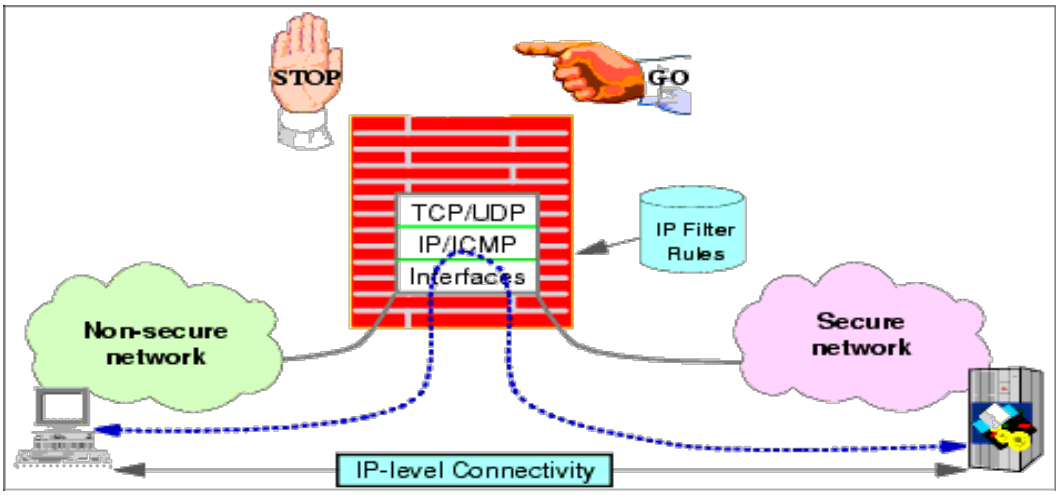
Packet Filtering & Proxy Servers

Packet Filtering :



Packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols. The process is used in conjunction with packet mangling and Network Address Translation (NAT). Packet filtering is often part of a firewall program for protecting a local network from unwanted intrusion.

In a software firewall, packet filtering is done by a program called a packet filter. The packet filter examines the header of each packet based on a specific set of rules, and on that basis, decides to prevent it from passing (called DROP) or allow it to pass (called ACCEPT).

Three ways in which a packet filter can be configured :

- ➔ First method : the filter accepts only those packets that it is certain are safe, dropping all others. This is the most secure mode, but it can cause inconvenience if legitimate packets are inadvertently dropped.

- ➔ Second method : The filter drops only the packets that it is certain are unsafe, accepting all others. This mode is the least secure, but is causes less inconvenience, particularly in casual Web browsing.

- ➔ Third method : The filter encounters a packet for which its rules do not provide instructions, that packet can be quarantined, or the user can be specifically queried concerning what should be done with it.

What should be inspected in a Packet Header :

In a packet header few of the possible things which should be checked are :

- ➔ Source IP address of the packet. This is necessary because IP spoofers might have changed the source IP address to reflect the origin of packet from somewhere else, rather than reflecing the original source.
- ➔ Destination IP Address. The firewall rules should check for IP address rather than DNS names. This prevents abuse of DNS servers.
- ➔ IP Protocol ID.
- ➔ TCP/UDP port number.
- ➔ ICMP message type.
- ➔ Fragmentation flags.
- ➔ IP Options settings.

Capabilities of a Packet Filter :

- ➔ **Examination of each packet data and headers :** Each packet is examined when it comes to the packet filter. This is done with the help of filtering rules defined in the next point.

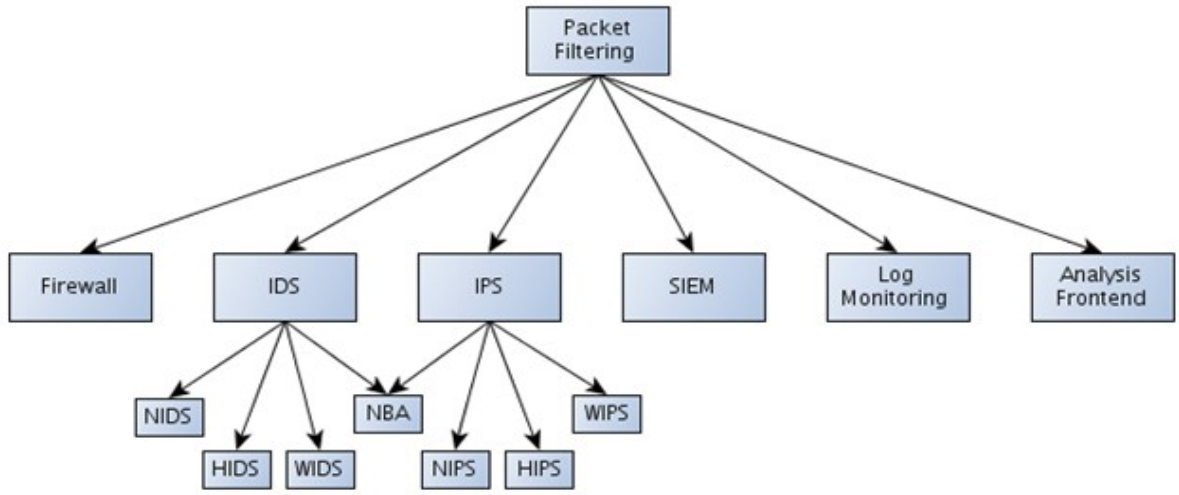
- ➔ **Set of rules which define what to do with the packet :** These rules define what a packet filter should look for when it receives a packet. It usually looks for the information like source IP address, destination IP address, source port number, destination port number, etc.

- ➔ **What actions are taken based on the result of examination :** There are numerous actions which can be used when a packet filter receives a packet and has filtering rules defined. Based on defined filtering rules, a packet filter can do the following:

- Accept only packets that are certainly safe – based on a set of rules. Drop all other packets.
- Drop only packets that are certainly unsafe – based on a set of rules. Accept all other packets.
- If a packet is received for which there is no filtering rule defined, ask a user what to do with it.

- Block a user coming from a defined source IP address, because too many packets were received in too short of a time window.
- Almost any action can be applied against a packet or a set of packets If we want to send a HTTP response, which includes “Hello, my name ” to every HTTP request coming from IP xxx.xxx.xxx.xxx, we could define a rule that could do that.

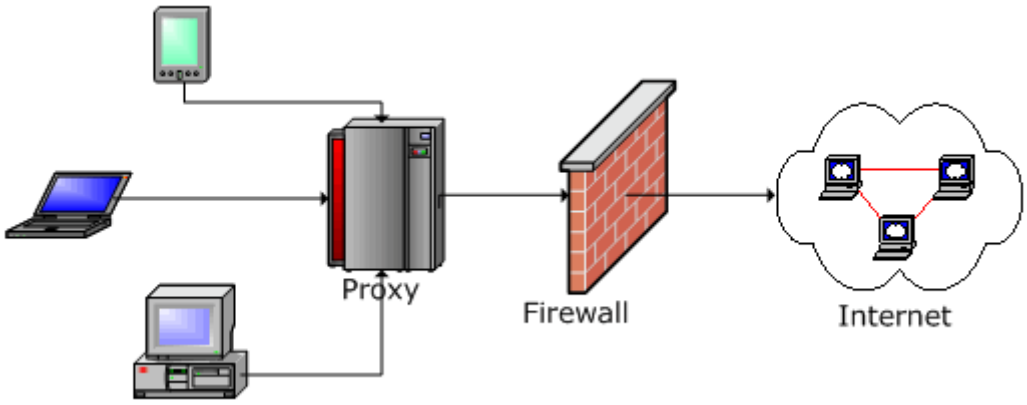
Packet Filtering Security Categories :



An overview of packet filtering :-

- ➔ Firewall.
- ➔ IDS (Intrusion Detection System).
  - NIDS (Network IDS).
  - HIDS (Host IDS).
  - WIDS (Wireless IDS).
  - NBA (Network Behavior Analysis).
- ➔ IPS (Intrution Prevention System).
  - IPS (Intrusion Prevention System).
  - NIDS (Network IPS).
  - HIDS (Host IPS).
  - WIDS (Wireless IPS).
- ➔ SIEM (Security Information & Event Management).
- ➔ Log Monitoring.
- ➔ Analaysis Foretend.

Proxy Servers :



A proxy server is a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service. The proxy server may exist in the same machine as a firewall server or it may be on a separate server, which forwards requests through the firewall.

How Proxy Servers work : When a proxy server receives a request for an Internet resource (such as a Web page), it looks in its local cache of previously pages. If it finds the page, it returns it to the user without needing to forward the request to the Internet. If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from the server out on the Internet. When the page is returned, the proxy server relates it to the original request and forwards it on to the user.

Proxy servers are used for both legal and illegal purposes. In the enterprise, a proxy server is used to facilitate security, administrative control or caching services, among other purposes. In a personal computing context, proxy servers are used to enable user privacy and anonymous surfing.

Types of Proxy servers : Proxy servers are classified into several types based on purpose and functionality. Some of the most common types and their uses can be described as below:

- **Web Proxy :** Web Proxy is the most common type of proxy application, which responds to the user requests by accessing resources from cached web pages and files available on remote web

servers. This facilitates quick and reliable access to data for local network clients. If the requested resource is not found in the cache, then a web proxy fetches the file from the remote server, and saves a copy in the cache before returning it to the client.

- **Transparent Proxy :** Transparent Proxy is mostly used for caching websites and overcoming simple IP bans. However, such proxies do not provide any user anonymity since user's original IP address is exposed. Transparent proxies are not specifically configured on the client computers.

- **Anonymous proxies :** Anonymous proxies do not hide the original IP address of the user however they provide adequate anonymity to most users. Anonymous proxies are easily detectable.

- **Distorting proxy :** Distorting proxy identifies itself as a proxy server, and modify the HTTP headers to disguise the original IP address.

- **Tunneling proxies :** Tunneling proxies are capable of passing client requests and return responses without making any modifications. These are also referred to as gateway proxies.

- **Forward proxy :** Forward proxy responds to client requests by retrieving data from a wide range of sources on the internet. It is also referred to as an Internet-facing proxy.

- **Open proxies :** Open proxies belong to the category of forwarding proxy servers, which are accessible by any internet user since they can receive and return requests from any client computer.

- **Reverse proxies :** Reverse proxies also known as surrogates, usually receive requests from the Internet and forward them to internal network servers. A reverse proxy server forwards requests to one or more proxy servers, whose response is returned to the client computer, the user of which has no knowledge on the origin of the response.

Basic uses of proxy servers :

- **Performance Improvement :** Proxy servers also contribute to improved web performance since the results of the user requests are saved in cache memory for a set period of time. This is achieved with the help of a caching proxy server, which could save a large amount of time while catering to the requests from a vast user load.
  A caching proxy server maintains a local copy of frequently requested web content. It can accelerate service requests by retrieving content from the cache memory, if it had already been requested by another client on the same network. This feature contributes to a significant reduction in upstream bandwidth usage and costs for large organizations with thousands of employees.

- **Monitoring and Filtering User Requests :** Web proxies can be used to filter user requests, and block certain content or web pages from being accessed. This can be achieved with the help of a content-filtering web proxy server that differentiates the users' level of control over the content, based on the user type Guest or Administrator.
  Content-filtering proxies are generally used in organizations and educational institutions with strict internet-usage policies. Blocking certain websites, and restricting access to specific key words and censoring undesirable content are some of the basic features provided by content-filtering or web-filtering proxies.

- **Anonymous Browsing :** An anonymous proxy server is another type of web proxy that anonymizes users' online activities. This type of proxy server directs the user requests to a destination server, which ultimately has no knowledge of the source of the request. Only the proxy is aware of the source of the request, including the user IP address and location.

- **Translation :** Considering the global audiences, translation proxies have been developed to localize/translate the content of a source website into a local language of the client computer. Responses for requests sent by local users are replaced with translated content from the source website, and passed back through the proxy server.