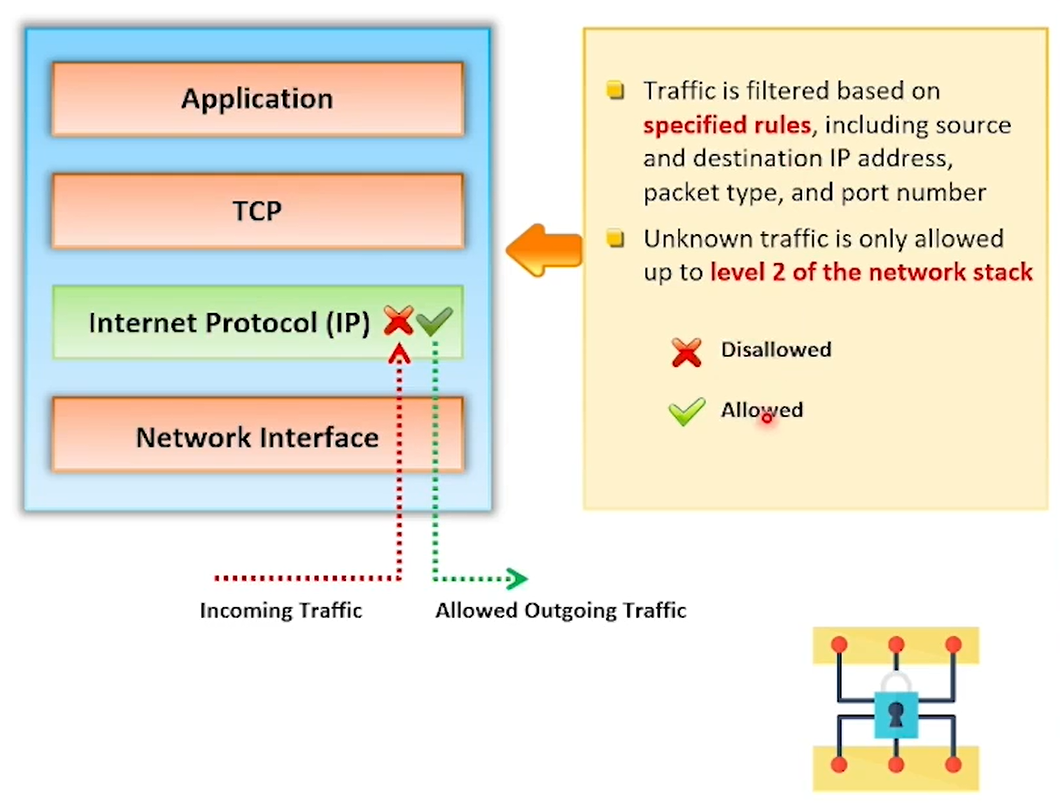
* Filter – inbound/ outbound traffic of an individual computer
* It comes as a part of OS

Example: Windows Firewall, Iptables, UFW etc

# Firewall Technologies:

* Firewalls are designed and developed with diff firewall services
* Each service provides security based on their efficiency and sophistication.

## Traditional

## Packet filtering firewall - at network layer

* Usually part of a router
* Before forwarding a packet – each packet is compared to a set of criteria

## Circuit-Level Gateway – at session layer

* Monitors TCP handshake b/w packets
* Determine whether requested session is legitimate or not

## Application Level Gateways: at application layer

* Evaluate the contents of packet
* They filter application specific commands like

http:post & get

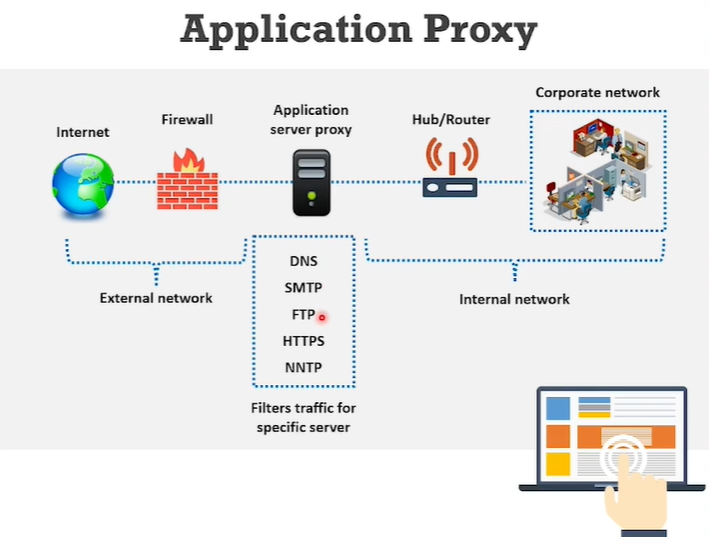
* This will not allow FTP, gopher, telnet or other traffic
* Can configure as web proxy

## Stateful Multilayer Inspection Firewall –web proxy

* Combines 1 , 2 & 3
* Unknown traffic allowed only upto layer 2
* Expensive
* Require competent personnel to aminister the device

## Application proxy

* Filters connections for specific devices
* Filteration based on services & protocols
* Ex: FTP proxy allows only FTP traffic and blocks the rest



## Network Address Translation(NAT) – works with router like Packet filtering

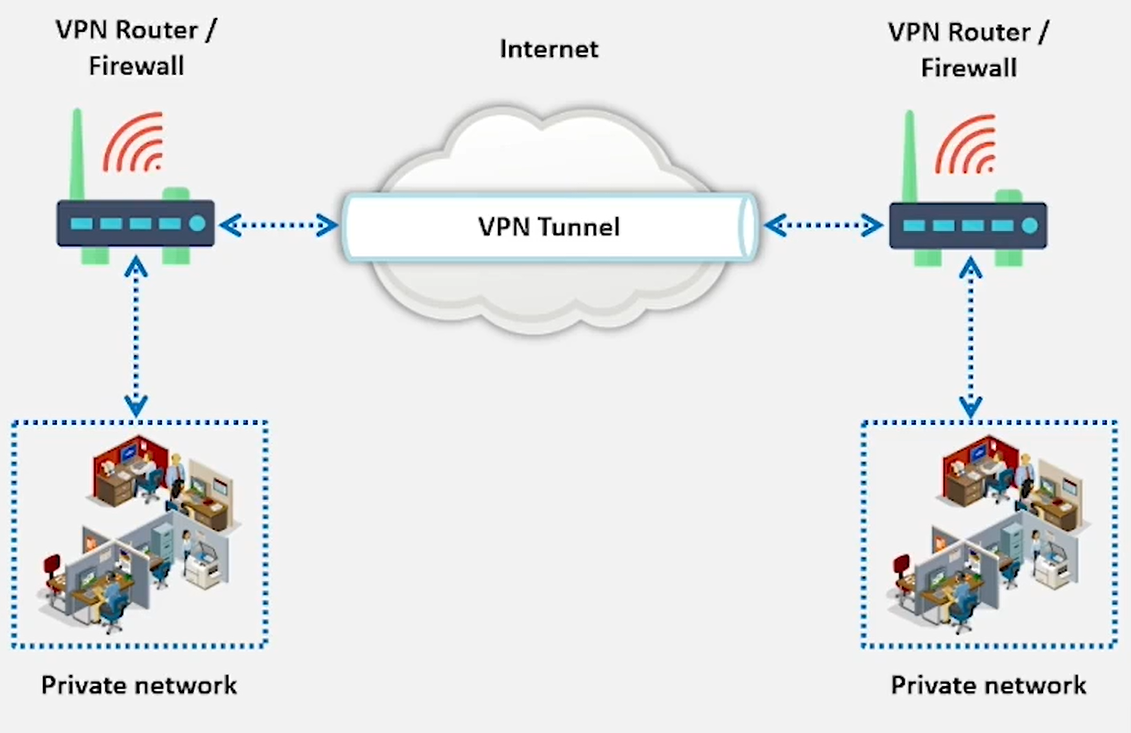
* Seperates IP address into 2 sets

Enables LAN to use these addresses for internal & external addresses respectively

* NAT’ll modify the packets the router sends at the same time of **Packet filtering**
* Can change the address of the packet and make it appear to have appear to have arrived from a valid address
* Limits the no.of public IP addresses an org. can use

## Virtual Private Network (VPN)

* Used for secure transmission of sensitive – using encapsulation & encryption
* Point –point connection through the use of dedicated connections
* The computing device running the VPN s/w can only access the VPN



## Next Generation Firewall (NGFW)

* 3rd generation firewall technology that moves beyond port/protocol inspection
* Has the capability to inspect traffic based on packet content
* 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
* Prevent n/w scanning
* Controls traffic
* Performs user authentication
* Filter packets, services and protocols
* Performs traffic logging
* Performs NAT
* Prevents malware attacks

# Limitations of Firewall:

* Doesn’t prevent the n/w from backdoor attacks
* Doesn’t prevent new viruses
* Can’t prevent social engineering threats
* Doesn’t prevent passwords misuse
* Doesn’t block higher level attacks of protocol stack
* Doesn’t protect from insider attacks
* Can’t do anything if n/w design and configuration is faulty
* It’s not alternative to antivirus or antimalware

# Firewall Implementation & Deployment process:

With proper process we can minimize any unforeseen issues and identify any potential pitfalls early on

Planning – their positioning

Configuring – hardware, software, policies, implementing logging and alerting mechanisms

Testing – focuses on Firewalls rules are set according to the actions performed by firewall

Deploying (Phased approach) - Deploy multi firewalls on a network helps to detect and resolve regarding conflicting policies

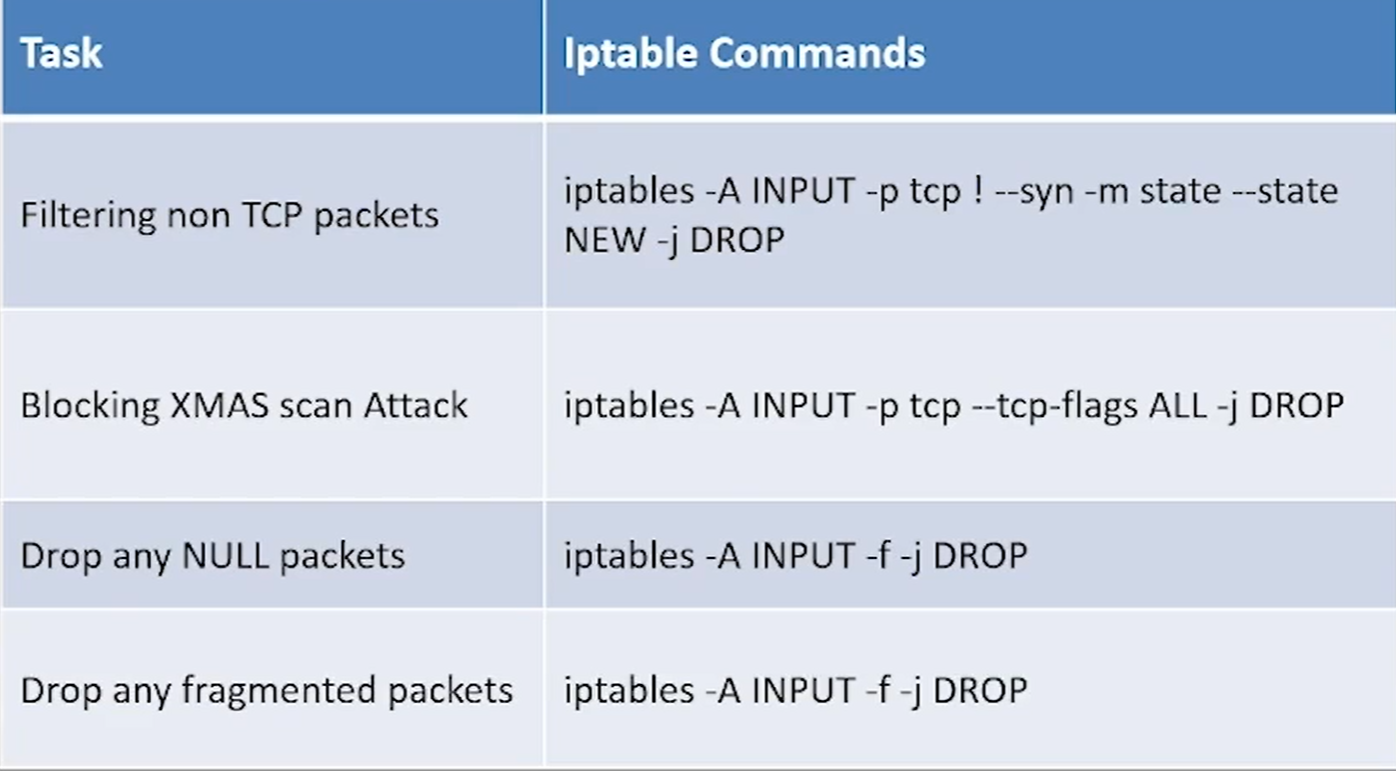
Managing and maintaining – Firewall architecture, policies, software and other components deployed on the network need to be maintained

# Host-based firewall protection with IP Tables:

* Iptables is a in-built firewall utility for Linux
* Iptables comes pre installed on Linux distribution
* Can update iptables

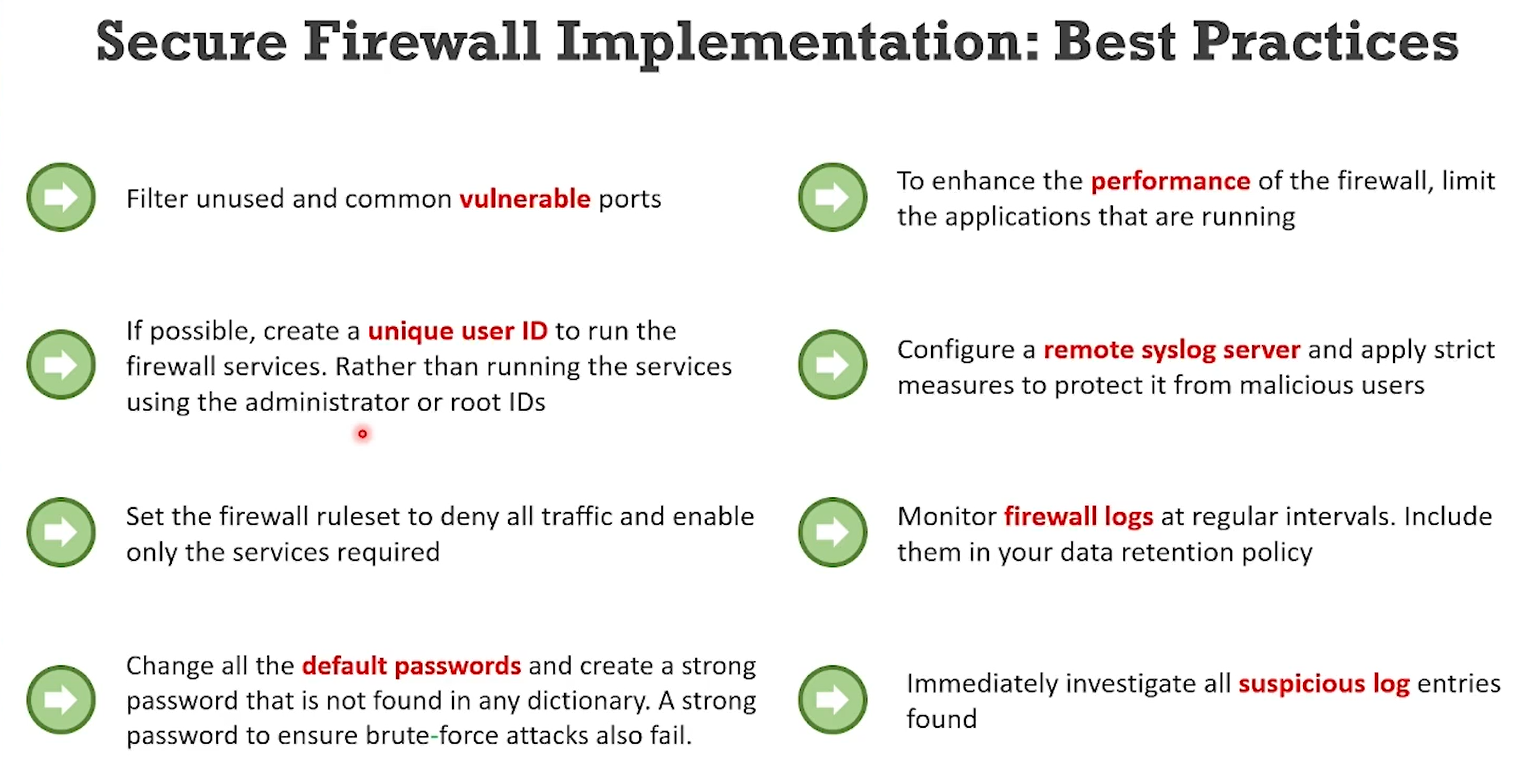
sudo apt-get install iptables

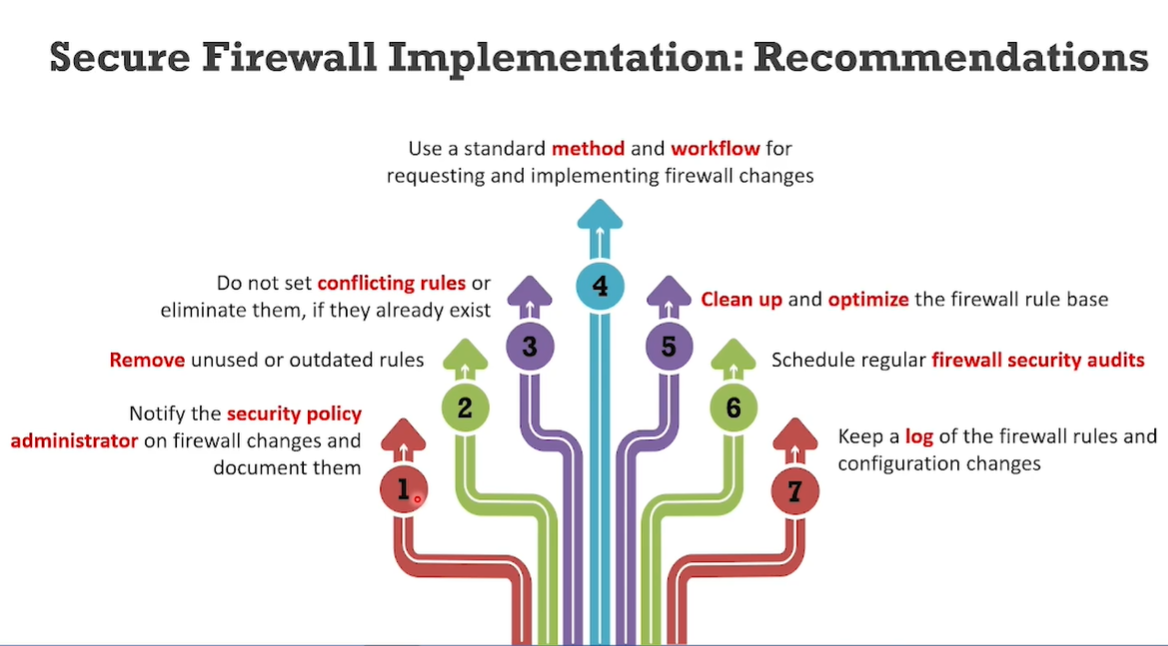
* Specific IP addresses can be blocked using Iptables firewall
* Existing rules can be checked command: sudo iptables –L –n –v





# Secure firewall Implementation:





# Do’s and don’t’s

