

# **Introduction to Firewalls**

## **Open Source Security Tools for Information Technology Professionals**

**School of Professional Studies (SPS)**

**The City University of New York (CUNY)**

Aron Trauring  
Adjunct Professor  
CEO, Zoteca

Class 5 October 24th, 2005

# What is a Firewall?

- Most important element of host defense against attack
- Filters all network traffic by examining all TCP/IP packets
- Decides whether to allow packet to continue on network or to drop packet

## Three Functions of a Firewall

1. Deal with incoming traffic
2. Deal with outgoing traffic
3. Log suspicious or malicious traffic

## Minimalism and Viligance

- Start: deny everything from everywhere and to everywhere
- Defining “bad behavior” puts you in an endless treadmill
- Access to host should be exception not the rule
- Create a wall and remove “bricks” for access one at a time

# Firewall Types

- Perimeter firewalls — Cisco PIX, Check Point, Smoothwall
- Perimeter firewalls are usually associated with routers
- Host firewalls — iptables, Zone Alarm

## TCP Three Way Handshake

- Machine wanting to communicate sends a SYN packet (“ready”)
- Receiving machines sends a SYN/ACK (“got it”)
- Sending machine sends ACK back (“I’m going to start sending”)

# TCP/IP Session Communication

- If three way handshake successful communication begins
- Data packets tagged with sequence numbers
- Acknowledges receipt of packets

## TCP/IP Session Close

- One side (can be either depending on circumstances) sends a FIN (“got everything”)
- Other machine sends a FIN/ACK (“ready to end”)
- Other side sends ACK back (“Let’s finish this”)

# Stateless Firewall

- Stateless firewall looks at packet headers
- Sees each packet in isolation not in context of a session
- Filters packets based on header only
- Prevents/allows connection from specific IP address or network
- Prevents/allows connection based on TCP/UDP port or type of application
- Prevents/allows connection based on category of packet (e.g. ICMP)

# Stateful Firewall

- Keeps track of state of TCP/IP session
- Can do more sophisticated packet filtering
- Block SYN packets

# Perimeter Firewalls

- Two or more ethernet connections
- Trusted network — internal LAN
- Public network — outside WAN
- DMZ — servers that need to be exposed to the outside but may serve internal functions
- Commercial boxes — many have Linux built in
- Built your own — use multiple NICs for ethernet connections
- Smoothwall — Linux based software distribution

## Firewall Setup Business Process

1. Develop a network use policy — IM? P2P?
2. Map out inbound and outbound services
3. Convert 1 and 2 into firewall rules
4. Implement firewall rules and test
5. Review and test periodically

# Host Firewalls

- Securing perimeter is not enough
- Particularly important on bastion hosts and trusted computer
- Bastion host — internet-facing server
- Problematic on client machines