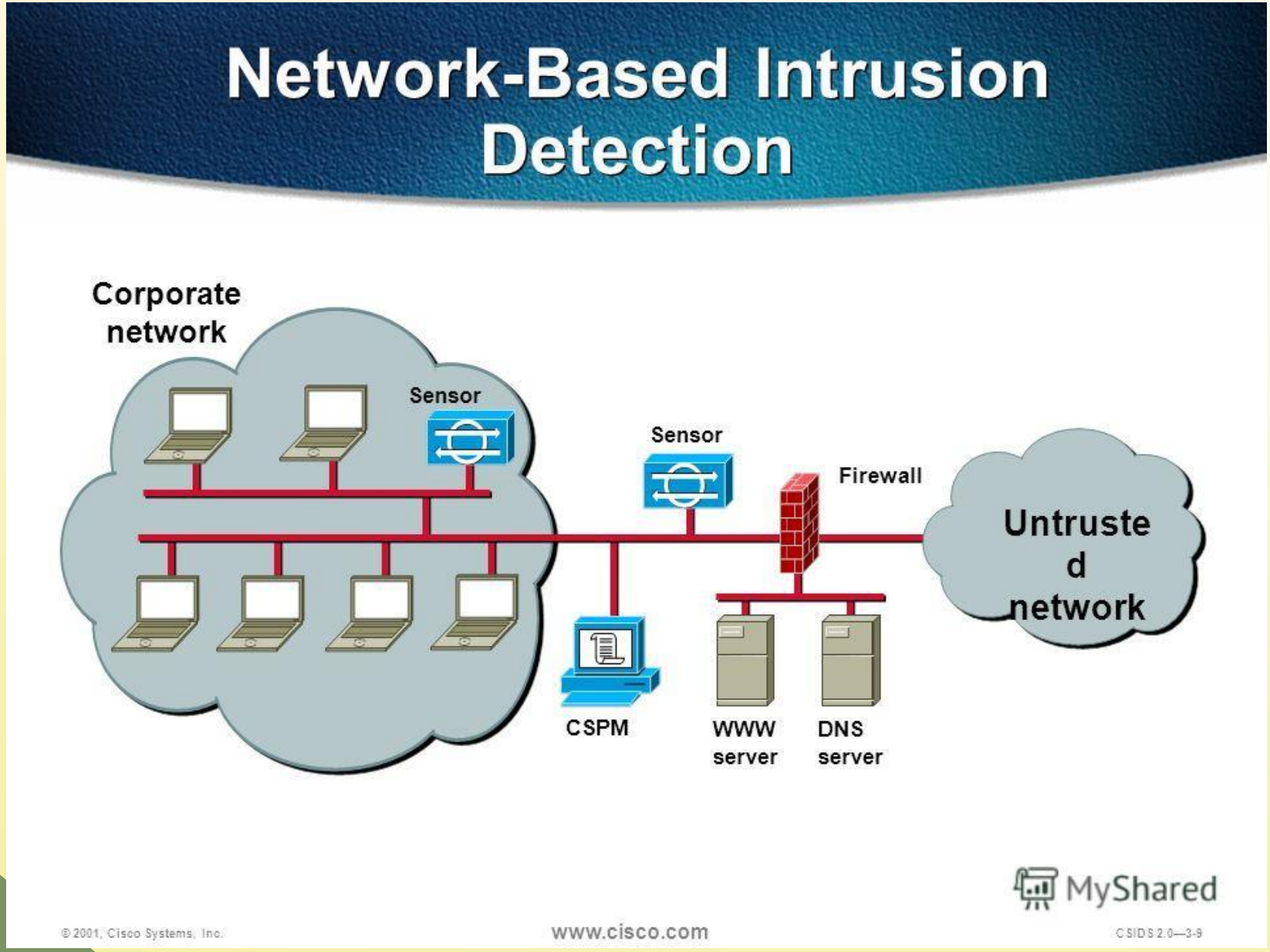
Firewalls

By Sreenidhi

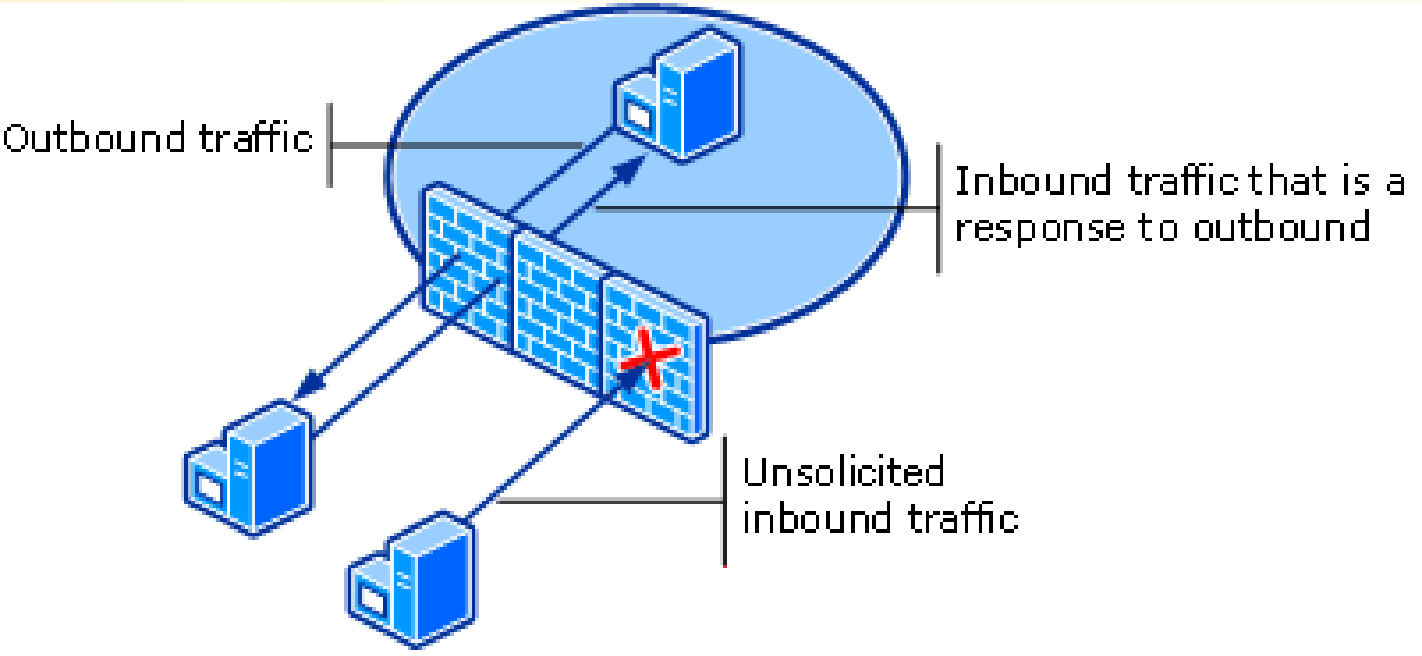
Introduction to firewall

- A firewall is a security system designed to prevent unauthorized access on a private network
- It is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.
- Hardware or Software firewalls.
- The Uncomplicated Firewall (ufw is available on Ubuntu systems by default) is a front-end for iptables and is particularly well-suited for host-based firewalls.
- ufw provides a framework for managing netfilter, as well as a command-line interface for manipulating the firewall.
- Windows in-built firewall.

Network based firewall



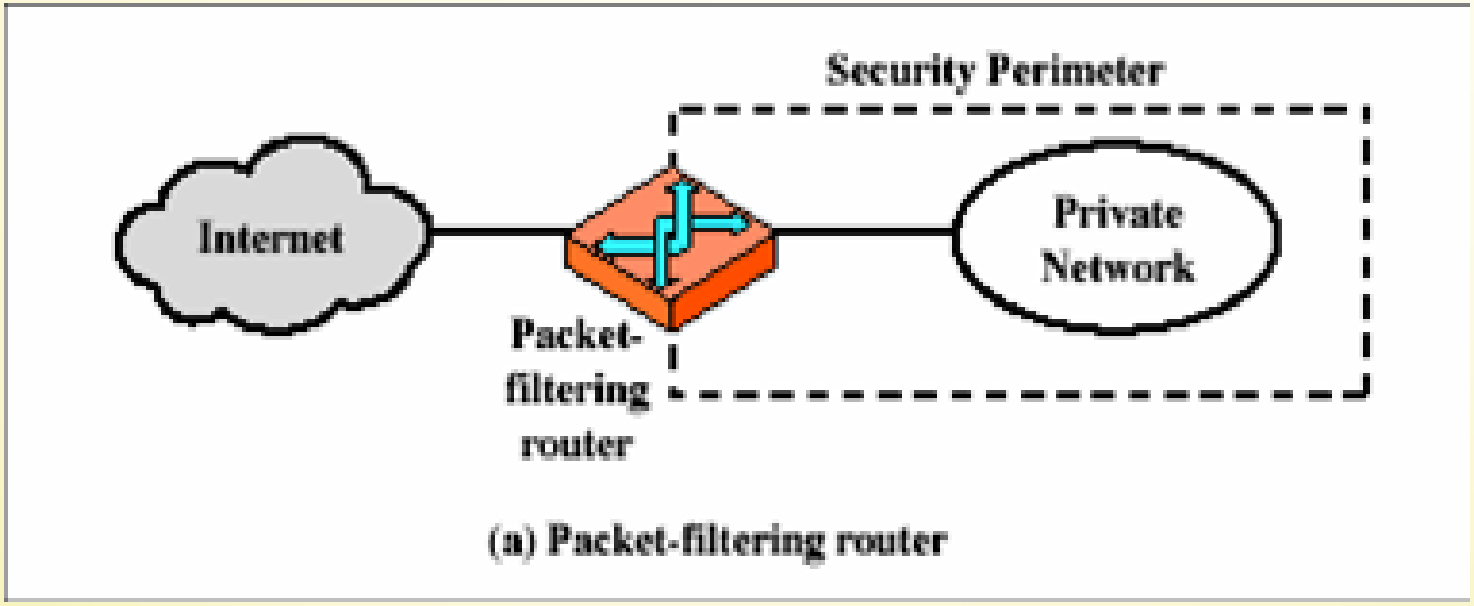
Host based firewall



1st Generation – Packet filters

- Firewalls (initially packet filtering routers) were implemented as a system to check the incoming packets
- The **IP addresses of source and destination, port numbers and protocol types** were checked.
- Worked mainly on first 3 layers of OSI model – **Physical, Data link and Network.**
- **Limitations:**
- **IP address spoofing -** fake IP addresses
- **Source routing attacks -** To find the route that packets take through a network, attackers use IP source route attacks. The attacker sends an IP packet and uses the response from the network to get information about the operating system of the target computer or network device.
- **Tiny fragment attacks -** A Tiny Fragment attack is IP fragmentation that is the process of breaking up a single Internet Protocol (IP) datagram into multiple packets of smaller size

Packet filtering routers



2nd Generation -Stateful firewall

- Only packets matching **a known active connection** are allowed to pass the firewall.
- Stateful packet inspection (SPI), also referred to as dynamic packet filtering, is a security feature often included in business networks.
- **Works on first 4 layers of OSI Model, i.e. Transport layer as well.**

Stateful firewalls with TCP

- **TCP is a stateful protocol** as connections are established with a three-way handshake ("SYN, SYN-ACK, ACK") and ended with a "FIN, FIN-ACK, ACK" exchange.
- All packets with **"SYN"** in their header received by the firewall are interpreted as to open new connections.
- If the service requested by the client is available on the server, it will respond with a **"SYN-ACK"** packet which the firewall will also track.
- **Once the firewall receives the client's "ACK" response, it transfers the connection to the "ESTABLISHED" state as the connection has been authenticated as bidirectional.**
- This allows tracking of future packets through the established connection.
- **The firewall drops all packets which are not associated with an existing connection recorded in its state table (or "SYN" packets)**

Stateful firewalls with UDP, ICMP

- **UDP and ICMP, are not based on bidirectional connections like TCP**, making a stateful firewall somewhat less secure.
- To track a connection state in these cases, a firewall must transfer sessions to the ESTABLISHED state after seeing the first valid packet.
- It can then only track the connection through addresses and ports of the following packets' source and destination.
- Unlike TCP connections, which can be closed by a "FIN, ACK" exchange, these connectionless protocols allow a session to end only by time-out.

Example: Stateful Inspection Packet Filter

Table : Stateful Firewall Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.212.212	1046	192.168.1.6	80	Established

Application Layer Firewalls

- The key benefit of application layer filtering is that it can "understand" certain applications and protocols (such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP)).
- Helps to detect if an unwanted application or service is attempting to bypass the firewall using a protocol on an allowed port, or detect if a protocol is being abused in any harmful way.
- Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis.

Application proxy or gateway firewalls

- A proxy server (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets.
- Firewalls often have network address translation (NAT) functionality.
- A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.
- An application gateway firewall uses software to intercept connections for each Internet protocol and to perform security inspection. It involves what is commonly known as proxy services.

- Many information security experts believe proxy firewalls offer the highest degree of security because the firewall does not let endpoints communicate directly with one another. Thus, a vulnerability in a protocol that could slip by a packet filter or stateful packet inspection firewall could be caught by the proxy program.
- In addition, the proxy firewall can offer the best logging and reporting of activities.
- Stateful multilevel inspection, or SMLI firewalls eliminate the redundancy and CPU-intensive nature of proxy firewalls.
- SMLI's unique approach screens the entire packet, OSI layers 2 through 7, and rapidly compares each packet to known bit patterns of friendly packets before deciding whether to pass the traffic.
- A **bastion host** is a special purpose computer on a network specifically designed and configured to withstand attacks.

Distributed Firewalls

- A central management system for designing the policies.
- A transmission system to transmit these polices.
- Implementation of the designed policies in the client end.
- Overcome single point of failure drawback

Distributed Firewalls

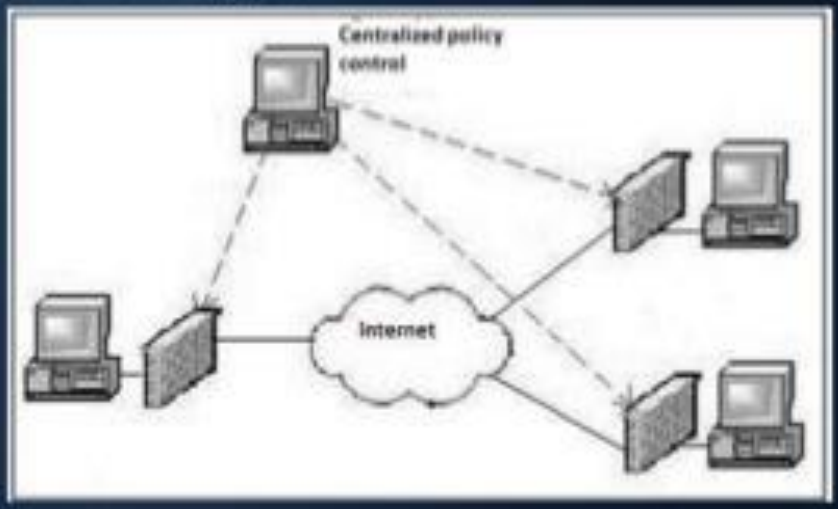
Distributed firewalls are mechanisms that enforce centrally managed security policies that are distributed to endpoints, forming a distributed firewall system.

Design of distributed firewalls are based on three elements:

- Keynote – Firmato: A general policy language for defining security policies.
- Web Server: Mechanism to distribute security policies.
- IPSec: Security protocol that provides network level encryption.

Examples of Distributed Firewalls

- Network Edge Security (NES)
- Distributed Embedded Firewall (EFW)
- Automatic Distributed Firewall (ADF)
- Stateful Clustered Security Gateway (Stateful CSG)



(Ramsurrun and Soyjaudah, 2009)

- http://www.wideband.net.au/blog/host-based-vs-network-based-firewalls/
- http://www.webopedia.com/DidYouKnow/Hardware_Software/firewall_types.asp
- https://www.icsalabs.com/products