Examples of The Way Firewalls Are Used

Use Case ONE

- Edge devices that separate the internet from an internal network translate routable public IP addresses to non-routable private IP addresses.

    - They can help prevent attacks on internal networks, keep out malware, and prevent leakage of sensitive information to the public internet.

Use Case TWO

- Large networks are typically divided into subnets. Each department could have its own subnet. Each subnet can be separated by a Firewall.

Use Case THREE

- Firewalls can run on different servers and workstations, Firewalls can preform a form of access control. Firewalls can also be configured to prevent certain types of port scanning and DoS attacks.

An Overview of IP Tables

A common misconception is that the name of a Firewall in Linux is IP Tables. In reality the name of a Linux Firewall is netfilter.

The advantages of IP Tables:

- It's easy to use iptable commands in shell scripts to create your own Firewall configuration.

- It has great flexibility and makes it easy to setup a simple port filter, a router or a VPN

- It comes pre-installed on all Linux distros.

- It is very well documented with lots of tutorials online.

Mastering The Basics of IP Tables

Filter table is for basic protection, this may be the only table you need
NAT table used to connect to the public internet
Mangle table this alters network packets as they go through the firewall
Raw table is for packets that don’t require connection tracking
Security table is only used for systems that have SELinux installed
Since we are only focused in host protection in this scenario we will only focus on the **Filter table**

Blocking ICMP with IP Tables

The conventional wisdom you may hear is you should block ALL ICMP packets. The idea behind this philosophy is to make your server invisible to ping packets. It is true that there are some vulnerabilities:

- By using a botnet a hacker could inunate your server with ping packets from multiple sources at once.

- Certain vulnerabilities that are associated with ICMP can allow a hacker to obtain admin privileges on your system or redirect your traffic to a malicious server.

- By using simple hacking tools someone could embed sensitive data in the data field of an ICMP packet.

However, while blocking certain types of ICMP packets is good, blocking all ICMP packets is BAD. The harsh reality is that certain types of ICMP messages are necessary for the proper functionality of the network.

Three Types of ICMP Messages We Want To Allow

Type 3 - These are destination unreachable messages. Not only can they tell your server that it can’t reach a certain host, but it can also tell you why.

- **For Example**: if a server has sent out a packet that's too large for a network switch to handle, the switch will send back an ICMP message that tells the server ro fragment the packet.

Type 11 - Time exceeded messages tell your server that a packet that it sent out has sent out has either exceeded its TTL (Time To Live) value or that a fragmented packet cannot be reassembled before the TTL times out.

Type 12 - These messages indicate the server has sent a packet with a bad IP header.

- The header could either be missing an option or exceeded the length allowed.

Blocking Everything That Isn't Allowed With IP Tables

To block stuff we don't want we have to do two things. We can set a DROP or REJECT policy for the INPUT chain.

- Input - This chain is used to control the behavior for incoming connections
    - The one you choose is you preference.

The difference between DROP and REJECT is that DROP blocks packets without sending any messages back to the sender. REJECT sends a message back to the sender as to why the packets were blocked.

- If making the host invisible use DROP
    - If you need your host to inform other hosts why they can't make a connection, use REJECT

Blocking Invalid Packets With IP Tables

The story of why we may want to block invalid packets starts with our old friend the TCP connection. As you recall a TCP connection happens in the sequence of a three way handshake. If you don't remember what this is, now is a good time to go back and review it. This is part of the foundational knowledge of networking and cyber security.

How Hackers Can Use Invalid TCP Packets To Attack Your System

The illicit packets can be used to elicit responses from a target machine in order to find out what operating system it is running, which services are running, which services are running and the versions of the services running.

The invalid packets could be used to trigger certain types of security vulnerabilities on the target machine.

Some of the packets require more processing power which means a hacker can use these packets to do a DoS attack.

Uncomplicated Firewall For Ubuntu Systems

In the versions of Ubuntu higher than 16.04 there is something called ufw (Uncomplicated Firewall) This still uses iptables, but it offers a very simplified set of commands. You just perform one simple command to open a desire port and another to activate it and you have a good basic Firewall.

There are separate files for configuring IPv4 and IPv6 with iptables. When using ufw, you just have to configure it once and it automatically configures IPv4 and IPv6 with just one command which is a big time saver.

Configuring UFW

On your version of Linux ufw should be installed but in order to use it , you must activate it.

The first thing you want to do is open port 22 to allow it to connect to the machine via secure shell (ssh)

- sudo ufw allow 22/tcp