Name of Faculty: Kamlesh Chandravanshi

Designation: Assistant Professor

Department: Information Technology

Subject: Wireless Mobile Computing

Subject Code: (IT-602)

Unit: V

Topic: Firewall and its Design Principles

Sem: VI

Section: A

Year: 3rd Year

Firewall and its Design Principles

Firewall:

1. Firewall is a security barrier between two networks that screens traffic coming in and out of the gate of one network to accept or reject connections and services according to a set of rules.
2. A firewall is like a secretary for a network which examines requests for access to the network. It decides whether they pass a reasonableness test. If they pass it they are allowed through and if not they are refused.
3. If a man wants to meet the chair of the community department, the secretary does a certain level of filtering but if the man wants to meet the President of the country, the secretary will perform a much different level of filtering.
4. A network firewall is placed between the internal network, which might be considered safe and the external network or the Internet which is known to be unsafe.
5. The job of the firewall is to determine what to let into and out of the internal network. In this way, a firewall provides access control for the network.
6. There are essentially three types of firewalls. Each type of firewall filters packets by examining the data up to a particular layer of the network protocol stack.

The firewalls are:

i. A packet filter is a firewall that operates at the network layer.

ii. A stateful packet filter is a firewall that lives at the transport layer.

iii. An application proxy is a firewall that operates at the application layer where it functions as a proxy.

Design Principles:

i. All traffic from inside to outside and vice versa must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. The configurations used for this are screened Host Firewall (Single and Dual) and Screened Subnet Firewall.

ii. Only authorized traffic as defined by the local security policy will be allowed to pass. Various types of firewalls that can be used are Packet-Filters, Stateful Filters and Application Proxy Filters.

iii. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

Firewall Characteristics:

i. All traffic from inside to outside and vice versa must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. The configurations used for this are screened Host Firewall (Single and Dual) and Screened Subnet Firewall.

ii. Only authorized traffic as defined by the local security policy will be allowed to pass. Various types of firewalls that can be used are Packet-Filters, Stateful Filters and Application Proxy Filters.

iii. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

Techniques for Control:

Four general techniques that firewalls use to control access and enforce security policy are as follows

i. Service Control- This determines the types of internet services that can be accessed inbound or outbound.

ii. Direction Control: This determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

iii. User Control: Control access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter.

iv. Behaviour Control: Controls how particular services are used.

Capabilities of Firewalls: The expectations from a firewall are as follows

i. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits vulnerability and provides protection from spoofing and routing attacks.

ii. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.

iii. A firewall is a convenient platform for several internet functions that are not security related which include network address translator and a network management function.

iv. A firewall can serve as the platform for IPsec. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.

Limitations of Firewalls:

i. The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modern pool that provides dial-in capability for traveling employees and telecommuters.

ii. The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.

iii. The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter it would be impractical and impossible for the firewall to scan all incoming files for viruses.

References:

1: https://www.ques10.com/p/3532/what-are-firewall-design-principles/

2: https://www.ques10.com/p/13015/what-is-a-firewall-what-are-the-firewall-design--1/