A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic

Reject : block the traffic but reply with an “unreachable error”

Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

History

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.

But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type code instead of port number which identifies purpose of that packet.

Arranging devices and creating connections

Step 2: Configure wireless router and connect server to wireless router using Ethernet cable

Step 3: Configure Server by setting IP Config in Server0 to DHCP

Step 4: Configure and connect all PC’s to wireless router

Step 5: Changing port to wireless adapter of all PC’s

After adding wireless adapter of all PC’s they will automatically get connected with

wireless router because of DHCP

Checking connection of pc’s with server

from pc0 ping 192.168.0.100

browser http://192.168.0.100

If receiving response from server our connection is done successfully

Step 7: Configure IPv4 firewall to setup networks based firewall and add conditions

server --> desktop --> firewall

action deny

protocol icmp

remote ip 0.0.0.0

wildcard 255.255.255.255

action allow

protocol ip

remote ip 0.0.0.0

wildcard 255.255.255.255

now we should not be able to ping to the server but should be able to view the server data