CHAPTER 3: SECURING NETWORKS 2
PART 1: FIREWALLS 2
Learning Objectives 2
1.1 Introduction 2
1.2 Firewall 2
1.2.1 Firewall Functionalities 3
1.2.2 Firewall types 5
1.2.3 Firewall Configurations 7
1.2.4 Common Implementation Structures of Firewalls 11
1.2.5 Limitations of Firewalls 15
1.2.6 Firewall Product Types 15
1.2.7 Unified Threat Management 16
1.2.8 Firewall Life Cycle 17
1.2.9 Baseline Configuration for Firewalls 18
1.3 Summary 18
1.4 References 19

CHAPTER 3: SECURING NETWORKS
PART 1: FIREWALLS

Learning Objectives

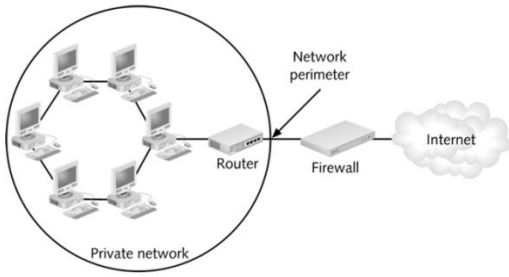
- To gain understanding of Firewalls
- To gain an overview of types of Firewalls
- To gain an understanding of Common Implementations of Firewalls
- To understand Limitations of Firewalls
- To get an overview of Unified Threat Management
- To understand Firewall Life Cycle
- To understand Baseline Configuration of Firewalls

1.1 Introduction

With the increased use of networked systems, the threat profile to organisations' information assets has increased manifold. Organisations' information resources are accessed by users from different access points. Further internal users also need to access Internet. However, while Internet access provides benefits, it enables the outside world to reach and interact with local network assets, creating a threat to the organisation. This exposes assets to attacks, both malicious and unintentional.

1.2 Firewall

Firewall is a system or group of systems to enforce Control policy. Firewalls are an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet. Firewall may be a hardware device or a software program running on a secure host computer, or a combination of hardware and software. Firewalls and associated technical controls have become fundamental security tools. Firewall is deployed at the perimeter of the network, i.e. the entry point. (The term 'Firewall' is coined after the firewalls which are used to prevent the spread of Fire from one area to another; in this case, they limit the damage that could spread from one subnet to another).



Firewall – at the perimeter of the organisation's intranet

As an access control mechanism, the firewall enforces the security policy between an organisation's secured network and the unsecured environment. Based on the rules configured, it filters the traffic both in-bound and outbound from the secured network and determines,

- Which inside machines, applications and services may be accessed from outside,
- Who outsiders are permitted access to internal and what resources, and
- Which outside services, the insiders may access.

In general, the design goals for a firewall are:

- All traffic from inside (secured) to outside (unsecured), and vice versa, must pass through the firewall.
- Only authorised traffic, defined by the local security policy, will be allowed to pass the firewall.

1.2.1 Firewall Functionalities

Fundamentally, firewalls perform the following tasks:

- **Manage and control network traffic** - Firewalls typically do so by inspecting the packets and monitoring the connections that are being made, and then filtering connections based on the packet-inspection results and connections that are observed.
- **Authenticate access** - if the authentication is not successful, the packet would be dropped even though it was permitted based on inspection and the state of the connection. Authentication can be carried through
    - User name/ID and password of the user initiating the connection prior to allowing the connection to be established. Once the connection has been authenticated and authorised by the security policy, the user is no longer prompted for authentication for that connection.
    - The use of pubic keys and certificates under the PKI.

    - The use of pre-shared keys among the hosts.
- **Act as an intermediary** - firewall can be configured to act as an intermediary, i.e. proxy in the communications process between two hosts.
- **Protect resources** - firewall can protect the internal resources and can be configured to inspect the actual application data itself (for example, allowing it to differentiate between legitimate HTTP traffic and malicious HTTP traffic) before presenting the data to the protected resource.
- **Record and report on events** - the firewall can be configured to maintain logs that can be examined on the happening of a security event. The firewall can also be configured to issue notifications in form of alerts on firewall policy violation.

Access Control Techniques

The firewalls generally use following techniques to control access and enforce security policy.

- **Service control**: Determines the types of internet services that can be accessed. The firewall may filter traffic on the basis of IP address and TCP port number.
- **Direction control:** Determines the direction in which particular services requests may be initiated and allowed to go through the firewall.
- **User control**: Controls access to a service according to the user who is attempting to access it. This is usually applied to inside users.
- **Behaviour control**: Controls how particular services are used. For example, it may enable external access to only a portion of the information on a local Web server.

Access Control Policy

There are two approaches in configuring the firewall rules that are manifested through the firewall policy

- **Default Deny Policy or Mandatory Access Control Policy**
  Under this policy, the recommended approach is to deny everything and then selectively allow certain traffic through the firewall.
  This will block all traffic on all interfaces in either direction from anywhere to anywhere unless explicitly permitted. This type of policy is normally implemented when dealing with granting access from an untrusted source to a protected system.
- **Allow All Policy or Discretionary Access Control Policy**
  This policy follows the opposite approach. It allows, by default, all access and denies only the traffic that is explicitly configured to be denied. This type of security policy is frequently implemented for granting access from a trusted network to external systems (e.g. Internet).

NAT Technique in Firewalls

Network Address Translation (NAT) allows a network to use one set of network addresses internally and a different set when dealing with external networks. NAT is a now a function of almost every firewall whether in a SOHO (small office home office) environment or implemented in an enterprise. NAT firewalls automatically provide protection to systems behind the firewall because they allow connections that originate from the systems inside of the firewall only. It conceals the internal network.

1.2.2 Firewall types

Network Based Firewall

A network firewall is a device deployed between networks to restrict which types of traffic can pass from one network to another. Organisations typically use one or more network firewalls at their network perimeter to provide protection from external threats. Network-based firewall could be implemented on a perimeter router, multi-layered switch or could be a dedicated firewall.

Network firewalls work by comparing network traffic to a set of rules, each of which typically specifies a network or application protocol and the source and destination of the communication. For example, a rule might permit e-mail to reach the organisation's e-mail server from external hosts.

Host Based Firewalls

A host-based firewall is a piece of software running on a single host that can restrict incoming and outgoing network activity for that host only. They can prevent a host from becoming infected and stop infected hosts from spreading malware to other hosts. Host-based firewall runs on computer running OS such as Windows 7 or UNIX. Host-resident firewalls filter and restrict the flow of packets. These can be implemented on a server also.

Advantages of Host Based Firewall

- Filtering rules can be tailored to the host environment. Host-based firewalls are particularly important for systems that are network-connected but are not protected by network firewalls and other network-based security controls.
- They provide an additional layer of protection on the network. When a new server or host is attached to the network, it can have its own firewall, without the need to change the configuration of the network firewall.

Personal Firewalls

A personal firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side. Personal firewall functionality can be used in the home environment and on corporate intranets. Typically, the personal firewall is a software module

on the personal computer. Personal firewalls assume that outbound traffic from the system is to be permitted and inbound traffic requires inspection.

Personal firewall capabilities are normally built into operating system. In a SOHO environment having multiple computers connected to the Internet, firewall functionality can also be housed in a router that connects all of such computers to a DSL, cable modem, or other network interface. Such a firewall is known as a Personal Firewall Appliance.

Some key terms related to Firewalls

Dual Homed

It simply means house with two doors. It is a computer that has at least two network interfaces (NIC), one connected to secure side other unsecure side.

Demilitarized Zone (DMZ)

The name comes from Demilitarized zone between North and South Korea, where neither North Korean nor South Korean military is present.

In Networks, Demilitarized Zone (DMZ) usually houses the IT components that require public access such as a mail server, web server, etc.

Bastion Host

Bastions are highly fortified projections on the outer walls of forts. Bastions are exposed to outside but are critical to a fort's security and enemy's primary effort is to break the bastions thus making security weak.

Similarly Bastion Hosts are computer systems that have Hardened systems because they are vulnerable to attack, as they are exposed to the Internet and are a main point of contact for users of internal networks.

Common characteristics of a bastion host are as follows,

- Its Operating system is hardened, in the sense that only essential services are installed on it.
- It may be configured to require additional authentication before a user is granted access to proxy services.
- It is configured to access only specific hosts.
- It can maintain detailed logs of all traffic.
- It has each proxy independent of other proxies loaded on it.

1.2.3 Firewall Configurations

Packet Filtering Router Firewall

This is the simplest firewall, and is usually implemented on a screening router deployed between the private network and the public network. A router is a device that receives packets from one network and forwards them to another network. The screening router examines the header of every packet of data travelling between the Internet and the corporate network. Packet filtering firewalls work at the network layer of the OSI model, or the Internet layer of TCP/IP model.

The header of a packet would contain:

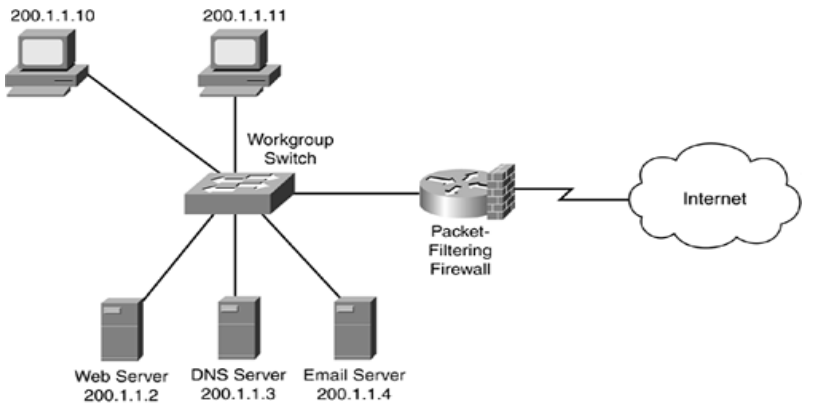
- Type of packet i.e. TCP.UDP, ICMP, IP SEC
- IP Address of Source
- Port Number of Source
- IP Address of Destination
- Port Number of Destination

Firewall rule could be based on any of these.

In case, the rule is matched, and the rule permits, the packet is passed to the next server/device as per the information in the Routing Table of the screening router. If match is found but the rule disallows, the packet is dropped. However, if match is not found, the action to forward or drop the packet is taken as per the default parameter.

Sample Access Control List (ACL)

Source Address	Source Port	Destination Address	Destination Port	Protocol	Action
Any	Any	200.1.1.2	80	TCP	Allow
Any	TCP	200.1.1.3	53	UDP	Allow
Any	TCP	200.1.1.4	25	TCP	Allow
Any	Any	Any other	Any	Any	Deny



Packet Filtering Router

In the above example, the packet filtering router allows access from outside to the Web server (port 80), DNS Server (port 53) and the Email server (port 25). In case any traffic does not meet criteria as per the first three rules, then the last rule is followed and the packets are denied access. As per the above rules, no traffic is permitted to secured servers 200.1.1.10 and 200.1.1.11.

Advantages of Packet Filtering Firewalls

Packet filtering firewalls have two main strengths: speed, and flexibility. They are not very costly and have low impact on network performance.

Limitations of Packet Filtering Firewalls

- Configuring the packet filtering firewalls and defining the Access Criteria poses difficulty.
- Most packet filtering firewalls do not support advanced user authentication schemes.
- Many packet filtering firewalls lack robust logging facilities as only limited information is available to the firewall.

The primary focus of Packet Filtering Firewalls is to limit inbound traffic while providing for outbound and established traffic to flow unimpeded. Thus, packet filter firewalls are very suitable for high-speed environments where logging and user authentication with network resources are not important. Packet filtering firewalls are prone to following types of attacks,

IP Address Spoofing attack

In this type of attack, the attacker fakes the IP address of either an internal network host or a trusted network (outside) host so that the packet will pass the access rules defined in the firewall. For example using a TOR Browser which provides proxy services we can fake our IP address and breach a Packet filtering firewall which has rule to restrict our IP Address.

Source routing attack: In this process, it is possible to define such a route that it bypasses the firewall. To prevent such attacks, all packets wherein source routing specification is enabled may be dropped. However, this control will not be effective where the topology permits a route to be defined.

Tiny Fragment attack: Using this method, an attacker fragments the IP packet into smaller ones and pushes it through the firewall in the hope that only the first of the sequence of fragmented packets would be examined and the others would pass without review.

Stateful Inspection Packet Filtering Firewall

Stateful inspection firewalls are packet filters that incorporate added awareness of the OSI model data. The Stateful Firewalls keep track of the current connection to ensure that only permitted traffic is allowed to pass. Thus, these firewalls filter traffic based on both packet characteristics (like the packet-filtering firewall) as also session checks to make sure that the specific session is allowed.

Stateful inspection firewalls create a directory of outbound TCP connections, along with each session's corresponding client port. This "State Table" is then used to validate any inbound traffic. The Stateful inspection solution is more secure because the firewall tracks client ports individually rather than opening all "high numbered" ports for external access.

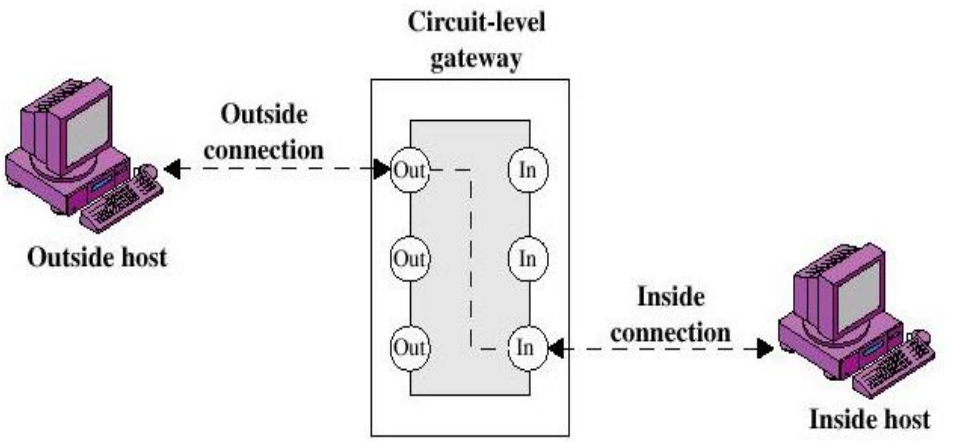
Source Address	Source Port	Destination Address	Destination Port	Action
192.168.1.0	1035	200.12.39.201	80	Established

In this example, as a connection is established between the (source port 1035), with the remote server having port 80, the Stateful inspection firewall makes an entry in the Connection Status table. This state of a connection becomes one of the filtering criteria. If an incoming packet matches an existing connection listed on the table, it will be permitted access without further checking.

Circuit Level Gateways

This type of firewall validates the connections before data is exchanged. It functions at the session layer of the OSI model. A circuit-level gateway relays two TCP connections, one between itself and an inside TCP user, and the other between itself and a TCP user on an outside host. Once the two connections are established, it relays TCP data from one connection to the other without examining its contents. The security function consists of determining which connections will be allowed.

It is typically used when internal users are trusted to decide what external services to access. Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.



Disadvantage of a Circuit Level Gateway

A circuit-level gateway cannot examine the application-level content of the packets it relays between a trusted network and an untrusted network.

Application Level Gateway Firewall

An application-level gateway acts as a relay of application-level traffic. It operates at the Application Layer of OSI model. These are implemented on hardened operating systems. Application level gateways, also called proxies, are similar to circuit-level gateways except that they are application specific. It forces both sides of the conversation to conduct the communication through the proxy. Application level gateway firewalls are capable of permitting or rejecting requests based on the content of the network traffic.

Examples of access control functions that the application-level gateway can process:

- Access control based on content - whether the request contains known exploits?
- Access control based on user authentication- whether the user is permitted to access the resource requested?
- Access control based on source network zone - whether the access to the requested resource from the source network is allowed? For example, certain intranet resources from the Internet may be prohibited access to particular service(s).
- Access control based on source address - whether the sender address is allowed access to the resource?

The working of an Application level gateway firewall is depicted here.

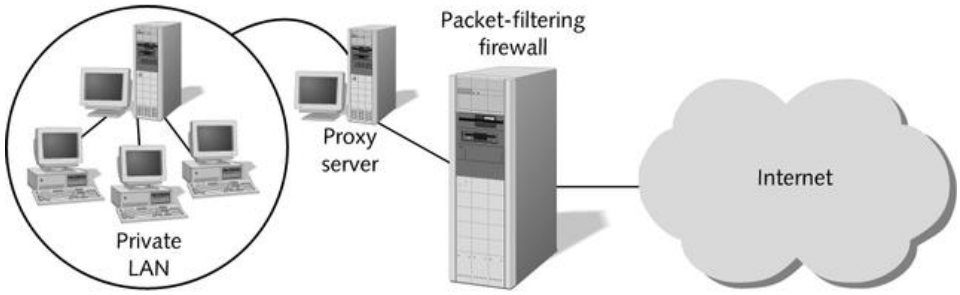


Fig: Application Level Gateway Firewall

Advantages of Application Level Gateway

- Application level gateway (and also the circuit level gateway) firewall systems employ the concept of bastion hosting. Therefore, in the event of a break-in, only the firewall system is compromised, not the entire network.
- Application-level gateways are more secure than packet filters and Stateful Inspection Firewalls as they authenticate individuals and not the devices.
- They can provide auditing and logging functions so that the network traffic can be monitored or analysed at a later time.
- Application level gateways provide complete control over type of service.

Limitations of Application Level Gateway Firewalls

- They are very process intensive and hence can cause performance issues. This can be addressed by using proxy services for critical applications only.
- They are vulnerable to bugs present in the operating system and any application running on the system.

1.2.4 Common Implementation Structures of Firewalls

The deployment strategy for a firewall in an organisation depends upon the objective of the network and the ability of the organisation to implement the architecture. Following are the most common architectural implementations of firewalls:

- Packet filtering routers
- Screened host firewalls
- Dual-homed firewalls, and
- Screened subnet firewalls (DMZ).

Packet Filtering Routers

This is the simplest implementation of a firewall configuration, and is deployed at the perimeter of the network having an untrusted (internet connection). The perimeter routers can be configured to control the passage of packets as per filtering rules defined.

Single Homed Firewalls

This architecture combines the packet filtering router with a separate, dedicated firewall, a Bastion Host acting as application proxy server. The packet filtering router screens the packets before allowing the permitted packed to the proxy server, thus reducing the network traffic and load on the proxy. The application proxy examines an application layer protocol and performs the proxy services.

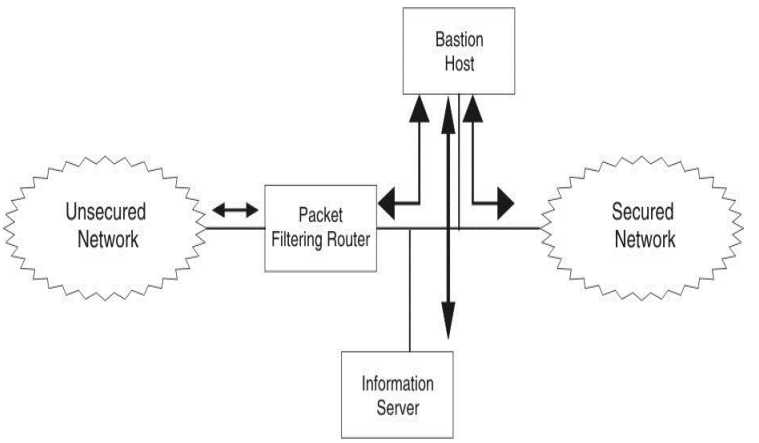


Fig: Single Homed Firewall

Advantages of a Single-homed firewall

- This architecture ensures greater security than a single packet filtering router or an application level gateway firewall alone:
- Its implementation scheme uses both packet-level and application-level filtering, allowing for considerable flexibility in defining security policy.
- An intruder has to penetrate two separate systems before the security of the internal network is compromised.

Limitations

- In this set-up, if the packet filtering router is completely compromised, traffic flows directly through the router between the internet and other hosts on the private network.

Dual-Homed Host Firewalls

In this approach the bastion host is Dual Homed i.e. contains two NICs: one connected to the external network, and one connected to the internal network providing an additional layer of protection by requiring all traffic to go through the Bastion Host to move between the internal and external networks.

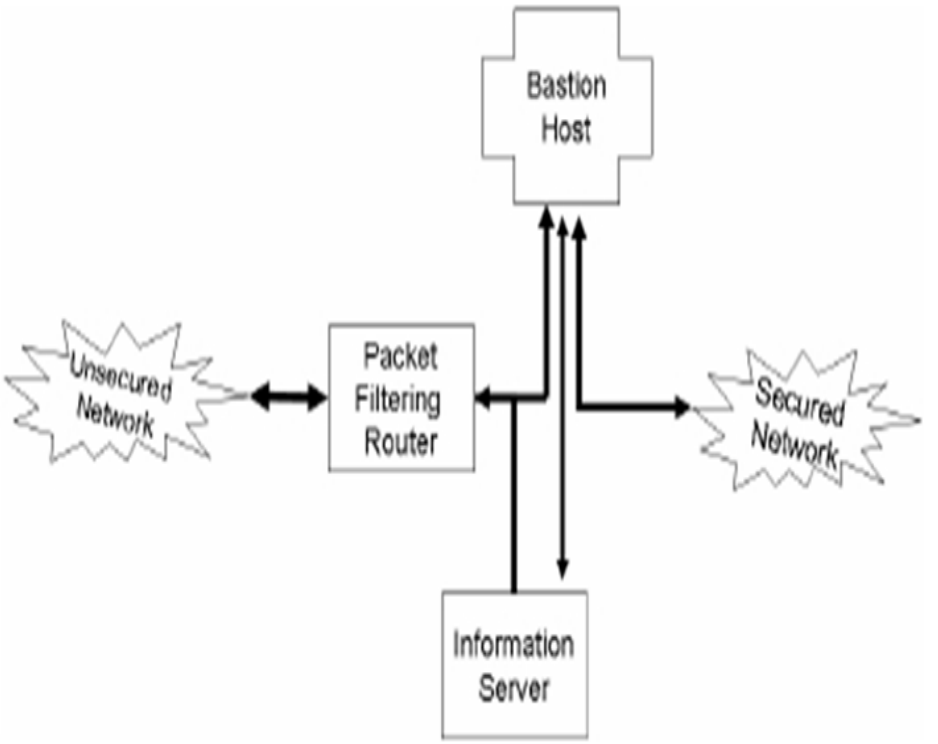


Fig: Dual-homed Firewall

Screened Subnet Firewalls (with DMZ)

The screened subnet firewall configuration is the most secured environment. It has two packet-filtering routers, one between the bastion host and the Internet and the other between the bastion host and the internal network, creating an isolated sub-net. For all incoming traffic, the outside router (the router facing the internet) directs all the packets to the bastion host. The bastion host together with the firewall does preliminary filtering and if the packet passes the test, directs the packet to the less secure or DMZ, the demilitarized zone.

However, where the packet has to travel into the secure network, which is configured as a separate segment, the inside router along with the second firewall provides a second line of defence, managing DMZ access to the private network by accepting only traffic originating from the bastion host. For

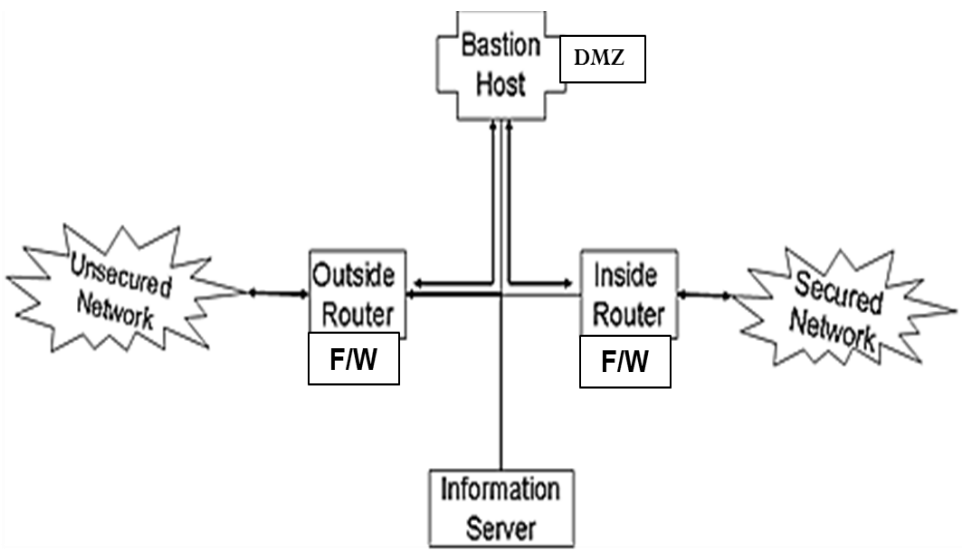
outgoing traffic, the inside router manages private network access to the DMZ network. It permits internal systems to access only the bastion host. The filtering rules on the outside router require use of the proxy services by accepting outgoing traffic only from the bastion host.

It would be observed that in a screened sub-net firewall, the internal network (the private segment) is highly secured. The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity.

The advantages of a screened subnet firewall system are explained here.

An intruder must penetrate three separate devices - the outside router, the bastion host, and the inside router to infiltrate the private network.

- Since the outside router advertises the DMZ network only to the Internet, systems on the Internet do not have routes to the protected private network. This ensures that the private network is invisible.
- Since the inside router advertises the DMZ network only to the private network, its systems do not have direct routes to the Internet. This ensures that inside users access the Internet via the proxy services residing on the bastion host.
- Packet-filtering routers direct traffic to specific systems on the DMZ network, eliminating the need for the bastion host to be dual-homed.
- Since the DMZ network is a different network than the private network, a Network Address Translator (NAT) can be installed on the bastion host to eliminate the need to renumber or re-subnet the private network.



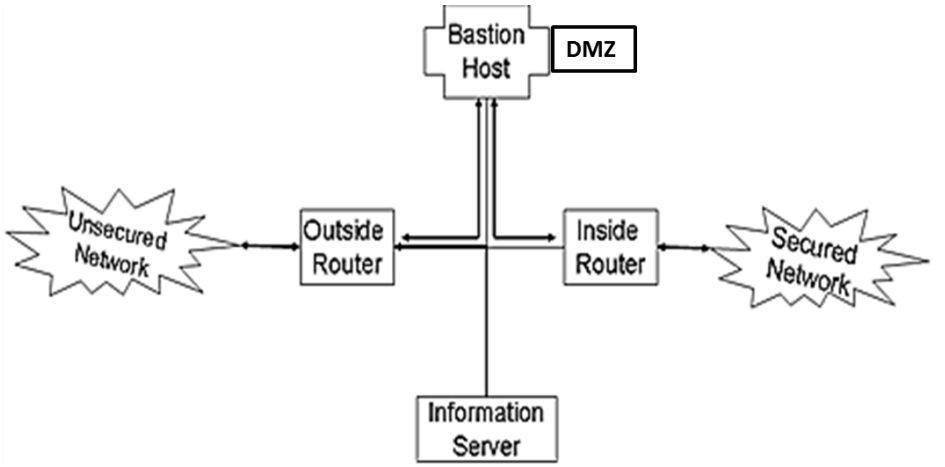


Fig: Screened subnet firewall

1.2.5 Limitations of Firewalls

A firewall is a critical component of network security. It is designed to address the issues of data integrity or traffic authentication and confidentiality of internal network.

The firewalls do have the following limitations:

- A firewall cannot prevent users or attackers with modems from dialling in to or out of the internal network, thus bypassing the firewall and its protection completely.
- Firewalls cannot enforce password policy or prevent misuse of passwords.
- Firewalls are ineffective against non-technical security risks such as social engineering.
- Firewalls cannot stop internal users from accessing websites with malicious code.
- Firewall may not have been implemented on a secured Operating system/hardened system.
- The access list configured in the firewall might not be properly defined, implemented or adequate.
- Network segmentation might not be as per security requirements of the organisation.
- Firewalls cannot provide complete protection against viruses.
- Monitoring of firewall alerts may be inadequate.

1.2.6 Firewall Product Types

The firewall can be either a stand-alone appliance system or it can be implemented on top of a commercial operating system. This depends largely upon the organisation's requirements.

Appliance Based Firewall

The appliances have the firewall software embedded as firmware, making them more secure than those implemented on top of commercial operating systems as appliance based firewalls do not suffer from security vulnerabilities associated with underlying operating systems. These firewalls are faster than firewalls implemented on top of commercial operating systems. However, these firewalls suffer from the scalability issues.

Software Based Firewall

The main advantage of implementing firewalls on top of commercial operating systems is scalability. If an environment requires improved performance, it is usually a simple matter to install a larger system on which to run the firewall software. Most appliances do not offer this level of flexibility or scalability.

The greatest disadvantage of implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that might undermine the security posture of the firewall platform itself. In most cases, vulnerabilities in the underlying operating system are the cause of firewalls' compromise.

1.2.7 Unified Threat Management

Unified threat management (UTM) is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single appliance. To meet new threats the organisations are required to add more security solutions or security appliances. This poses the problem of increased complexity and cost, as each new technology means a new device to deploy, a new set of policies to configure, and a new management console to monitor. And, because each new stand-alone product is not integrated with the existing product set, it also creates potential blind spots in an organisation's security strategy, through which threats could pass undetected.

How UTM secures the network

A single UTM appliance simplifies security strategy, with just one device taking the place of multiple layers of hardware and software. Also from one single centralised console, all the security solutions can be monitored and configured. The UTM has a customised Operating System holding all the security features at one place. This can lead to better integration and throughput than a collection of disparate devices.

UTM Functionalities

Following functionalities are normally supported by the UTM.

- **Firewall:** performs stateful packet inspection

- **VPN:** enables secure remote access to networks
- **Gateway anti-virus:** prevents malicious payloads
- **Gateway anti-spam:** prevents unsolicited messages from entering the network
- **Intrusion Prevention:** detects and blocks intrusions and certain attacks
- **Content filtering:** stops access to malicious, inappropriate, or questionable websites and online content.
- **Bandwidth management:** enables effective management of Bandwidth.
- **Application control:** provides visibility and control of application behaviour and content
- **Centralised reporting** as the basic features.

They can also support data-loss prevention by blocking accidental or intentional loss of confidential, proprietary, or regulated data. For enterprises with remote networks or distantly located offices, UTMs are a means to provide centralised security with complete control over their globally distributed networks.

Key advantages

- Reduced complexity: It is a single security solution integrated together that reduces the complexity.
- It makes the task of installation of various security products easier. Hence maintenance and vendor issues become simpler.
- UTM facilitates easy management of the solution. Generally, it works on simple plug and play architecture. It supports GUI interface for manageability.
- Reduced technical training requirements, one product to learn.

Key Disadvantages

- Becomes a Single point of failure (SPOF) for network traffic. In case of its failure, the complete network is exposed. The vulnerabilities in the OS or the UTM can make it the single point of compromise.
- Deployment of UTM may have impact on latency and bandwidth when the UTM cannot keep up with the traffic

Regulatory compliance: Identity-based UTMs deliver identity-based reports on individual users in the network. This offers short audit and reporting cycles and facilitates the meeting of regulatory compliance requirements in enterprises.

1.2.8 Firewall Life Cycle

The firewall life cycle can be defined in five phases. The firewall life cycle stems from the network security policy of the organisation. This policy should be maintained and updated frequently as new attacks or vulnerabilities arise or as the organisation's needs in terms of network applications change. Based on the Network Security policy, the firewall policy is developed. This policy should make the

process of creating the firewall rule base less error-prone and more verifiable. The rule base should be properly mapped to the applications and the access matrix. The next phases relate to selection of the solution, its implementation, and configuration and patch management. Phases follow an iterative approach and at each stage the configuration is changed as per changing policy. Changes are effected as per the documented and approved Change Management policy.

1.2.9 Baseline Configuration for Firewalls

Before deciding upon the baseline configuration for a firewall, a general risk assessment and cost-benefits analysis should be performed on the network. This would provide a list of the network applications and the methods that will be used to secure the applications.

In the context of a commercial organisation having offices/users at various locations, a border router or other firewall should be used at the Internet connection point to create an internal DMZ. Web servers and other publicly accessible servers should be placed on the DMZ so that these are accessible as needed and still have some protections from the firewall. Internal users should be protected with an additional firewall. The default policy for the firewall should be to block all traffic and connections unless the traffic type and connections have been specifically permitted, as this approach is more secure. Remote users should be allowed access through a VPN. Firewall should be configured so that it itself is immune to penetration.

1.3 Summary

Firewall acts as security policy enforcement point for inbound and outbound access to the internal networks as packets cross network boundaries. This is done by inspecting the data that is received and tracking the connections that are made to determine what data should be permitted and what data should be denied. Stateful packet filtering examines packet data with memory of connection state between hosts. Network Address Translation (NAT) is the addressing method that hides internal network addresses. Application layer gateways (proxy servers) control how internal network applications access external networks by setting up proxy services.

For a firewall to be able to successfully protect resources, it is critical to implement a design that lends itself to protecting those resources in the most efficient manner. From a simple packet filtering to the screened sub-netting implementations, there are various implementation strategies. Although a single firewall will do an adequate job of protecting most resources, certain high security environments may warrant using multi-firewall architecture to minimize exposure and risk. Like any other security device firewalls have to be properly configured and monitored.

1.4 References

1. http://csce.uark.edu/~kal/info/private/Networking%20Bookshelf/fire/ch06_01.htm