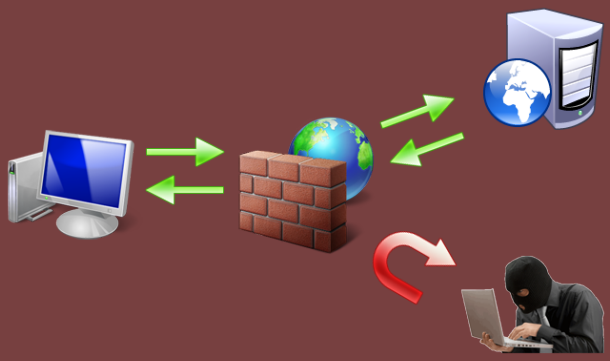
Firewalls for Fun and Profit



Penguicon 4/2017
Tony Bemus

Notes:

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.

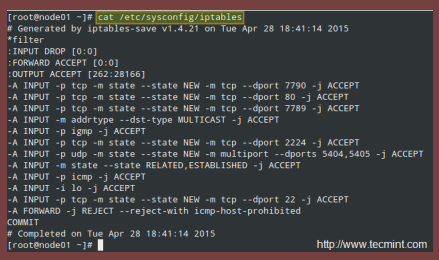
- Wikipedia.org Firewalls (Computing)

Notes:

Host Based Firewalls

Host based is an application installed on the machine and manages connections in and out of the single device.

Linux: IPTables, FirewallD, UFW
BSD: pf



Notes:

Network Based Firewalls

Network Based is a network appliance that controls the connections between two or more networks.
(Internal and Internet)
Most home routers have a basic firewall built into it now.

Linux Distros: IPCop / IPFire, Smoothwall, Sophos UTM
BSD: pfSense, OPNsense, BSD Router Project

Notes:

Firewall History

- First Generation Firewalls were called Packet Filters and first used in the late 1980s. In 1988 DEC published the first paper on Packet Filter Firewall systems.
- Second Generation Firewall are called Statefull Firewalls Orignaly called Circuit-level Gateways, AT&T Bell Labs developed them on 1990. The Statefull Firewall was first introduced by Checkpoint in 1994
- Third Generation Firewalls are call Application Gateways First developed in 1995 but because it was processor insinsive it iddn't become popular for some time. In 2012 some firewall manufactors rename it NGFW or the Next Generation Firewalls

Notes:

Packet Filtering

Packet Filter is the most basic type of firewall.

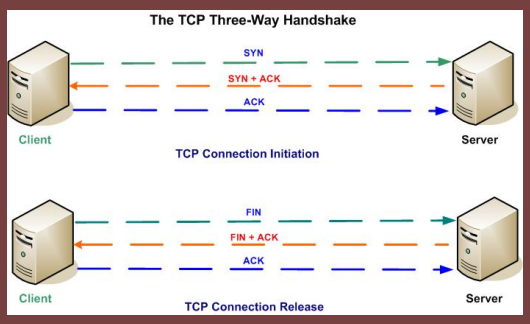
- It allows or denies network traffic based on the Source and Destination IP addresses, the port number, and Protocol (UDP/TCP).
- Packet filters work on OSI Layer 3 and treats each packet individually.
- Cisco ACL is a popular use of a packet filter still used today:
  access-list 107 permit tcp any 172.69.0.0 0.0.255.255 eq 23
  ACL Number, action, protocol, source IP , Destination IP, port

Notes:

Statefull Firewalls

- Statefull Firewall maintains a table of open connections,
  inspecting the payload of some packets and intelligently associating new connection requests with existing legitimate connections.
- OSI Layer 3 and 4.
- TCP uses a three way handshake to create and end a connections
  SYN, SYN-ACK, and ACK.
  FIN, FIN-ACK, and ACK.

  SYN is a new connection
  ESTABLISHED is a concurrent connection.



Notes:

Application Level/Layer Gateway (ALG)

- Operates on the OSI Layer 7
- Filters based on the application.
- Its considered to be an extension to a Statefull firewall and goes beyond the source/destination and port and inspects the application. It can tell the difference between HTTP for web and HTTP for file shareing.

Notes:

Who uses a firewall?

Everyone should be using one

Notes:

Creating Firewall Rules

Every rule needs a

- Source
- Destination
- Protocol
- Port or service.

Wild cards and supernets are acceptable.

By default everything is blocked
Thus ANY legitimate traffic needs to be allowed

All Rules are enforced top down.

Notes:

Typical Rules:

Action	Protocol	Source	Port	Destination	Port	Description
LAN Interface:						
allow	TCP	LAN	* (any)	Local IP	80,443,22	(Administration)
allow	* (any)	LAN	* (any)	* (any)	* (any)	Internet Access
WAN Interface:						
Deny	* (any)	* (any)	* (any)	* (any)	* (any)	(Implicit Default Rule)

Notes:

Sources

- https://en.wikipedia.org/wiki/Firewall_(computing)
- https://en.wikipedia.org/wiki/Stateful_firewall
- https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work
- https://distrowatch.com/search.php?ostype=All&category=Firewall&origin=All&basedon=All&notbasedon=None&desktop=All&architecture=All&package=All&rolling=All&isosize=All&netinstall=All&language=All&status=Active#simple

Notes:

Contact Info:

Tony Bemus

tony@bemushosting.com

http://bemushosting.com

This Presentation:

http://bemushosting.com/present/firewall

Notes: