# Countering SYN Flood Denial-of-Service (DoS) Attacks

**Ross Oliver**

**Tech Mavens**

**reo@tech-mavens.com**

# What is a Denial-of-Service (DoS) attack?

- Attacker generates unusually large volume of requests, overwhelming your servers
- Legitimate users are denied access
- Can last from a few minutes to several days

# What is a SYN Flood?

- One kind of Denial-of-Service attack
- Simulates initial handshake of TCP/IP connection
- Web servers are particularly vulnerable

# Example SYN Flood Attack

- February 5th – 11th, 2000
- Victims included CNN, eBay, Yahoo, Amazon
- Attacks allegedly perpetrated by teenagers
- Used compromised systems at UCSB

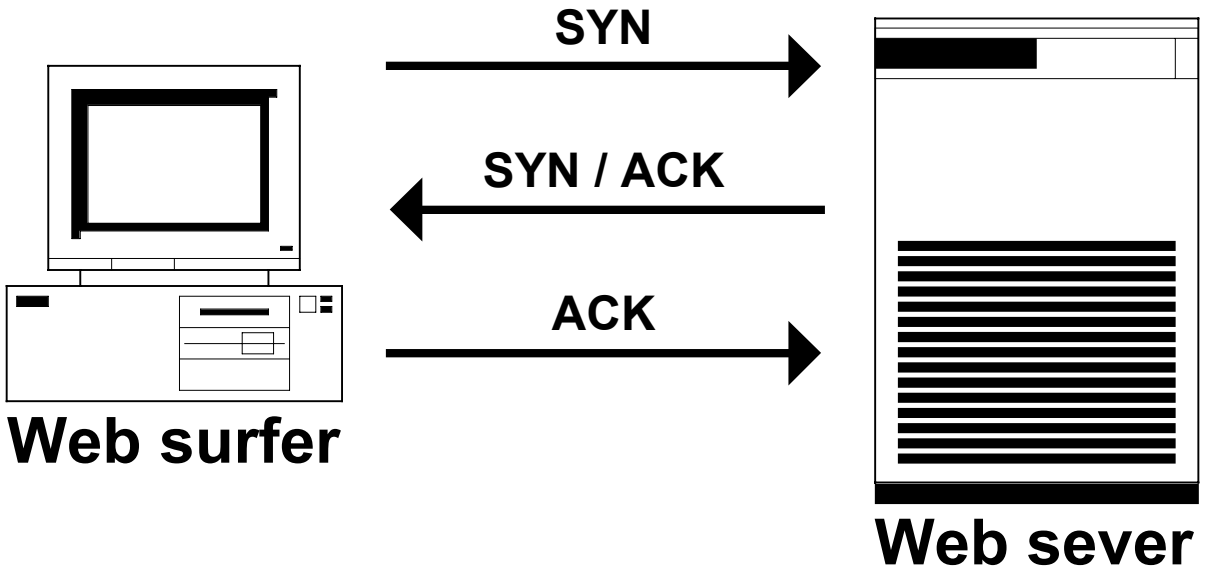
# Detailed Account of DDoS

- Gibson Research Corporation
  www.grc.com/dos/intro.htm
- May 4th–20th, 2001
- DDoS attack from 474 machines
- Completely saturated two T1s
- 13-year-old claimed responsibility

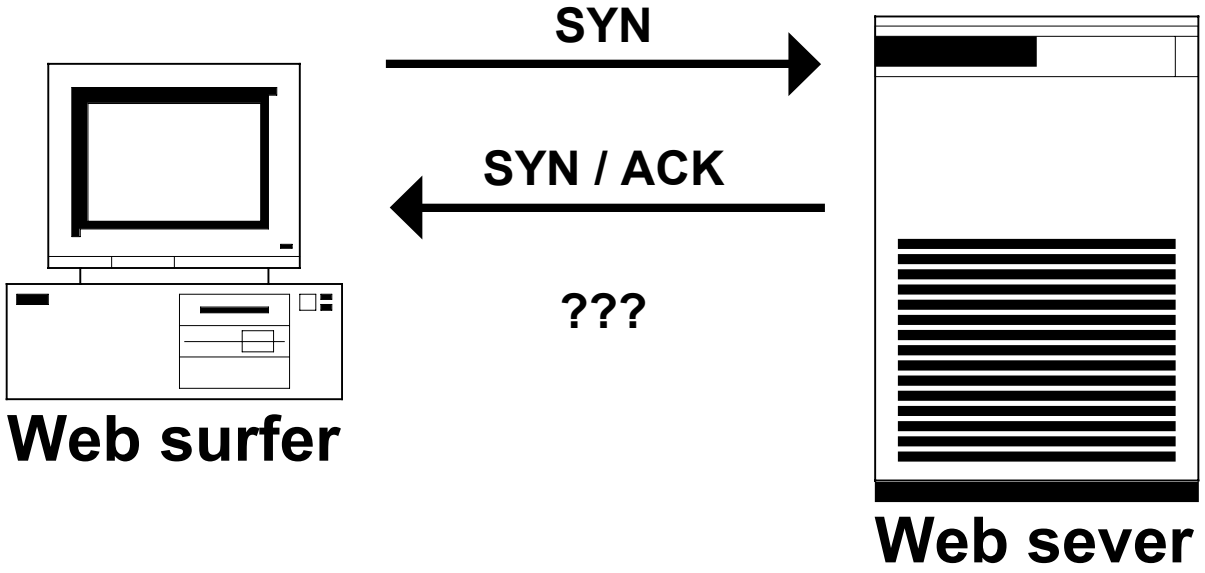
# Don't Expect Outside Help

- GRC discovered:
- ISPs were unresponsive
- Law enforcement unable to help
- Under-age perpetrators have blanket immunity

# Normal TCP/IP Connection Initiation



# Unfinished TCP/IP Connection Initiation



# Web Server's Table of Normal TCP/IP Connections

| Address | Port | State |
|---|---|---|
| 192.168.3.16 | 80 | ESTABLISHED |
| 192.168.15.88 | 80 | TIME_WAIT |
| 192.168.3.94 | 80 | ESTABILISHED |
| 192.168.54.7 | 80 | SYN |
| 192.168.27.112 | 80 | ESTABLISHED |
| 192.168.4.23 | 80 | TIME_WAIT |
| 0.0.0.0 | 0 | FREE |
| 0.0.0.0 | 0 | FREE |
| 0.0.0.0 | 0 | FREE |

# Connections Table During SYN Flood

| Address | Port | State |
|---|---|---|
| 192.168.7.99 | 80 | SYN |
| 192.168.7.99 | 80 | SYN |
| 192.168.7.99 | 80 | SYN |
| 192.168.7.99 | 80 | SYN |
| 192.168.7.99 | 80 | SYN |
| 192.168.7.99 | 80 | SYN |
| 192.168.7.99 | 80 | SYN |
| 192.168.7.99 | 80 | SYN |
| 192.168.7.99 | 80 | SYN |
| 192.168.7.99 | 80 | SYN |

# Why Defense is Difficult

- SYN packets are part of normal traffic
- Source IP addresses can be faked
- SYN packets are small
- Lengthy timeout period

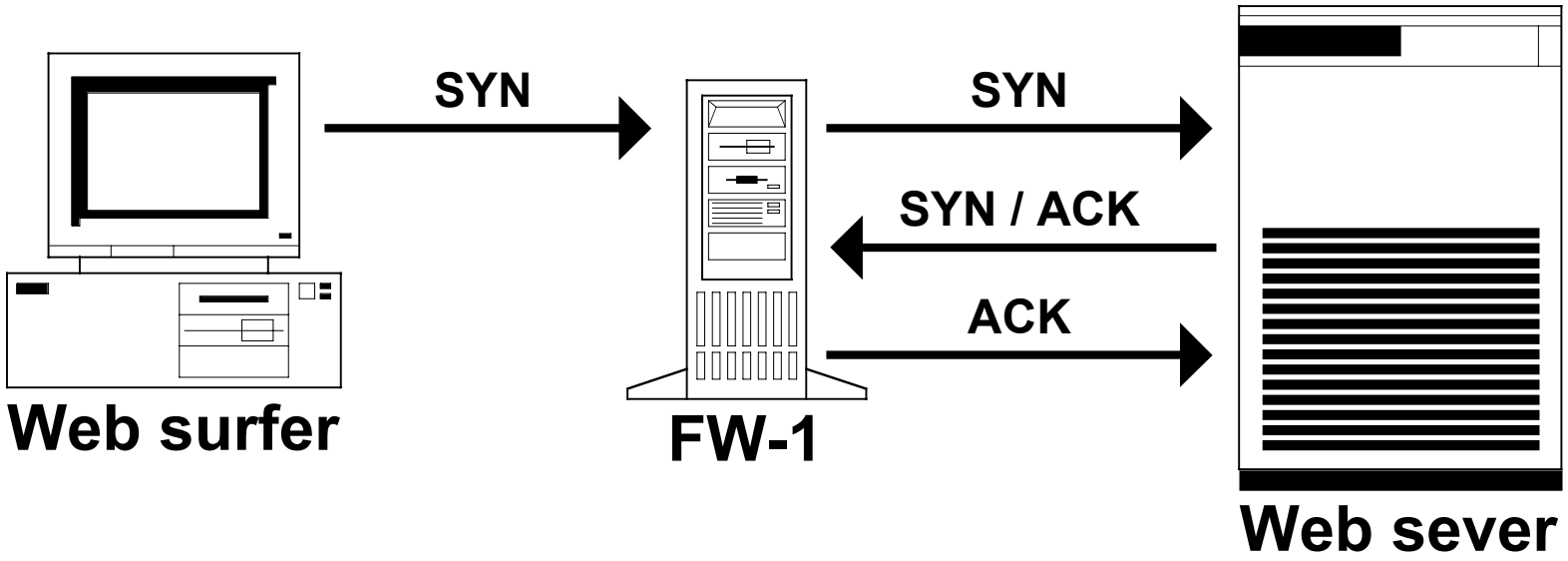
# Possible Defenses

- Increase size of connections table
- Add more servers
- Trace attack back to source
- Deploy firewalls employing SYN flood defense

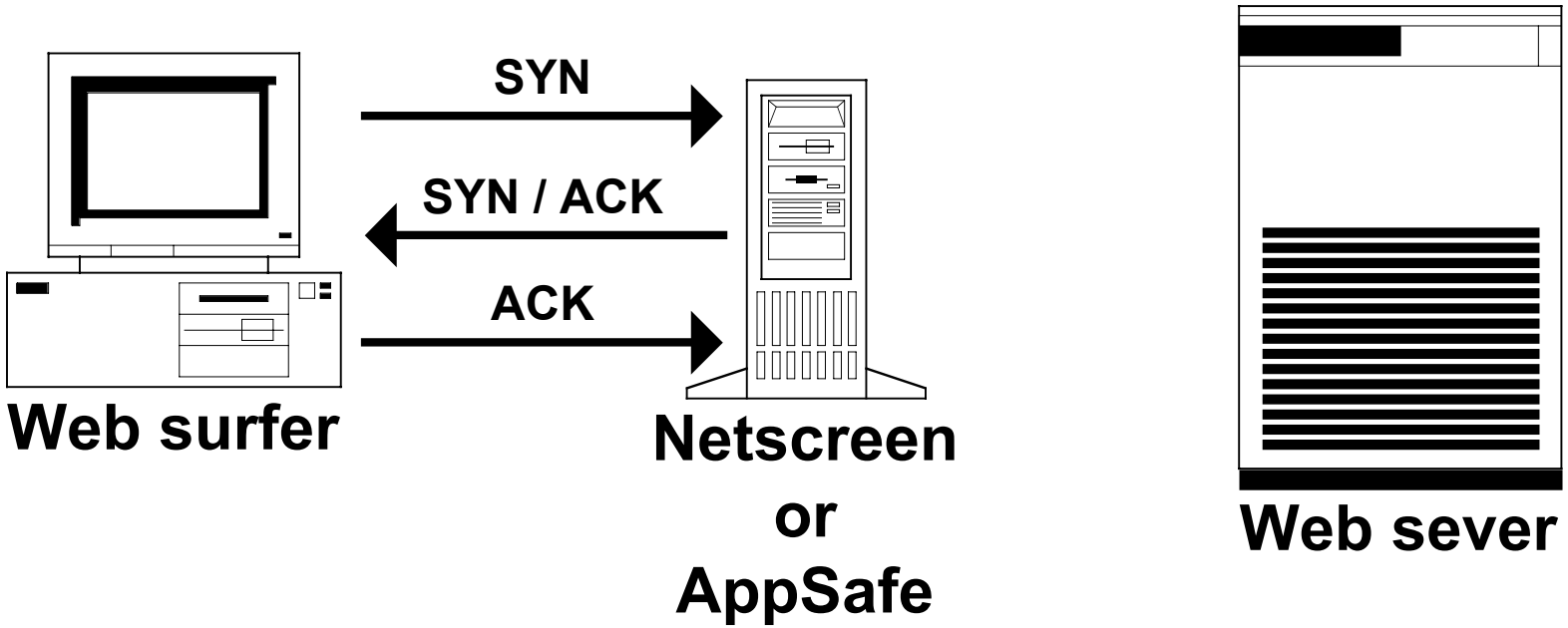
# Who Offers a Defense?

- PIX by Cisco
- Firewall-1 by Checkpoint
- Netscreen 100 by Netscreen
- AppSafe/AppSwitch by Top Layer

# Firewall-1 SYNDefender



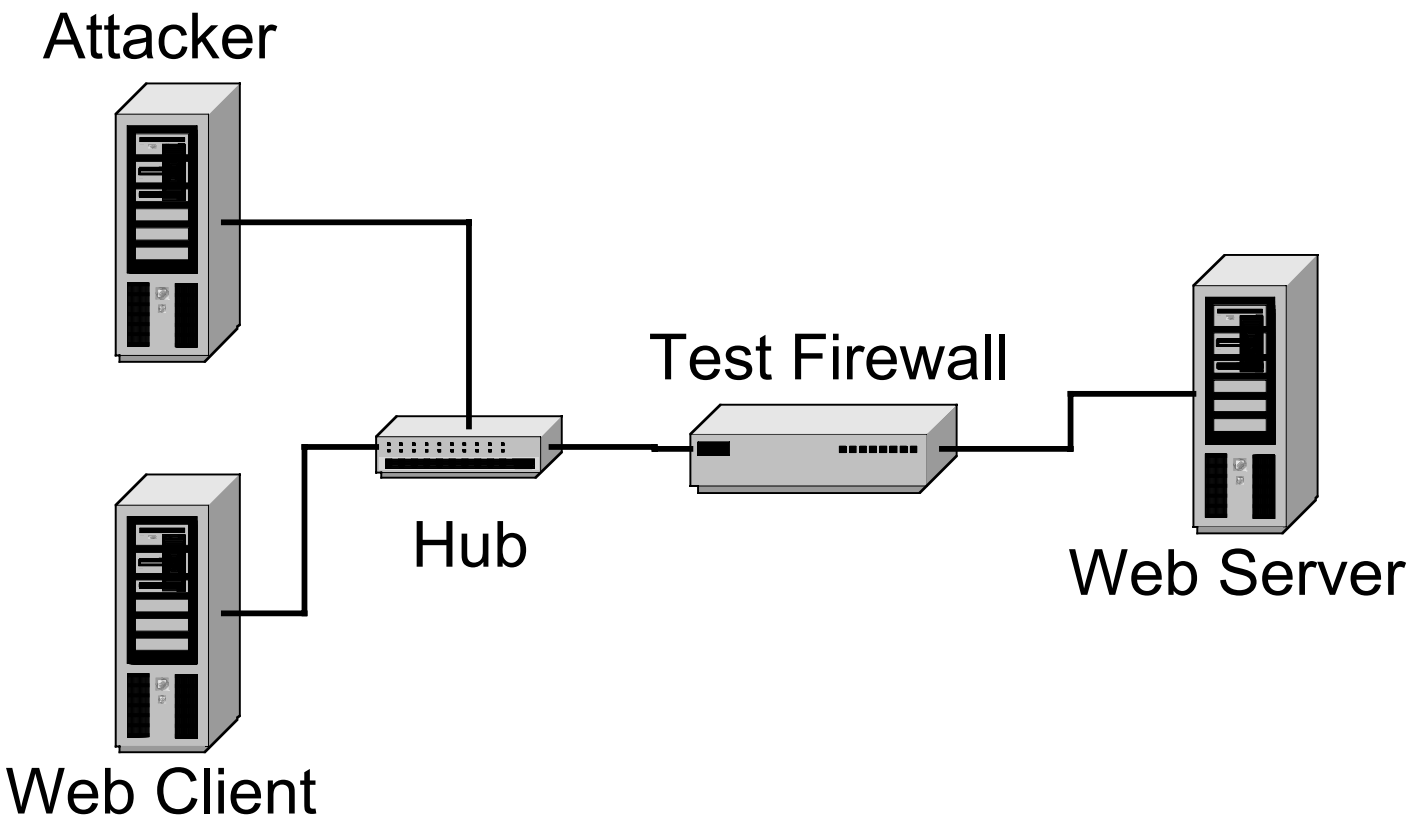
# SYN Proxy



# Measuring Effectiveness

- Create a realistic test environment
- Generate a SYN flood
- Measure how well each firewall keeps legitimate traffic flowing

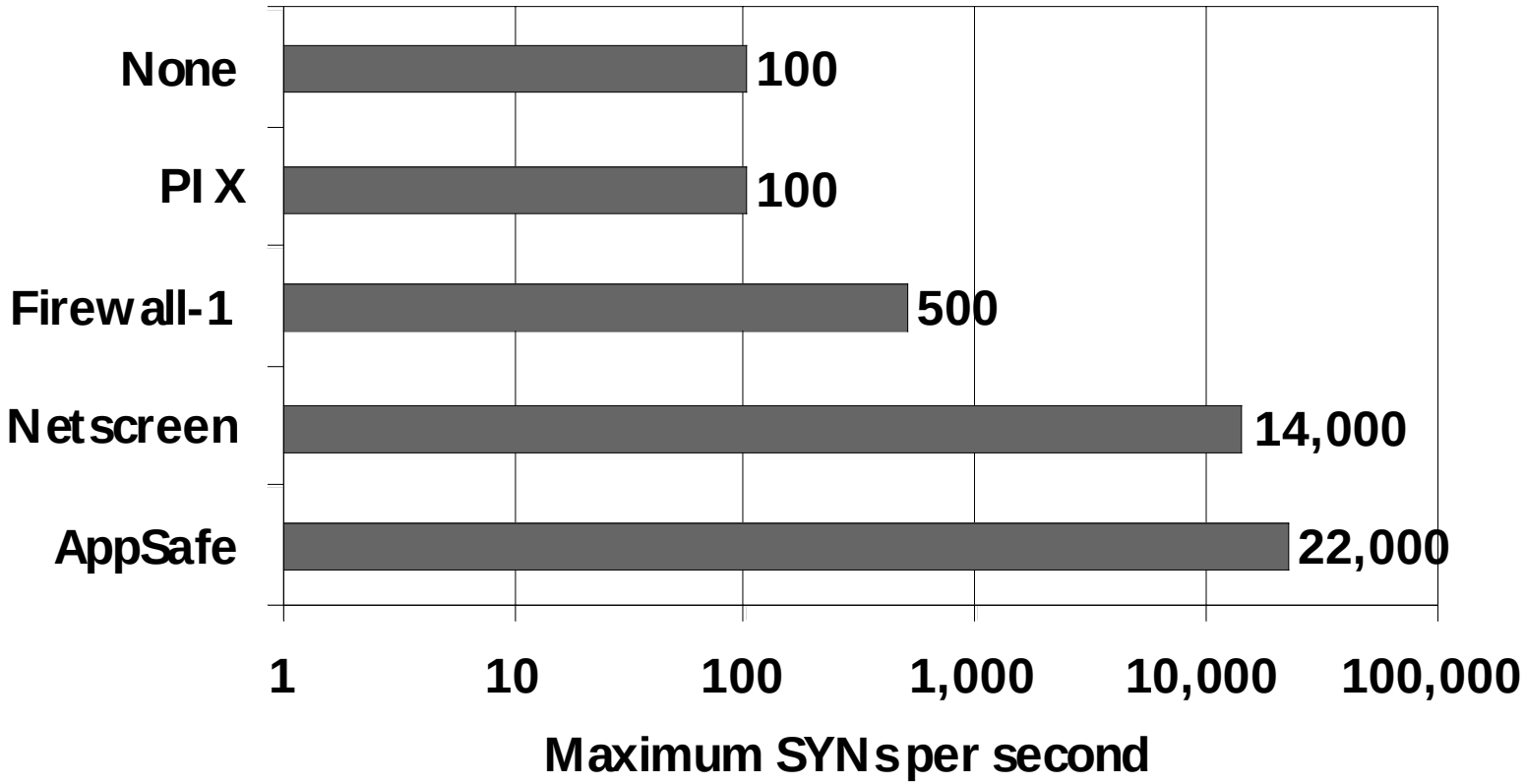
# Test Configuration



# Test Configuration

- Web Server: Linux (RedHat 7.2)
  - Apache web server
- Web Client: Windows 2000
  - Script using wget to fetch web pages, measure response time
- Attacker: Linux (RedHat 7.2)
  - SYN flood generator

# Benchmark Results



# Cisco PIX Results

- No significant difference over no firewall
- Large “embrionic” value allowed flood through to server
- Small “embrionic” value blocked both flood and normal traffic

# Firewall-1 Results

- Protected up to 500 SYNs/sec, but with degraded response time
- Above 500 SYNs/sec, web page requests failed
- Web server recovered to normal 3-10 minutes after attack ceased

# Netscreen 100 Results

- Protected up to 14,000 SYNs/sec with acceptable server response times
- Above 14,000, web server continued to respond, with increasing delays
- Response times recovered to normal immediately after attack ceased

# AppSafe Results

- Effective up to 22,000 SYNs/sec
- Maximum test setup could produce
- No measurable change in response time

# How Bad Can It Get?

- Theoretical maximums for attackers using:
  - Analog modem: 87 SYNs/sec
  - ISDN, Cable, DSL: 200 SYNs/sec
  - T1: 2,343 SYNs/sec
  - 474 hacked systems 94,800 SYNs/sec

# How Much Do You Need?

- Single firewall for attacker with single ISDN, DSL, or T1
- Multiple parallel units for higher bandwidth
- “Transparent” mode permits rapid deployment

# Conclusion

- SYN floods are nasty
- Firewalls with SYN flood defense can successfully counter attacks
- Multiple or distributed attacks may require multiple parallel firewalls

# Acknowledgements


- PIX provided by Atebion, Inc.
- Netscreen 100 provided by Yipes Communications
- AppSafe provided by Top Layer Networks
- Information Warehouse! Inc.