Firewall

Introduction of Firewall in Computer Network

.

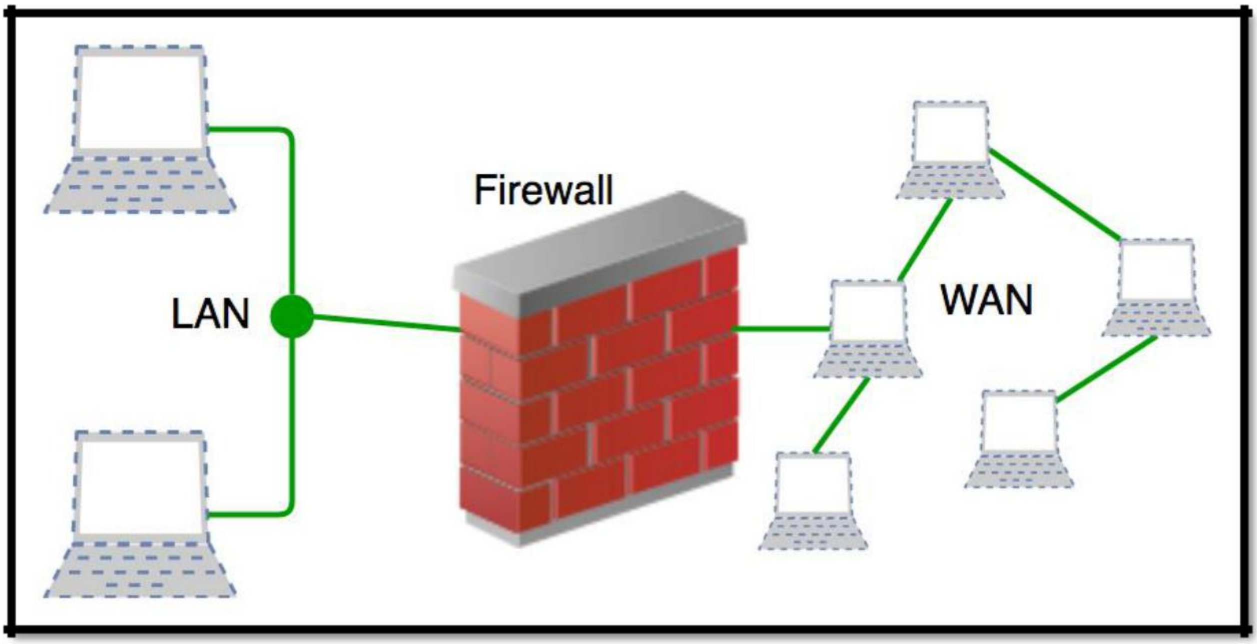
A firewall is a network security device, either hardware or software -based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic

Reject : block the traffic but reply with an "unreachable error"

Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



History and Need for Firewall

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.

But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type code instead of port number which identifies purpose of that packet.

Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop).

Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow t he default policy. If default policy on the firewall is set to accept, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as drop (or reject) is always a good practice.

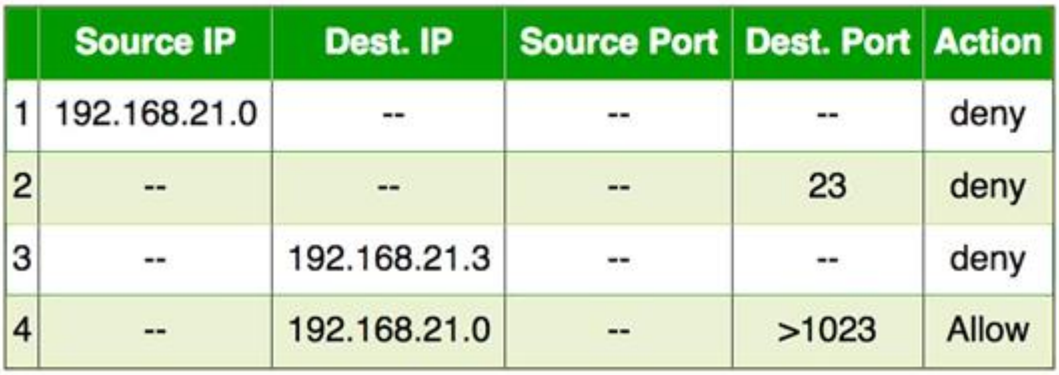
Generation of Firewall (TYPES OF FIREWALLS)

Firewalls can be categorized based on its generation.

<u>First Generation- Packet Filtering Firewall:</u>

Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers).

Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers. Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered according to following rules:

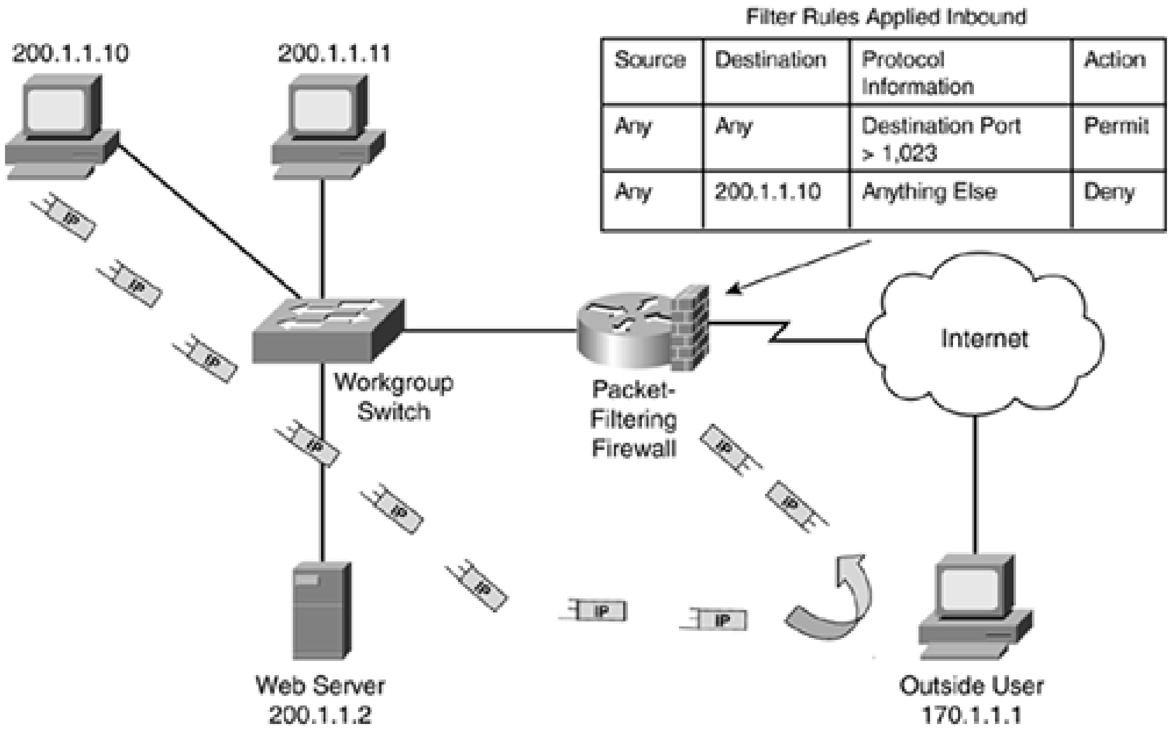


	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

Incoming packets from network 192.168.21.0 are blocked.
Incoming packets destined for internal TELNET server (port 23) are blocked.
Incoming packets destined for host 192.168.21.3 are blocked.
All well-known services to the network 192.168.21.0 are allowed.

- It is the simplest and easy to implement firewall
- If this firewall is placed just behind the router, then the traffic can be analyzed easily.
- The biggest disadvantage of the packet filtering firewalls is that it requires a lot of detailing to set policies.



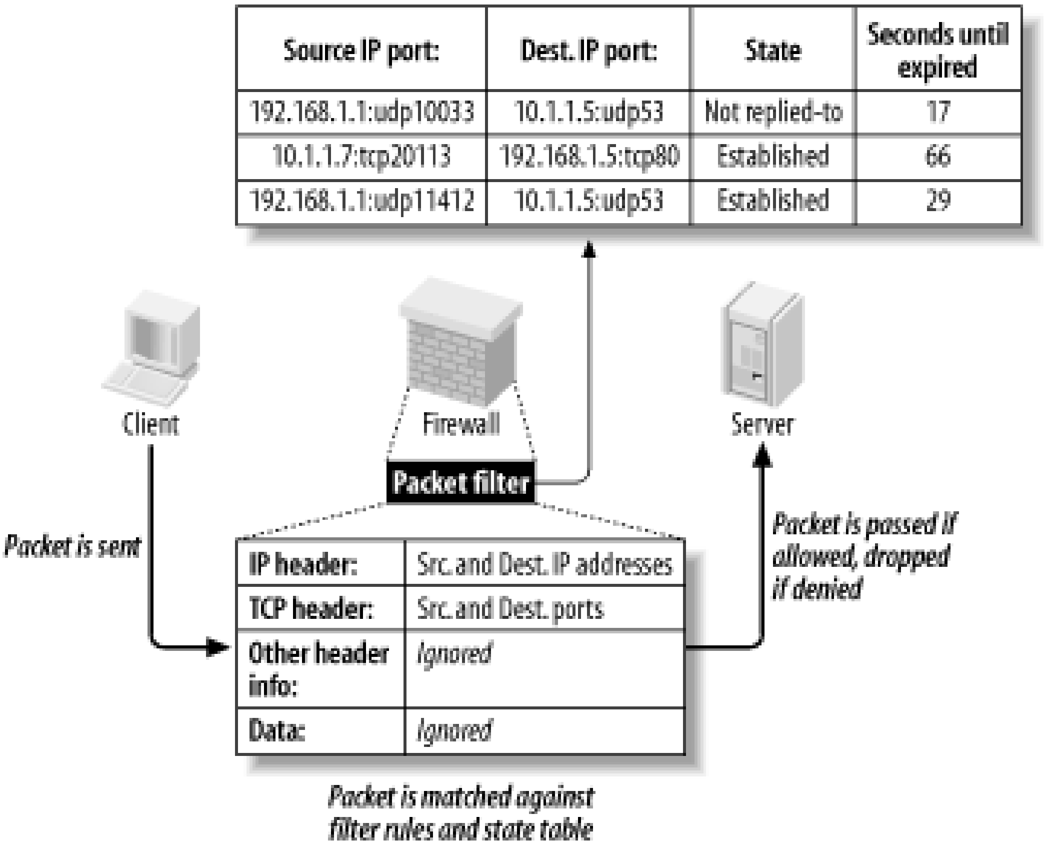
Filter Rules Applied Inbound

Source	Destination	Protocol Information	Action
Any	Any	Destination Port > 1,023	Permit
Any	200.1.1.10	Anything Else	Deny

Second Generation: Stateful Inspection Firewall:

Packet Filtering is done 1 packet at a time. Sometimes the attackers may use this technique for their attacks. Attackers can split their complete script of attack into different packets so that the complete script of attack cannot be identified by the packet filtering firewall. To avoid this, stateful inspection firewalls were introduced which keeps record of the states of the packets from one to another.

Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So, the filtering decisions would not only be based on defined rules, but also on packet’s history in the state table.



Source IP port:	Dest. IP port:	State	Seconds until expired
192.168.1.1:udp10033	10.1.1.5:udp53	Not replied-to	17
10.1.1.7:tcp20113	192.168.1.5:tcp80	Established	66
192.168.1.1:udp11412	10.1.1.5:udp53	Established	29

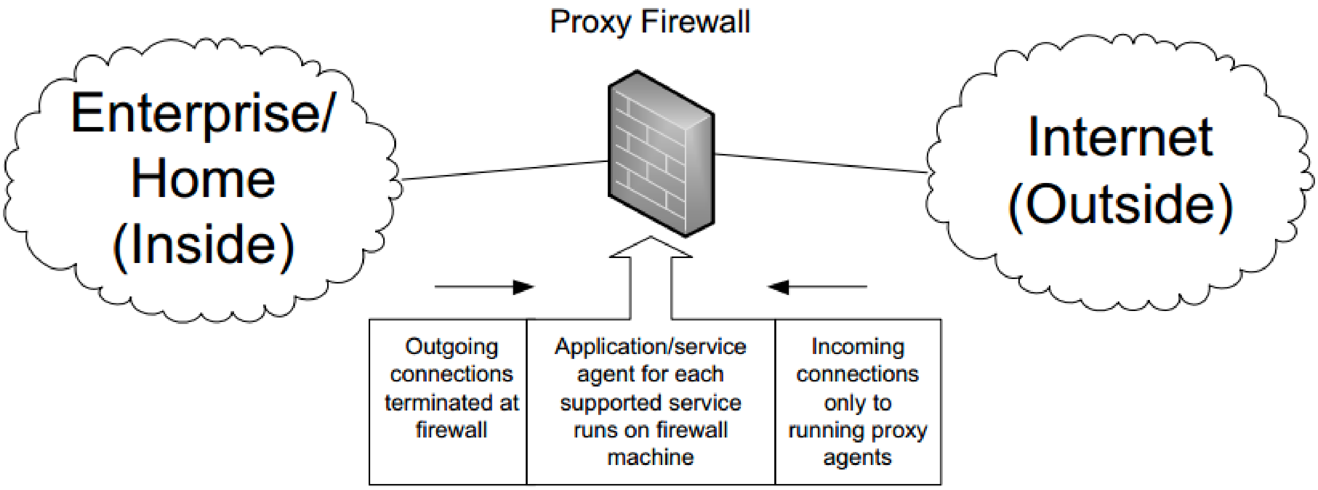
IP header:	Src. and Dest. IP addresses
TCP header:	Src. and Dest. ports
Other header info:	*Ignored*
Data:	*Ignored*

Client
Firewall
Server
Packet filter
Packet is sent
Packet is passed if allowed, dropped if denied
Packet is matched against filter rules and state table

Third Generation- Application Layer Firewall (Proxy Firewalls):

Packet filters cannot see the content of each packet. From the packet headers, they just get the IP addresses for filtering. Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.

In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.


Proxy Firewall
Enterprise/ Home (Inside)
Internet (Outside)
Outgoing connections terminated at firewall
Application/service agent for each supported service runs on firewall machine
Incoming connections only to running proxy agents

Personal Firewalls:

A personal firewall is software application that shields internet users from potential hackers by permitting or denying network traffic to and from their computer and warning them about attempted intrusions. It’s like a filter between the Internet and your network.

A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.[1] Typically it works as an application layer firewall.

A personal firewall differs from a conventional firewall in terms of scale. A personal firewall will usually protect only the computer on which it is installed, as compared to a conventional firewall which is normally installed on a designated interface between two or more networks, such as a router or proxy server. Hence, personal firewalls allow a security policy to be defined for individual computers, whereas a conventional firewall controls the policy between the networks that it connects.

Common personal firewall features:

- Block or alert the user about all unauthorized inbound or outbound connection attempts.
- Allows the user to control which programs can and cannot access the local network and/or Internet and provide the user with information about an application that makes a connection attempt.
- Hide the computer from port scans by not responding to unsolicited network traffic.
- Monitor applications that are listening for incoming connections.
- Monitor and regulate all incoming and outgoing Internet users.
- Prevent unwanted network traffic from locally installed applications.

- Provide information about the destination server with which an application is attempting to communicate.
- Track recent incoming events, outgoing events, and intrusion events to see who has accessed or tried to access your computer.
- Blocks and prevents hacking attempt or attack from hackers.

Next Generation Firewalls (NGFW):

Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

Some common features of next-generation firewall architectures include deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and surface-level packet inspection. Next-generation firewalls may include other technologies as well, such as intrusion prevention systems (IPSs) that work to automatically stop attacks against your network.

LIMITATIONS OF FIREWALLS

A firewall may be a pivotal component of securing your organization and is planned to address the issues of information integrity or activity verification (through stateful inspection firewalls) and secrecy of your inner network (through application proxies). Although there are some inherent limitations of the firewalls as mentioned below:

1) Viruses: Not all firewalls have full protection against computer viruses because viruses use different encoding techniques to encode files and transfer them over internet.

2) Architecture: Firewall architecture depends upon single security mechanism failure. If that security mechanism has a single point of failure, it will affect the entire firewall program which opens the loopholes to the intruders.

3) Configuration: Firewalls doesn’t have a mechanism to tell administrators about any incorrect configuration. Only trained professionals in the field of network security can configure a firewall properly.

4) Monitoring: Firewalls doesn’t give notifications about hacking. It will notify only about threat occurrences.

5) Masquerading: Firewalls can’t stop hackers who steal login information of authentic users to gain access to a secure network. Once the attacker gains complete access to the entire network, he/she can delete or change the network policies of the organization.

……..

ROUGH WORK