Name of Faculty: Shubha Mishra

Designation: Assistant Professor

Department: Information Technology

Subject & Subject Code: WMC & IT-602

Unit: V

Topic: Firewall Design Principles

Firewall Design Principles

Introduction to 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:

Design goals:

1. All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall) –
2. Only authorized traffic (defined by the local security policy) will be allowed to pass
3. The firewall itself is immune to penetration (use of trusted system with a secure operating system)

1. 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.
2. 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.

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

Three common types of Firewalls:

1. Packet-filtering routers

2. Application-level gateways

3. Packet-filtering Router

1. It applies a set of rules to each incoming IP packet and then forwards or discards the packet . Filter packets going in both directions . The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header . Two default policies (discard or forward)

Advantages: – Simplicity – Transparency to users – High speed

• Disadvantages: – Difficulty of setting up packet filter rules – Lack of Authentication

2. Stateful Packet Filter

Advantages: – Simplicity – Transparency to users – High speed

Disadvantages: – Difficulty of setting up packet filter rules – Lack of Authentication

3.Circuit level gateway

Circuit-level Gateway – Stand-alone system or – Specialized function performed by an Application-level Gateway – Sets up two TCP connections – The gateway typically relays TCP segments from one connection to the other without examining the contents

The security function consists of determining which connections will be allowed – Typically use is a situation in which the system administrator trusts the internal users.

References –

1. Chapman, D., and Zwicky, E. Building Internet Firewalls. O'Reilly, 1995
2. Cheswick, W., and Bellovin, S. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, 2000