Types of Firewalls and Configurations

Objectives

- Understand the differences between different kinds of firewalls
- Discuss how different firewalls protect different data

Firewalls

- Firewalls are designed to protect data
- There are 5 basic types:
  - Packet-based – IP addresses, packet type, port
  - Circuit-level – Sets up TCP connections, typically inside to outside
  - Stateful inspection – monitors connection state
  - Application level – Looks at application type traffic
  - Multilayer – All of the above

Network firewall topology

- Most firewalls are designed to protect systems themselves from internet traffic
- Network based firewalls include:
- Host Based Firewalls
- Dedicated or Bastion Host
- DMZ or Dual Bastion Host
- Distributed

Host Based

- Used to secure hosts themselves
- Software based
- Used primarily in operating systems
  - Windows Firewall
  - Iptables
  - Firewalld
- Should be on EVERY OS you have!
- Can be on home or consumer based routers

Bastion Hosts

- Protects systems on the network
- All traffic typically passes through
- Usually appliance with minimal code
- Very hardened dedicated OS
- OS has it’s own language
- Can be typically handle all types of traffic

DMZ

- Demilitarized Zone
- 2 Bastion Hosts with servers in the middle
- Outer bastion host usually has more systems open
- If internal DMZ host is compromised, internal systems are still protected

Distributed

- Most larger organizations have more than 1 firewall
- This is for 2 reasons
  - Can’t handle all the traffic
  - Disaster recovery
- Firewalls may talk to each other and share information such as:
  - Rules
  - Code
  - State of traffic

Application Level

- Application level firewalls operate in many different ways
- Most traditional way is to look at “normalized” traffic
- Think about a E-Commerce server
  - Used to processing cards
  - Fields only contain 16 digits
  - If data is more or less than that, firewalls protects system
- Web Application Firewalls
  - Designed to protect applications
  - Can be expensive due to the overhead