FIREWALL CATEGORIZATION METHODS

II. Application Gateways

The application gateway , also known as an application –level firewall or application firewall, is frequently installed on a dedicated computer , separate from the filtering router, but is commonly used in conjunction with a filtering router. The appliocation firewall is also known as a proxy server, since it runs special software that acts as a proxy for a service request.

An organization that runs a Web server can avoid exposing thee server to direct traffic from users by installing a proxy server, configured with the registered domain‘s URL. This proxy server will then receive requests for Web pages, access the Web server on behalf of the external client, and return the requested pages to the users.these servers can store the most recently accessed pages in their requested pages to the users. These servers can store the most recently accessed pages in their internal cache, and are thus also called cache servers.The benefits from this type of implementation are significant.

One common example of an application –level firewall or proxy server is a firewall that blocks all requests for an responses to requests from Web pages and services from the internal computers of an organization, and instead makes all such requests and responses go to intermediate computers or proxies in the less protected areas of the organizaionsnetwork.This techniques of using proxy servers is still widely used to implement electronic commerce functions.

The primary disadvanatage of application-level firewalls is that they are designd for specific protocol and cannot easily be reconfigured to protect against attacks on other protocols. Since application firewalls work at the application layer they are typically restricted to a single application (Eg, FTP, Telnet, HTTP, SMTP, SNMP). The processing time and resources necessary to read each packet down tot eh application layer diminishes the ability of these firewalls to handle multiple types of applications.

III. Circuit Gateways

The circuit firewall operates at the transport layer. Again connections are authorized based on addresses. Like filtering firewalls, circuit gateways firewalls do not usually look at data traffic flowing between one network and another, but they do prevent direct connections between one network and another. They accomplish this by creating tunnels connecting specific processes or systems on each side of the firewall,

and then allow only authorized traffic, such as a specific type of TCP connection for only authorized users, in these tunnels.

Writing for NIST in SP 800-110, John Wack describes the operation of a circuit gateway as follows: ―A circuit-level gateway relays TCP connections but does no extra processing or filtering of the protocol. For example, the use of a TELNET application server is a circuit –level gateway operation, since once the connection between the source and destination is established, the firewall simply passes bytes between the systems without further evaluation of the packet contents. Another Another example of a circuit –level gateway would be for NNTP, in which the NNTP server would connect to the firewall, and then internal systems NNTP clients would connect tot eh firewall. The firewall would again, simply pass bytes.

IV. MAC layer Firewalls:

MAC layer firewalls are designed to operate at the media access control layer of the OSI network mode. This gives these firewalls the ability to consider the specific host computer‘s identity in its filtering decisions. Using this approach, the MAC addresses the specific host computers are linked to ACL entries that identify the specific types of packets that can be sent to each host, and all other traffic is blocked.

Fig 6-5 shows where in the OSI model each of the firewall processing modes inspects data.

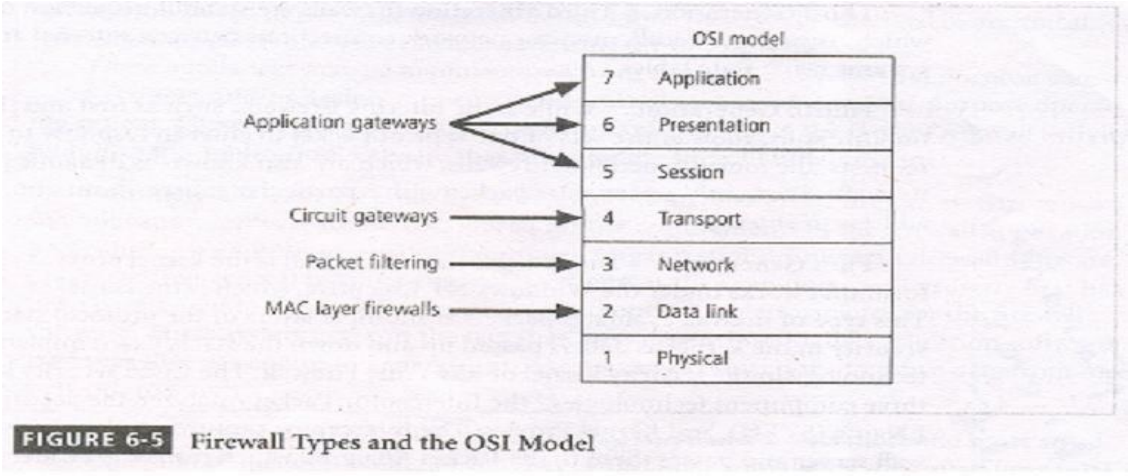

FIGURE 6-5 Firewall Types and the OSI Model

V. Hybrid Firewalls:

Hybrid Firewalls combine the elements of other types of firewalls-that is, the elements of packet filtering and proxy services, or of packet filtering and circuit gateways. Alternately, a hybrid firewall system may actually consist of two separate firewall devices: each is a separate firewall system, but they are connected so that they work in tandem. For example, a hybrid firewall system might include a packet filtering firewall that is set up to screen all acceptable requests then pass the requests to a proxy server, which in turn, requests services from a Web server deep inside the organization‘s networks. An added advantage to the hybrid firewall approach is that it enables an organization to make a security improvement without completely replacing its existing firewalls.

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