Firewall

Principles of Information Security and Privacy
(CSE607)

M.Tech. I, Semester I

Department of Computer Science and Technology
S.V.National Institute of Technology-Surat

September 2, 2022

Overview

Introduction

Firewall

A firewall forms a barrier through which the traffic going in each direction must pass. A firewall security policy dictates which traffic is authorized to pass in each direction.

Introduction

- Firewalls can be 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 Design Principles

- Evolution of information systems
  - Centralized data processing system (mostly mainframe machine).
  - Local Area Networks(LANs).
  - Premises Network.
  - Enterprise-wide Network (multiple, geographically distributed premises networks interconnected by a private wide area network).
  - Internet connectivity.

Firewall Design Principles

- Internet connectivity is no longer optional for organizations.
- While Internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets.
- From the maintenance perspective it is not a feasible solution equip each and every system in network with a strong security features.
- The firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter.
- The aim of the perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and audit can be imposed.

Firewall Characteristics

- All traffic from inside to outside, and vice versa, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The firewall itself is immune to penetration.

Firewall Access Control Techniques

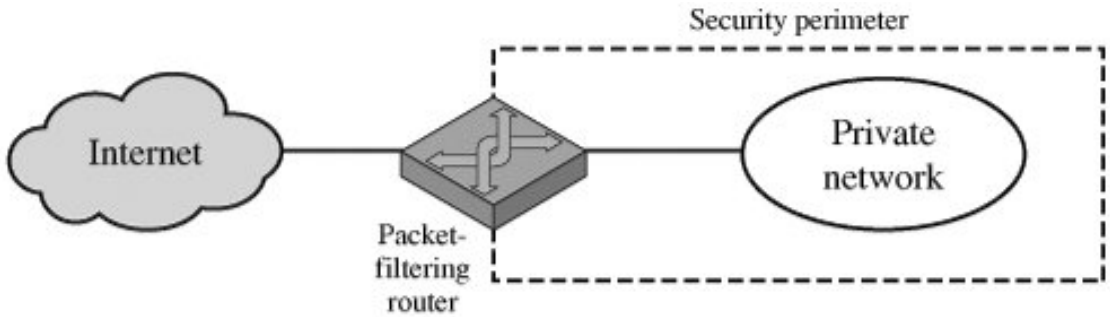
- Service control: Determines the types of Internet services that can be accessed, inbound or outbound.
  - may filter traffic on the basis of IP address and TCP port number.
  - may provide proxy software that receives and interprets each service request before passing it on.
  - may host the server software itself, such as a Web or mail service.
- Direction control: Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
- User control (Controls access to a service according to which user is attempting to access it).
- Behavior control: Controls how particular services are used.
  - may filter e-mail to eliminate spam.
  - may enable external access to only a portion of the information on a local Web server.

Limitations of firewall

- The firewall cannot protect against attacks that bypass the firewall.
- The firewall does not protect against internal threats.
- The firewall cannot protect against the transfer of virus-infected programs or files.

Types of Firewalls: Packet-Filtering Router

- Applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
- Configured to filter packets going in both directions (from and to the internal network).
- Filtering rules are based on information contained in a packet.



(a) Packet-filtering router

Types of Firewalls: Packet-Filtering Router

- Filtering rules are based on information contained in a network packet:
  - Source IP address.
  - Destination IP address.
  - Source and destination transport-level address(port number).
  - IP protocol field.
  - Interface.
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
- If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet.
- Two default policies:
  - Default = discard: That which is not expressly permitted is prohibited.
  - Default = forward: That which is not expressly prohibited is permitted.

Advantages and Disadvantages of Packet Filtering

- Advantages
  - Simple, transparent and fast.
- Disadvantages
  - Cannot prevent attacks that employ application-specific vulnerabilities or functions.
  - Most packet filter firewalls do not support advanced user authentication schemes.
  - They are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack(network layer address spoofing).
  - Susceptible to security breaches caused by improper configurations.

Types of Firewalls: Stateful Inspection Firewalls

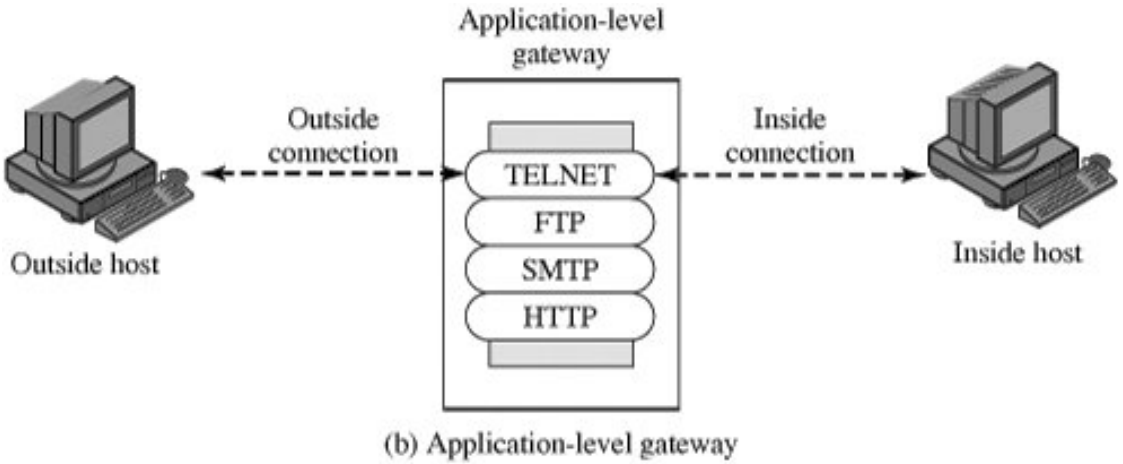
- A traditional packet filter makes filtering decisions on an individual packet basis and does not take into any higher layer context.
- A packet filtering firewall allows inbound traffic for all high numbered client ports (e.g., 1024 to 65535).
- An attacker can forge a server port number and then send malicious data to the client port number (high-numbered port).
- As the packet filtering firewall allows traffic for all high numbered ports, the packet bypasses the firewall.

Types of Firewalls: Stateful Inspection Firewalls

- Keeps track of the state information of the outbound TCP connections.
- Records an entry for each active outbound TCP connection.
- Allows only those inbound packets that come as a response to the outbound packets.
- Other than the state information, other rules to filter the packets remain same as in the packet filtering firewalls.

Types of Firewalls: Application-level Gateway

- An application-level gateway, also called a proxy server, acts as a relay of application-level traffic



(b) Application-level gateway

Types of Firewalls: Application-level Gateway

- Application proxy (firewall) is placed in the middle between the client the server.
- When the client contacts a server, an application proxy acts as a server and receives packets forwarded by the client.
- Application proxy acts as a server and forwards packets sent by the real server to the client as per the security policy.

Types of Firewalls: Application-level Gateway

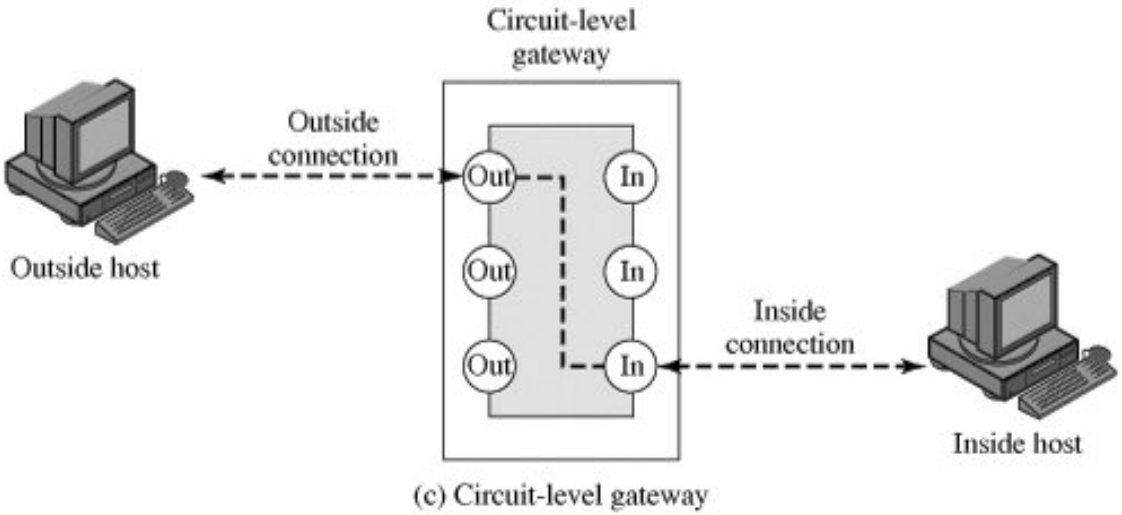
- Application proxy examines the contents of packets, and forwards/drops packets as per the security policy.
- If the contents of packets are valid, an application proxy sends the packets as a client to the server, and receives the packets forwarded by the server as a response.

Advantages and Disadvantages of Application-level Gateway

- Advantages
  - Application-level Gateway is more secure than packet filtering firewall or stateful inspection firewall.
    - ★ Examines payload of packets, and not only the headers.
    - ★ Configuration errors can be reduced, as it is application specific.
  - Application proxy has significantly more information in logs as compared to packet filtering firewall and stateful inspection firewall.
- Disadvantages
  - Processing overhead as it examines (header and payload) and forwards packets in both directions (i.e., client and server).
  - Must implement both client and server protocols to act as a client (to a server) and a server (to a client).
  - Application specific - Different applications require different application proxies.

Types of Firewalls: Circuit-level Gateway

- This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications.
- circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.
- Decides which connections are allowed and which connections are not allowed.



(c) Circuit-level gateway

Types of Firewalls: Circuit-level Gateway

- SOCKS package consists of the following components
  - SOCKS server - runs on a firewall.
  - SOCKS client - runs on internal hosts protected by the firewall.
  - SOCKS-ified versions of client programs such as FTP, TELNET, etc.

Advantages of Circuit-level Gateway

- Transparent to applications - Unlike an application proxy, a circuit-level proxy is not specific to applications, and it works for all applications.
- A circuit-level proxy does not examine the payload, and,hence, the processing overhead is less as compared to the application proxy.

Bastion Host

- A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security.
- Typically, the bastion host serves as a platform for an application-level or circuit-level gateway.

Characteristics of a bastion host

- The bastion host hardware platform executes a secure version of its operating system, making it a trusted system.
- Only the services that the network administrator considers essential are installed on the bastion host.
  - Proxy applications such as Telnet, DNS, FTP, SMTP, and user authentication.
- The bastion host may require additional authentication before a user is allowed access to the proxy services. In addition, each proxy service may require its own authentication before granting user access.
- Each proxy is configured to support only a subset of the standard application's command set.

Characteristics of a bastion host

- Each proxy is configured to allow access only to specific host systems. This means that the limited command/feature set may be applied only to a subset of systems on the protected network.
- Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection. The audit log is an essential tool for discovering and terminating intruder attacks.
- Each proxy module is a very small software package specifically designed for network security.
  - Because of its relative simplicity, it is easier to check such modules for security flaws.
  - A typical UNIX mail application may contain over 20,000 lines of code, while a mail proxy may contain fewer than 1000.

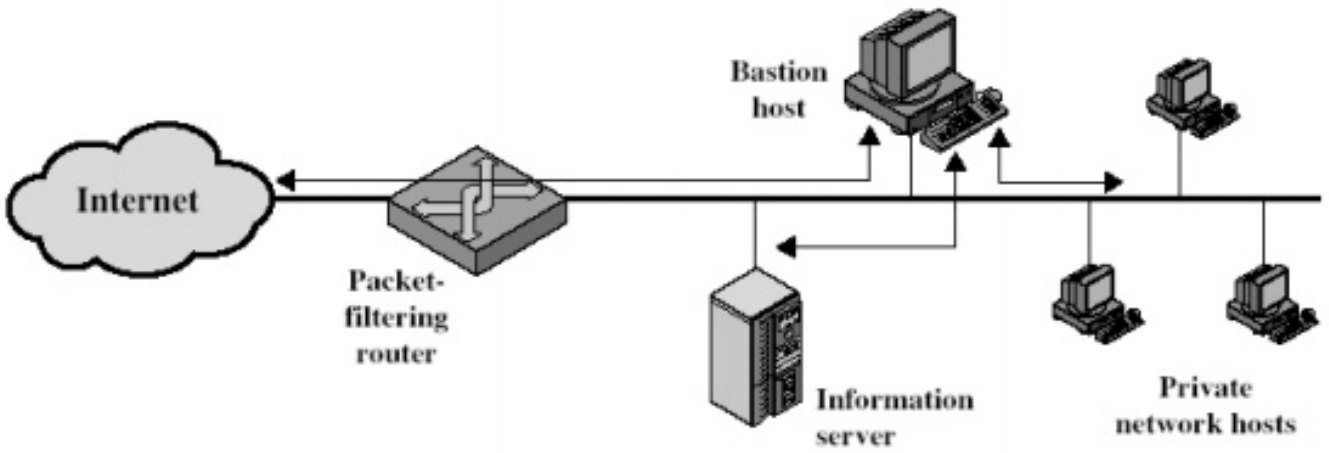
Characteristics of a bastion host

- Each proxy is independent of other proxies on the bastion host.
  - If there is a problem with the operation of any proxy, or if a future vulnerability is discovered, it can be uninstalled without affecting the operation of the other proxy applications.
  - Also, if the user population requires support for a new service, the network administrator can easily install the required proxy on the bastion host.
- A proxy generally performs no disk access other than to read its initial configuration file.
  - This makes it difficult for an intruder to install Trojan horse sniffers or other dangerous files on the bastion host.
- Each proxy runs as a nonprivileged user in a private and secured directory on the bastion host.

Firewall configurations

- screened host firewall, single-homed bastion
- screened host firewall, dual-homed bastion
- screened subnet firewall

screened host firewall, single-homed bastion



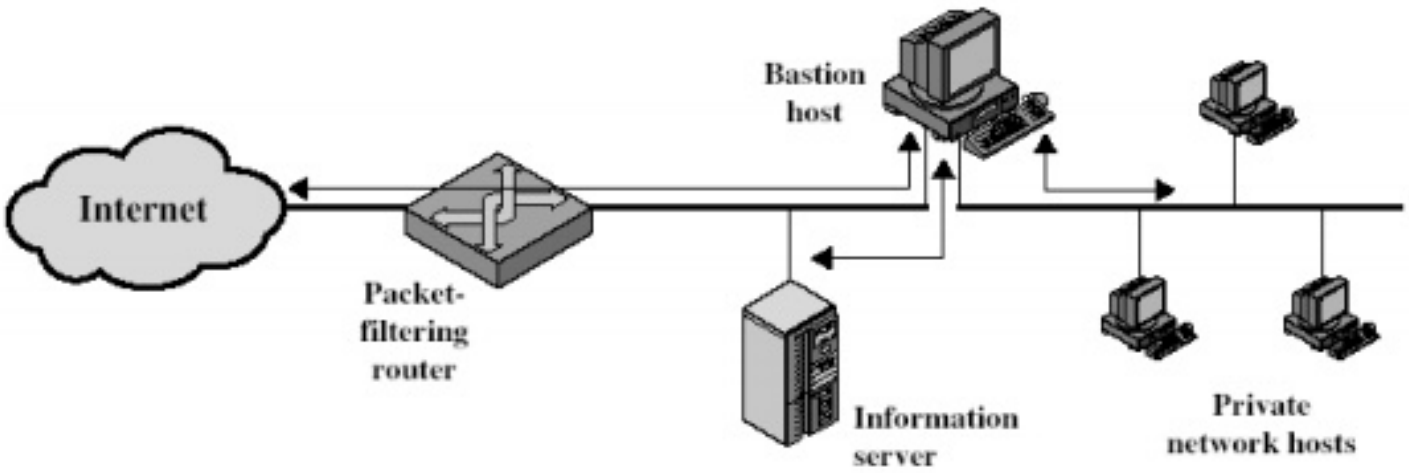
(a) Screened host firewall system (single-homed bastion host)

- In this configuration, the firewall consists of two systems
  - a packet filtering router
  - a bastion host. Typically, the router is configured so that
    - ★ For traffic from the internet, only IP packets destined for the basiton host are allowed in.
    - ★ For traffic from the internal network, only IP packets from the basiton host are allowed out.

screened host firewall, single-homed bastion

- The basiton host performs authentication and proxy functions.
- This configuration has greater security than simply a packet filtering router or an application level gateway alone, for two reasons
  - This configuration implements both packet level and application level filtering, allowing for considerable flexibility in defining security policy.
  - An intruder must generally penetrate two separate systems before the security of the internal network is compromised.

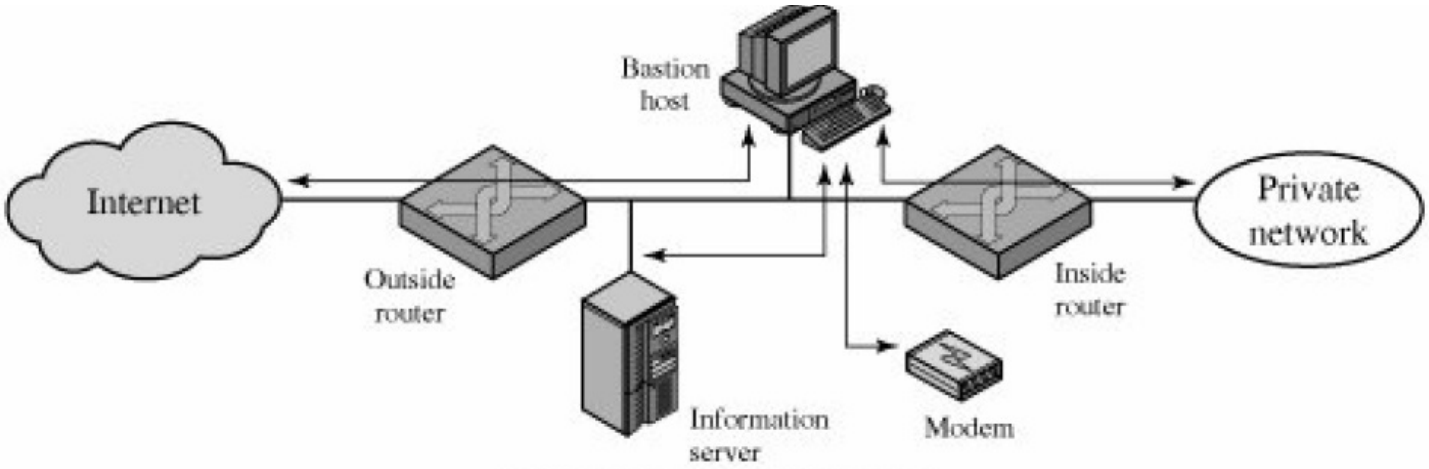
screened host firewall, dual-homed bastion



(b) Screened host firewall system (dual-homed bastion host)

- In the previous configuration, if the packet filtering router is compromised, traffic could flow directly through the router between the internet and the other hosts on the private network.
- This configuration physically prevents such a security break.

screened subnet firewall



(c) Screened-subnet firewall system

- In this configuration, two packet filtering routers are used
  - one between the basiton host and internet and
  - one between the basiton host and the internal network.
- This configuration creates an isolated subnetwork, which may consist of simply the basiton host but may also include one or more information servers and modems for dial-in capability.
- Typically both the internet and the internal network have access to hosts on the screened subnet, but traffic across the screened subnet is blocked.

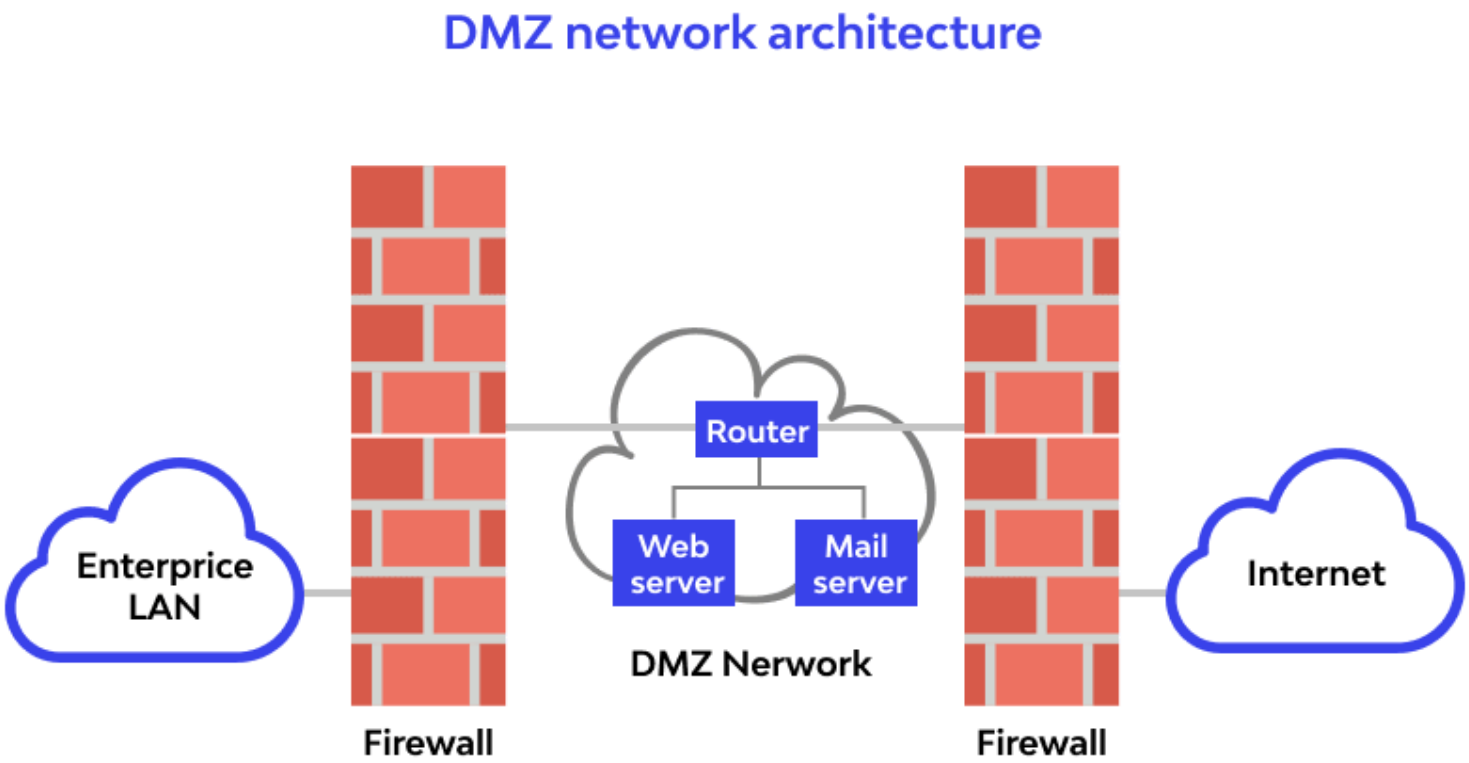
screened subnet firewall

- advantages
  - There are now three levels of defense to thwart intruders
  - The outside router advertises only the existence of the screened subnet to the internet; therefore the internal network is invisible to the internet.
  - Similarly, the inside router advertises only the existence of the screened subnet to the internal network; therefore the systems on the internal network cannot construct direct routes to the internet.

Demilitarized zone (DMZ) networks

- A DMZ is a physical or logical subnet that isolates a LAN from untrusted networks like the public internet.
  - Any service that is offered to users on the public internet should be set up in the DMZ network. The external-facing servers, services, and resources are usually placed there.
  - Services include web, Domain Name System (DNS), email, proxy servers and File Transfer Protocol (FTP), Voice over Internet Protocol (VoIP).
- The resources and servers in the DMZ network can be accessed from the internet but are isolated with very limited access to the LAN.
- Due to this approach, the LAN has an additional layer of security restricting a hacker from directly accessing the internal servers and data from the internet.
- Hackers and cyber criminals can reach the systems that run services on a DMZ server. The security on those servers must be tightened to be able to withstand constant attacks.
- The main objective of a DMZ is to enable organizations to use the public internet while ensuring the security of their private networks

Demilitarized zone (DMZ) networks



Demilitarized zone (DMZ) networks

- Need for an internal firewall
  - Protects the corporate network from network based attacks by stringent filtering rules such as default drop policy.
  - Protects the corporate network from attacks launched from DMZ systems, and vice versa.
  - Protects internal systems from each other.

Firewalls - Examples

- Linux - iptables
- Windows Firewall
- Bitdefender Box (Hardware firewall)
- Cisco Next-Generation Firewall Virtual