KEY TECHNOLOGY COMPONENTS

FIREWALLS

- A Firewall is a device that selectively discriminates against information following into or out of the organization.
- A Firewall is usually a computing device , or a specially configured computer that allows or prevents information from entering or exiting the defined area based on a set of predefined rules.
- Firewalls are usually placed on the security perimeter, just behind or as part of a gateway router.
- While the gateway router is primarily designed to connect the organization's systems to the outside world, it too can be used as the front-line defense against attacks as it can be configured to allow only a few types of protocols to enter.
- There are a number of types of firewalls, which are usually classified by the level of information they can filter.
- Firewalls can be packet filtering , stateful packet filtering, proxy or application level.
- A firewall can be a single device or a firewall subnet, which consists of multiple firewalls creating a buffer between the outside and inside networks.
- Thus, firewalls can be used to create to security perimeters like the one shown in Fig. 6.19

DMZs

- A buffer against outside attacks is frequently referred to as a Demilitarized Zone (DMZ).
- The DMZ is a no-mans land between the inside and outside networks; it is also where some organizations place web servers .

- These servers provide access to organizational web pages, without allowing web requests to enter the interior networks.

Proxy Servers

- An alternative approach to the strategies of using a firewall subnet or a DMZ is to use a proxy server, or proxy firewall.
- A proxy server performs actions on behalf of another system
- When deployed, a proxy server is configured to look like a web server and is assigned the domain name that users would be expecting to find for the system and its services.
- When an outside client requests a particular web page, the proxy server receives the requests as if it were the subject of the request, then asks for the same information from the true web server (acting as a proxy for the requestor), and then responds tot eh request as a proxy for the true web server.
- This gives requestors the response they need without allowing them to gain direct access to the internal and more sensitive server.
- The proxy server may be hardened and become a bastion host placed in the public area of the network or it might be placed within the firewall subnet or the DMZ for added protection.
- For more frequently accessed web pages, proxy servers can cache or temporarily store the page, and thus are sometimes called cache servers.
- Fig 6.20 shows a representative example of a configuration using a proxy .

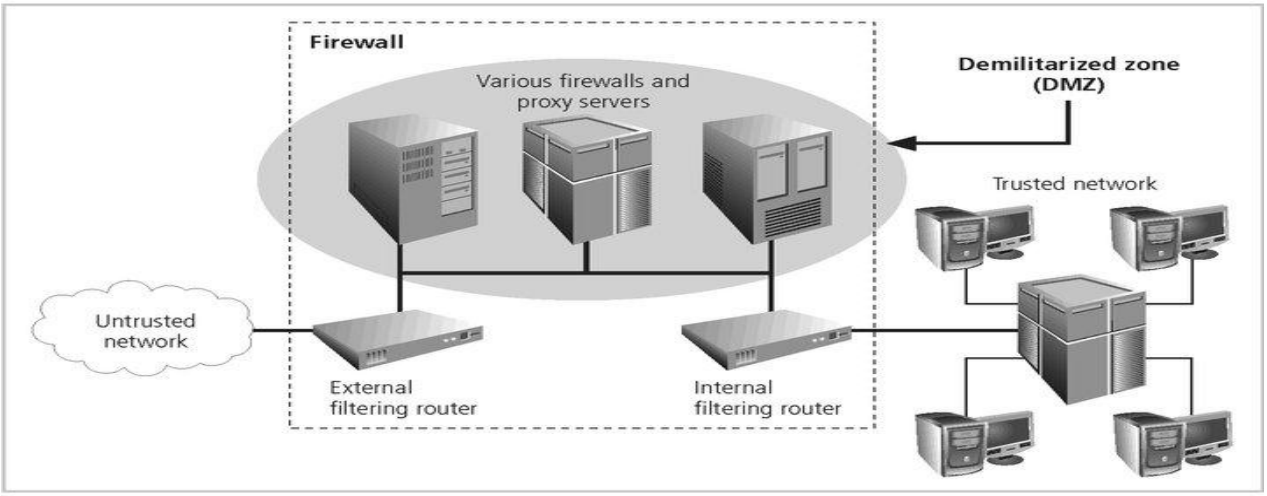

FIGURE 6-20 Firewalls, Proxy Servers, and DMZs

Intrusion Detection Systems (IDSs)

- In an effort to detect unauthorized activity within the inner network or an individual machines, an organization may wish to implement Intrusion Detection Systems (IDSs)
- IDSs come in TWO versions, with Hybrids possible.

Host Based IDS

- Host based IDSs are usually installed on the machines they protect to monitor the status of various files stored on those machines.
- The IDS learns the configuration of the system , assigns priorities to various files depending on their value, and can then alert the administrator of suspicious activity.

Network Based IDS

- Network based IDSs look at patterns of network traffic and attempt to detect unusual activity based on previous baselines.
- This could include packets coming into the organization's networks with addresses from machines already within the organization(IP Spoofing).

- It could also include high volumes of traffic going to outside addresses(As in a Denial of Service Attack)
- Both Host and Network based IDSs require a database of previous activity.
- In the case of host based IDSs, the system can create a database of file attributes, as well as maintain a catalog of common attack signatures.
- Network-based IDSs can use a similar catalog of common attack signatures and develop databases of " normal " activity for comparison with future activity.
- IDSs can be used together for the maximum level of security for a particular network and set of systems.
- FIG 6.21 shows an example of an Intrusion Detection System.

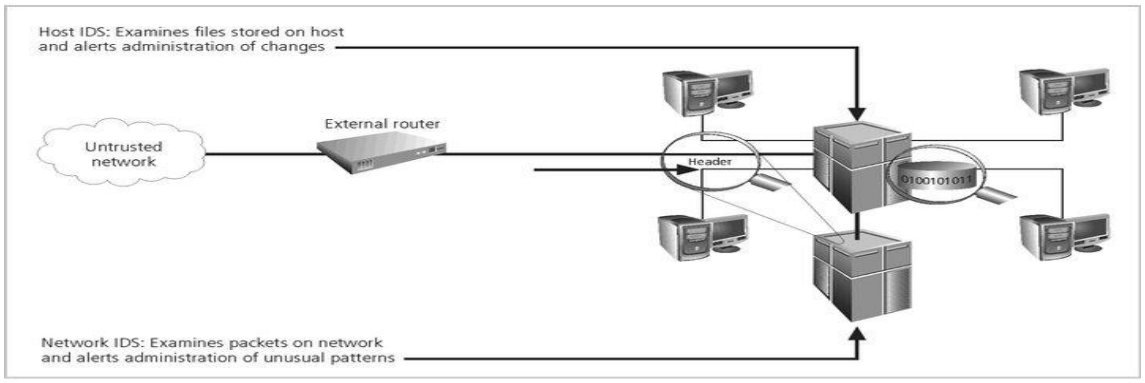

FIGURE 6-21 Intrusion Detection Systems

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf