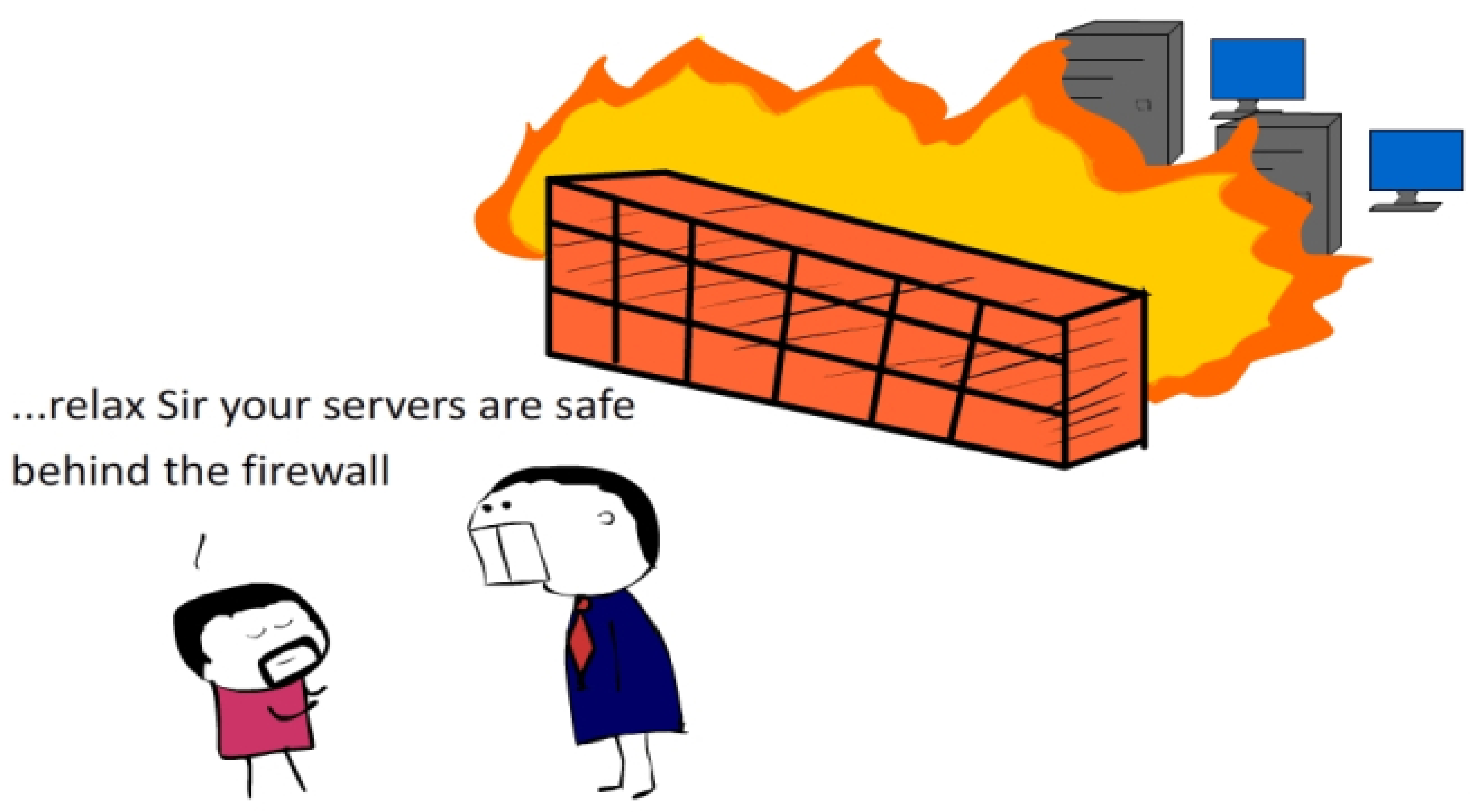
Firewall / UTM

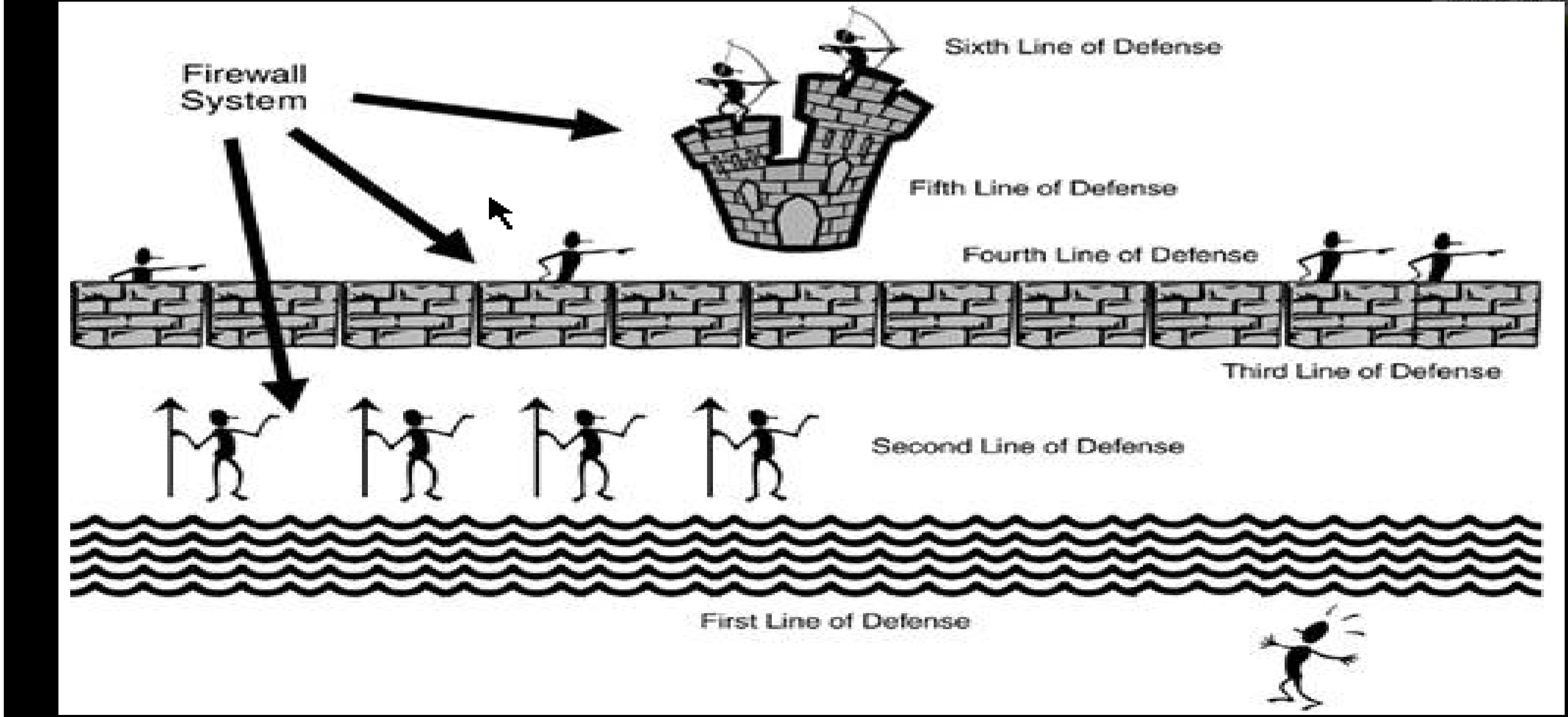
Mirox
Reinforce Your Security


...relax Sir your servers are safe behind the firewall

Topics To Cover :-

- ❑ Introduction
- ❑ Security Features
- ❑ Multiple components of Firewall
- ❑ Firewall Operations
- ❑ Types of Firewalls
- ❑ Firewall Features

❑ Introduction



- ❑ Firewall is a hardware or software system that prevents unauthorized access to or from a network.

- ❑ Firewall monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

- ❑ Firewall typically establishes a barrier between a trusted, secure internal network and another outside network.

- ❑ Controlling inbound and outbound communications on anything from a single machine to an entire network.

- ❑ Firewalls operate in two ways, by either denying or accepting all messages based on a list of designated acceptable or unacceptable sources.

(UTM) Unified Threat Management

- ❑ A new category of network security products.
- ❑ Perform content filtering
- ❑ Spam filtering
- ❑ Application control
- ❑ Web content filtering
- ❑ Intrusion detection and Antivirus duties
- ❑ Malicious activity on the computer network

❑ Security Features

❑ Identify and control applications on any port.

➢ Facebook or Yahoo, instant messaging applications, peer-to-peer file sharing like UTorrent, or VOIP.

❑ Identify and control circumventors.

➢ Hackers use proxies, remote access, and encrypted tunnel applications.

➢ Firewall solution must be capable of dealing with these types of circumventors.

❑ Decrypt outbound SSL.

➢ Firewall must be capable of decrypting and inspecting SSL traffic.

➢ Flexible enough to bypass selected segments of SSL traffic via policy.

❑ Provide application function control.

➢ WebEx vs. WebEx Desktop Sharing and Yahoo, Instant Messaging vs. the file transfer feature.

➢ IT environments heavily dependent on their sensitive intellectual property.

- ❑ Scan for viruses and malware in allowed applications.

  - ➢ Enterprises continue to adopt collaborative applications hosted outside the physical locations. Google Drive, Google Docs, DropBox, etc..

  - ➢ Many infected documents are stored in collaboration applications, along with some documents that contain sensitive information.

- ❑ Deals with unknown traffic by policy.

  - ➢ Firewall must attempt to classify all traffic, which provides a positive enforcement model.

❑ Identify and control applications sharing the same connection.

➢ Firewall must recognize and enable the appropriate policy response for each of applications.

➢ Platform such as Google, Facebook, Microsoft etc..

❑ Enable the same visibility and control for remote users.

➢ Employees working remotely and they expect to connect to their applications via WiFi, wireless broadband etc..

❑ Make network security simpler.

➢ Firewall must apply policy based on the user and application which significantly simplifies policy modeling and management.

❑ Deliver the same throughput and performance with application control fully activated.

➢ Firewall must have hardware optimized for specific tasks such as networking, security and content scanning and perform all those tasks without sacrificing speed or safety.

❑ Deep Packet Inspection DPI.

➢ Deep packet inspection (DPI) is one of the prior features of next-generation firewall (NGFW).

➢ Ensures the various pieces of each packet are thoroughly examined to identify malformed packets, errors, known attacks and any other anomalies.

➢ Can rapidly identify and then block Trojans, viruses, spam, intrusion attempts and any other violations of normal protocol communications.

□ Multiple components of Firewall

Firewall	Creating a Strong Firewall Security Policy
Mobile Access	Remote Access to the Network
IPsec VPN	Creating VPN Policies
Identity Awareness	Adding Users to the Security Policy
URL Filtering	Defining an Internet Access Policy
Application Control	
Anti-Bot	Threat Prevention Policies
Anti-Virus	
Anti-Spam	
Data Loss Prevention	Securing Data
Advanced Networking & Clustering	Maximizing Network Performance
SmartEvent	Monitoring and Logging
SmartLog	

❑ Firewall Operations

❑ Filter incoming network traffic based on source or destination.

➢ Stopping unwanted traffic from entering the network.

❑ Filter outgoing network traffic based on source or destination.

➢ Firewalls can also screen network traffic from internal network to the Internet.

➢ Prevent employees from accessing inappropriate websites.

- ❑ Filter network traffic based on content.

  - ➢ Firewall integrated with a virus scanner can prevent files that contain viruses from entering the network.

  - ➢ Firewalls integrate with email services to screen out unacceptable emails.

- ❑ Detect and filter malware.

  - ➢ Botnets and malware have driven firewall manufacturers to implement features designed to detect infected hosts through packet inspections.

- Make internal resources available.
  - Configure many firewalls to enable selective access to internal resources, such as a public web server.
  - Can accomplish this by using a DMZ, which is where the public web server would be located.

- Allow connections to internal network.
  - Common method for employees to connect to a network is using virtual private networks (VPN).
  - VPNs can also connect branch offices to each other over the Internet, saving on WAN costs.

❑ Report on network traffic and firewall activities.

- Firewall can also log activity to a syslog or other type of archival storage receptacle.

- Perusing firewall logs after an attack occurs is one of a number of forensic tools.

❑ Types of Firewalls

- ❑ Hardware Firewall
- ❑ Software Firewall
- ❑ Packet-filtering Firewalls/Network Layer Firewalls
- ❑ Circuit-level gateways
- ❑ Stateful inspection Firewalls
- ❑ Application-level gateways (proxies)
- ❑ Multilayer inspection Firewalls
- ❑ Application Layer Firewalls
- ❑ Web Application firewall (WAF)

❑ Hardware Firewall

SONICWALL
WatchGuard
paloalto NETWORKS
FORTINET
Juniper NETWORKS
STONESOFT
Real World Business Security
CISCO
Check Point
SOFTWARE TECHNOLOGIES LTD.

➢ Can protect every machine on a local network.

➢ A hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination.

➢ Compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.

❑ Software Firewall

pfSense
clearOS
IPFire
untangle
smoothwall

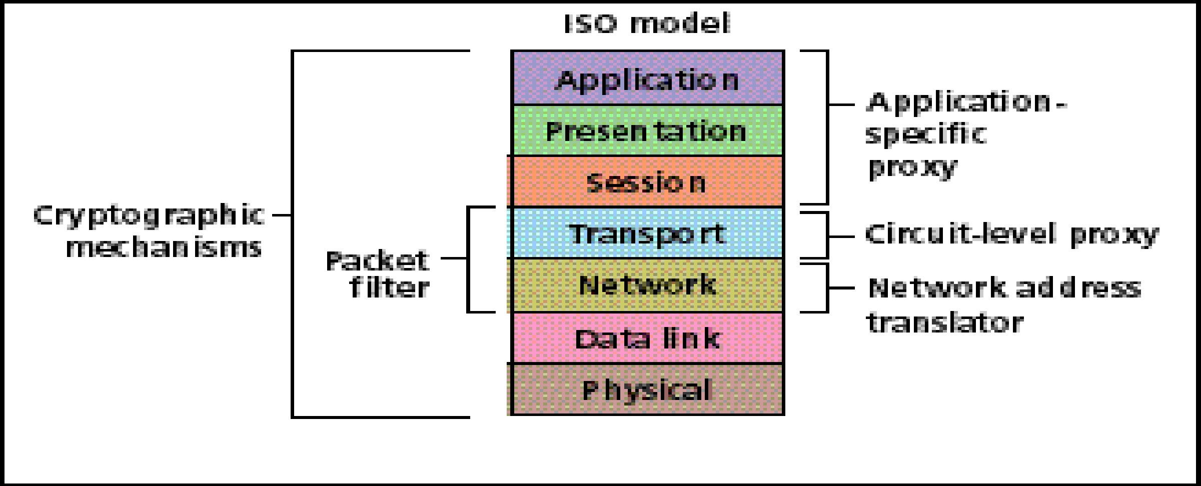
- ➢ Software firewalls are installed on your computer like any software.

- ➢ Protect your computer from outside attempts to control or gain access your computer.

- ➢ Provide protection against the most common Trojan programs or e-mail worms.

- ➢ Software firewalls may also incorporate privacy controls, web filtering and more.

❑ Packet-filtering Firewalls/Network Layer Firewalls

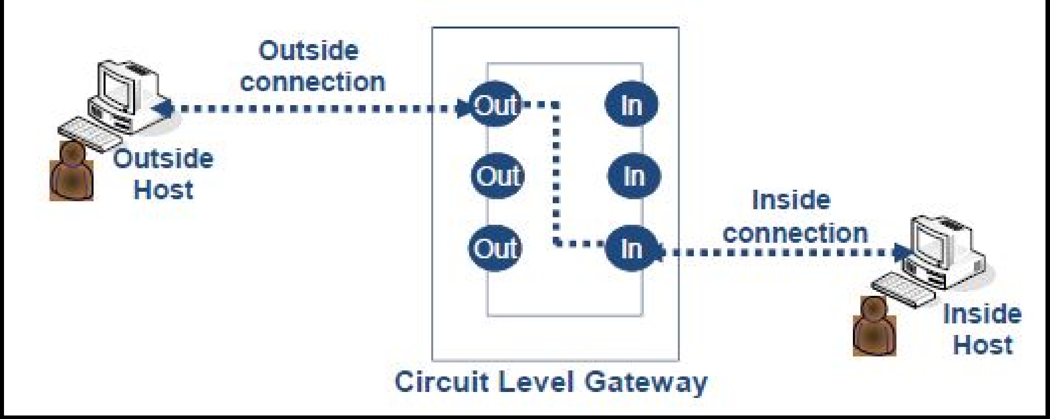


➢ A Packet filtering firewall applies a set of rules to each incoming and outgoing IP packet the forwards or discards the packet.

➢ Filtering rules are based on information contained in a network packet

- Source IP address
- Destination IP address
- Source and destination transport level access
- IP protocol field
- Interface

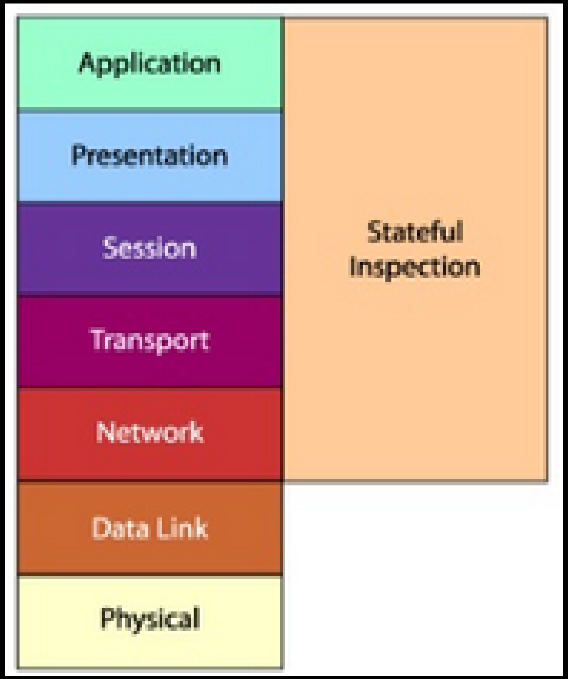
❑ Circuit-level gateways



- ➢ Works at Session Layer of the OSI model or the TCP layer of TCP/IP.

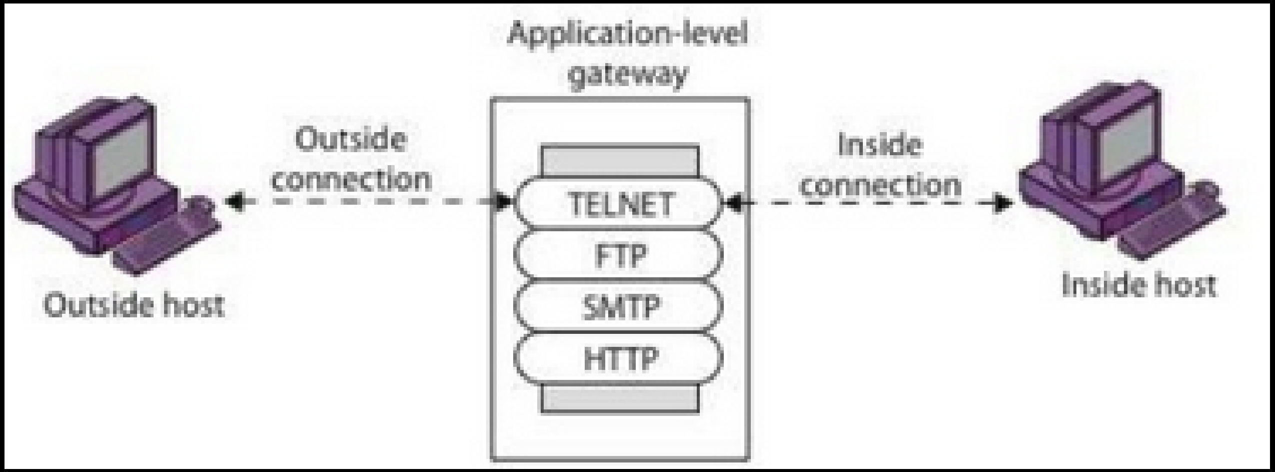
- ➢ Monitor the TCP handshaking going on between the local and remote hosts to determine whether the session being initiated is legitimate or trusted.

❑ Stateful inspection Firewalls



➢ Examines the Packet Header information from the Network Layer of the OSI model to the Application Layer to verify that the packet is part of a legitimate connection and the protocols are behaving as expected.

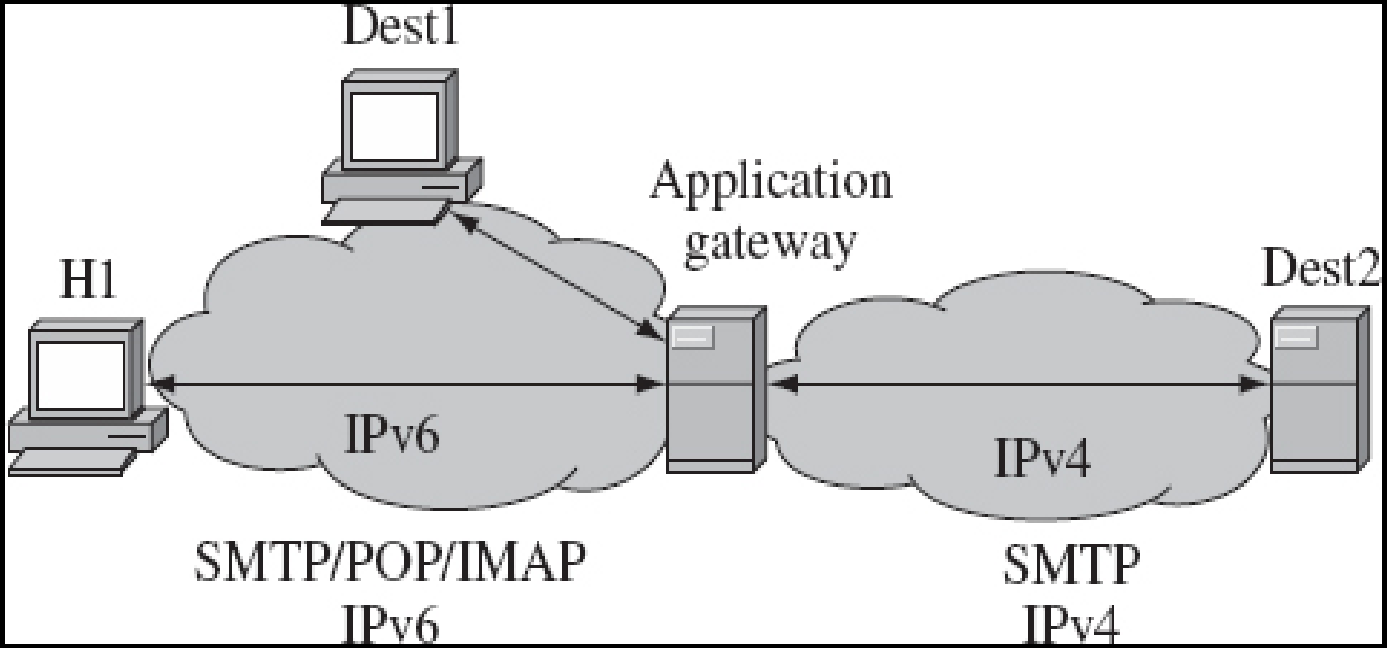
❑ Application-level gateways (proxies)



- ➢ Application proxy or application-level proxy, an application gateway is an application program that runs on a firewall system between two networks.

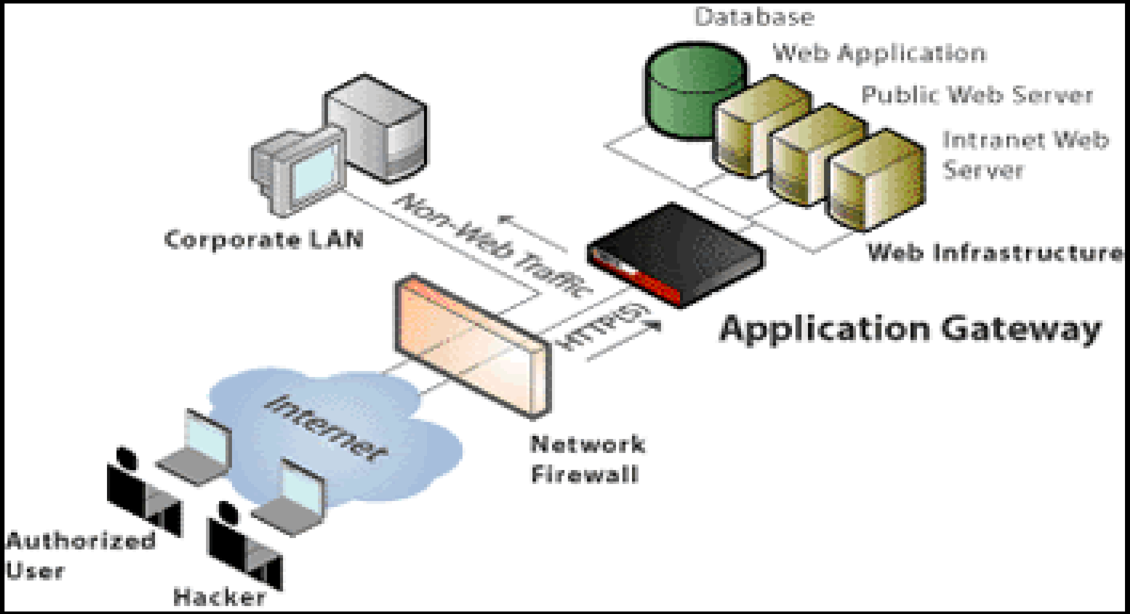
- ➢ Client program establishes a connection to a destination service, it connects to an application gateway, or proxy.

❑ Multilayer inspection Firewalls



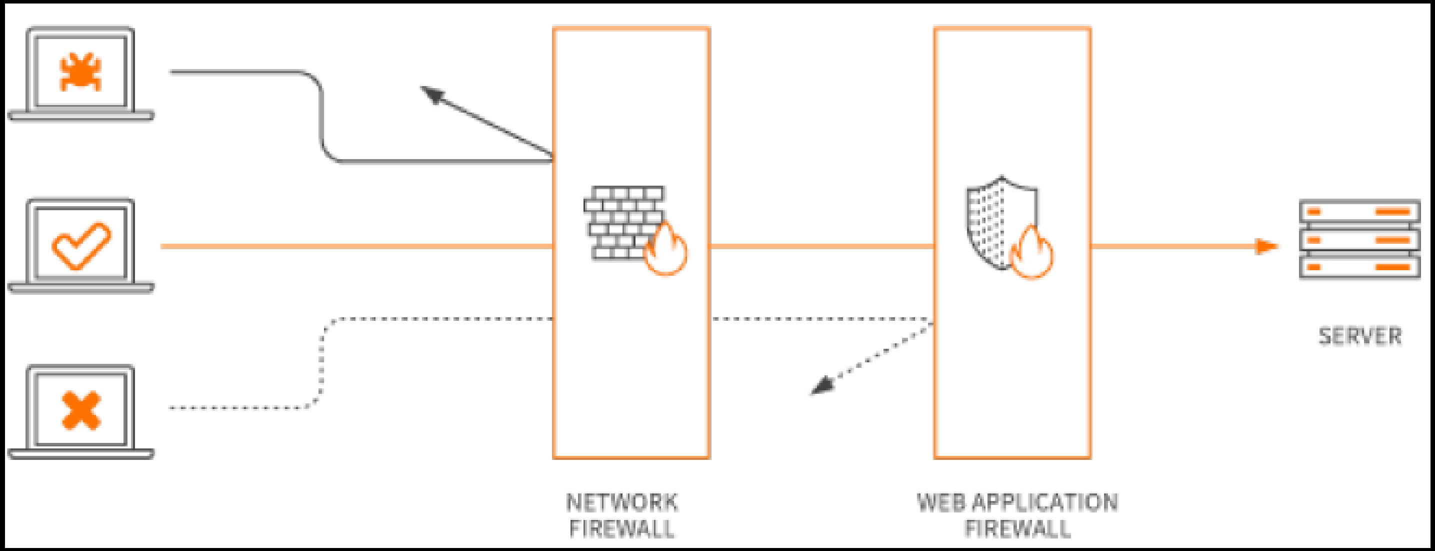
➢ Multilayer firewalls work by retaining the status (state) assigned to a packet by each firewall component through which it passes on the way up the protocol stack.

❑ Application Layer Firewalls



- ➢ Application-layer filtering is the ability to block specific content, such as known malware or certain websites, and recognize when certain applications and protocols such as HTTP, FTP and DNS.

❑ Web Application firewall (WAF)



- WAFs are designed to protect web applications/servers from web based attacks that IPSs cannot prevent.

- It monitors traffic before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns.

❑ Firewall Features

- Able to monitor SSL or other encrypted traffic.
- Integration with other security solutions.
- Inbuilt Antivirus and Anti-Bot solution.
- Centralized Management, Administration, Logging and Reporting.
- State-full Inspection.
- Deep Packet Inspection.
- Integrated IPS.
- Application Awareness.
- Identity Awareness.

THANK YOU !!!