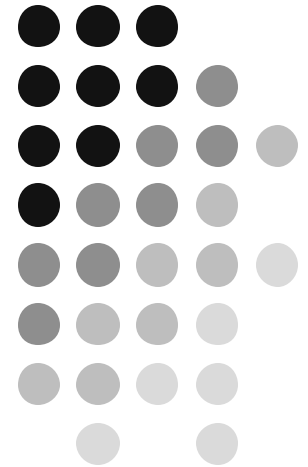
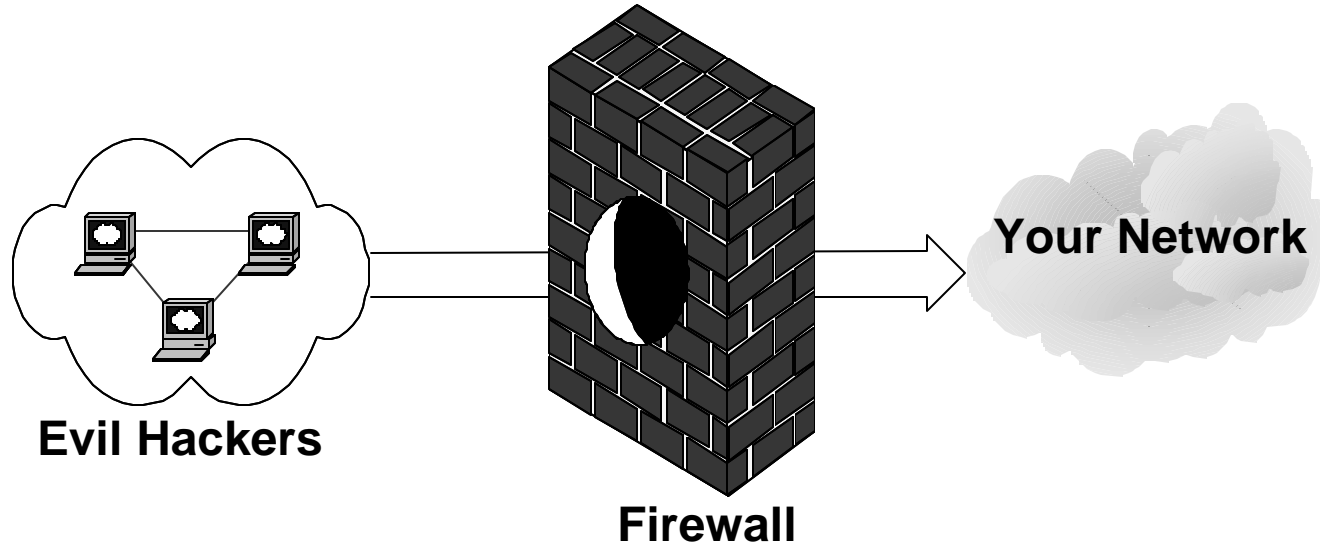
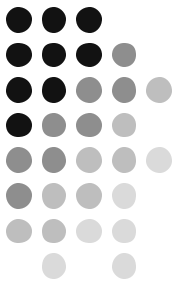


Firewall Tips & Tricks

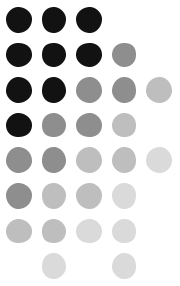
Paul Asadoorian
Network Security Engineer
Brown University
November 20, 2002



Holy Firewall Batman!

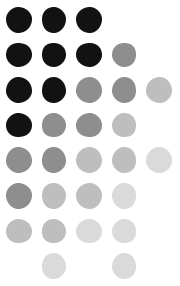


Defense in Depth

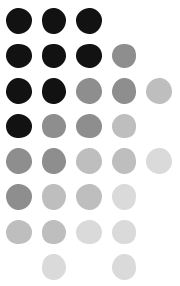


- Firewalls mitigate risk
- Blocking MOST threats
- They have vulnerabilities as well
- Improper configuration is the largest threat

Tips & Tricks Outline

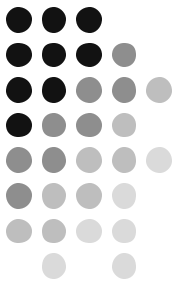


- Using the “DMZ” to your advantage
- Firewalls as Intrusion Detection devices
- Configure VPN’s for management



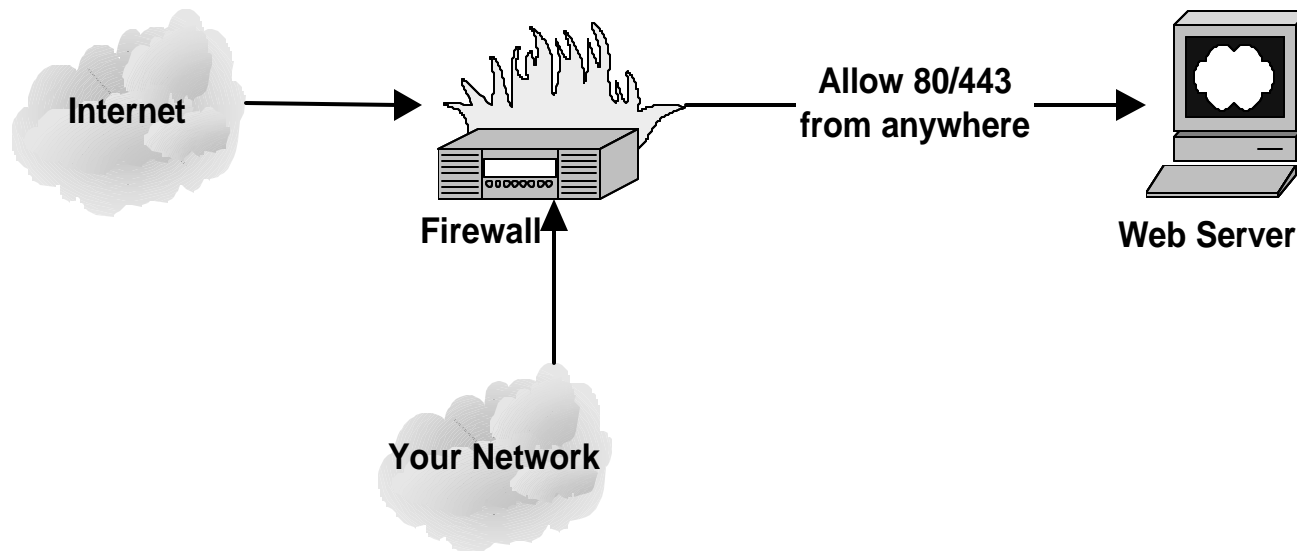
The “DMZ” Configuration

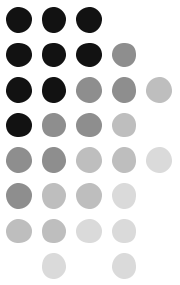
- Separate area off the firewall
- Usually a different subnet
- Commonly used to house Internet facing machines (i.e. Web Servers)
- Has its own firewall policy



The “DMZ” Configuration

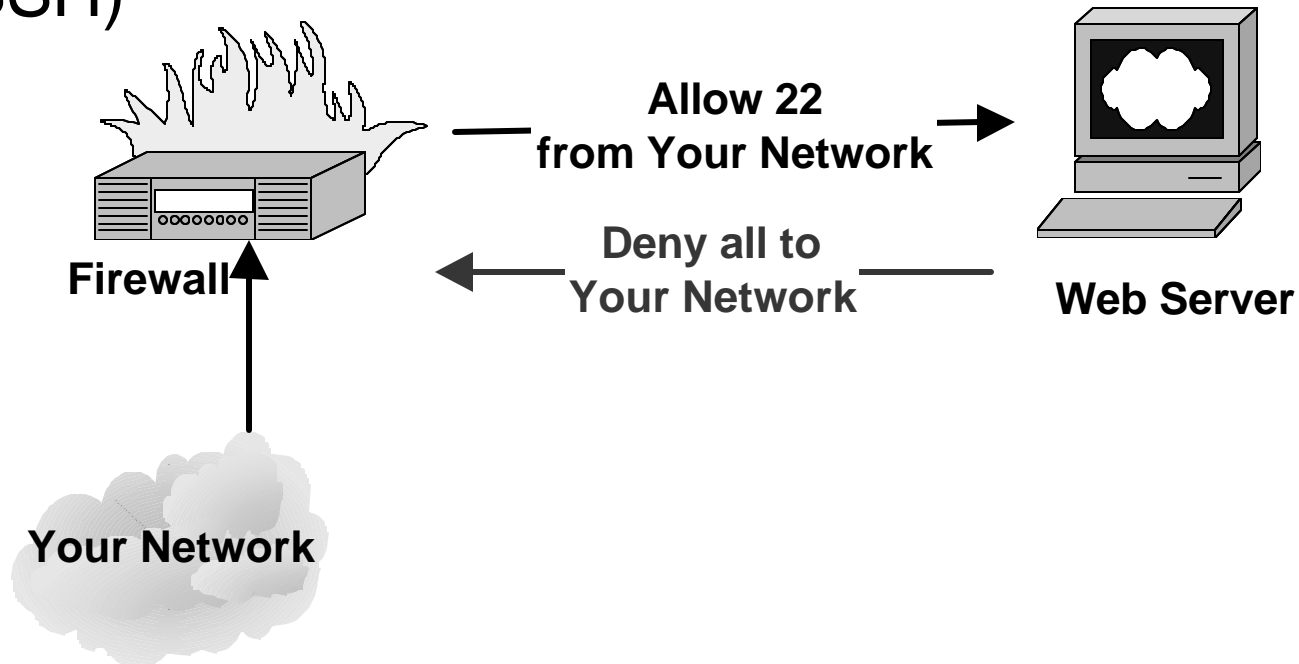
- Place web servers in the “DMZ” network
- Only allow web ports (TCP ports 80 and 443)



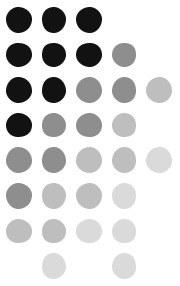


The “DMZ” Configuration

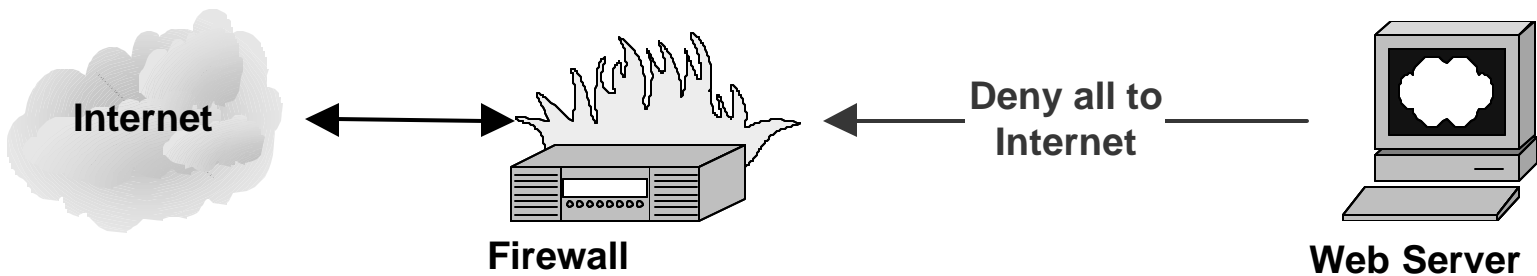
- Don't allow web servers access to your network
- Allow local network to manage web servers (SSH)



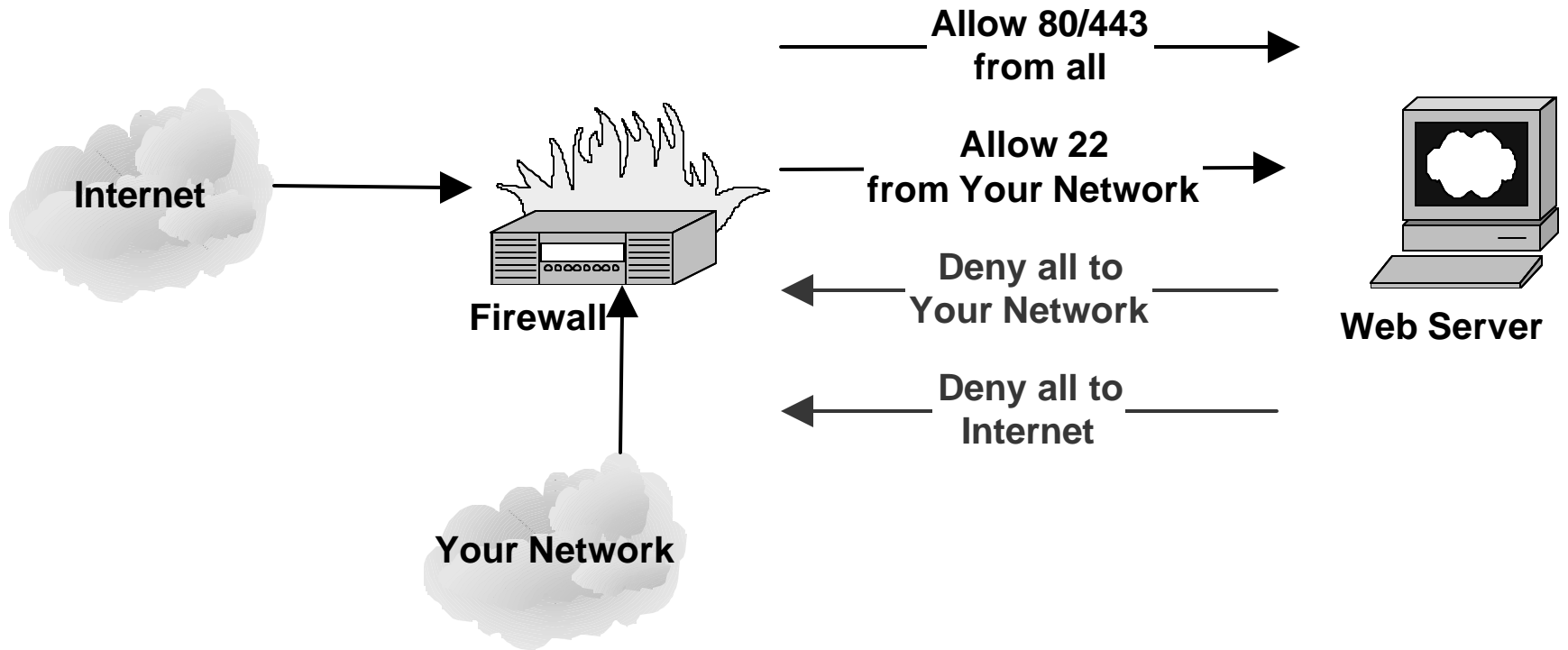
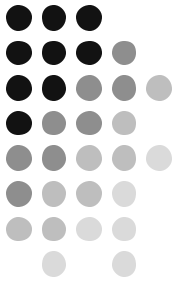
The DMZ Configuration



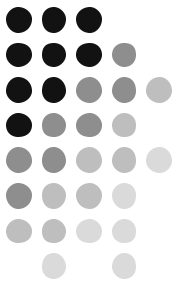
- Don't allow servers to connect to the Internet
- Patching is not convenient



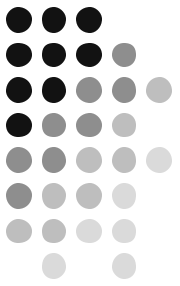
The DMZ Configuration



Firewalls as IDS



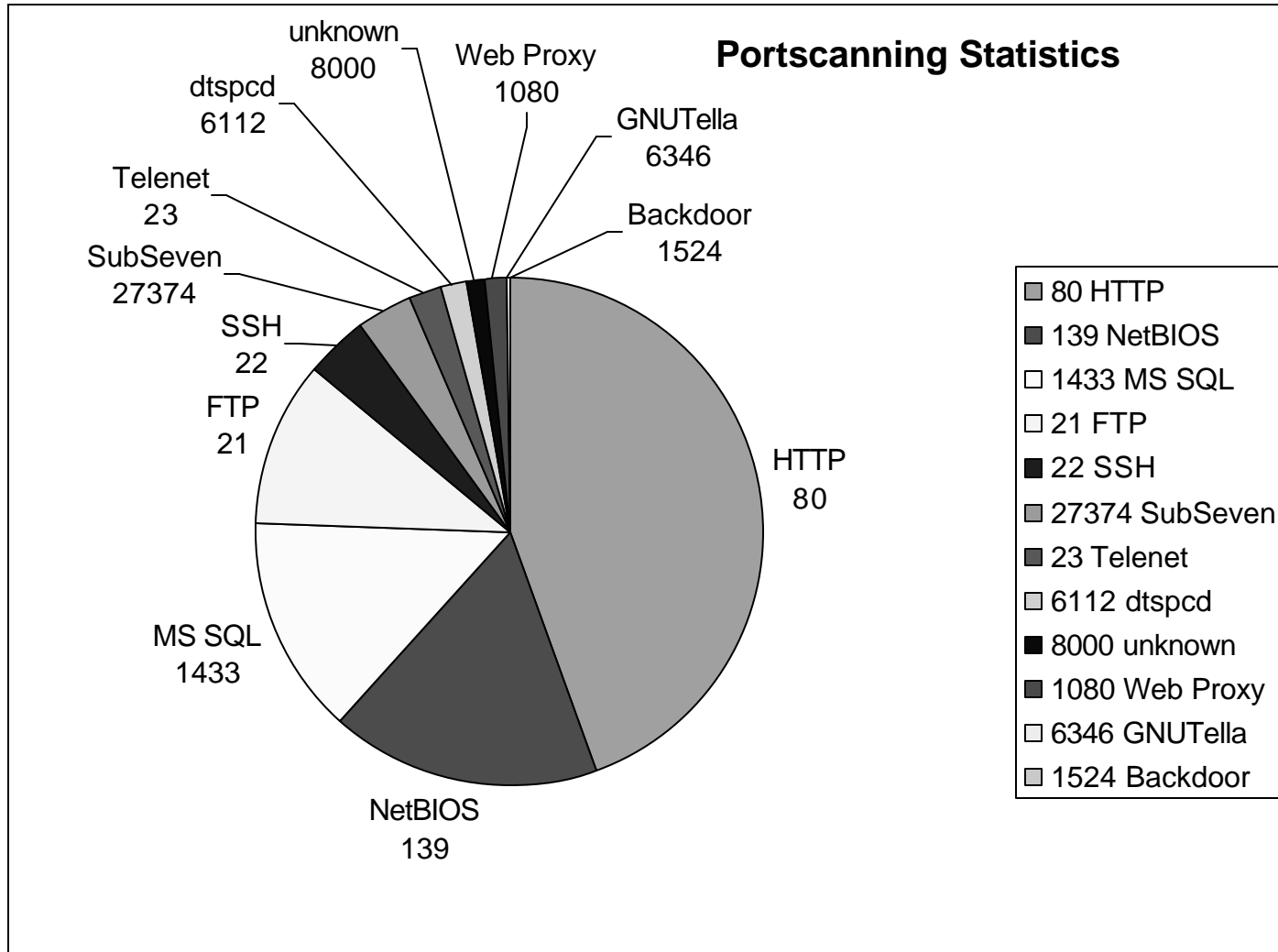
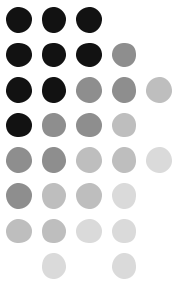
- Collect log information from the deny rules
- Find Portscanning, hacking attempts, etc...
- Isolate traffic with deny rules helps cut down the information overload



Firewalls as IDS

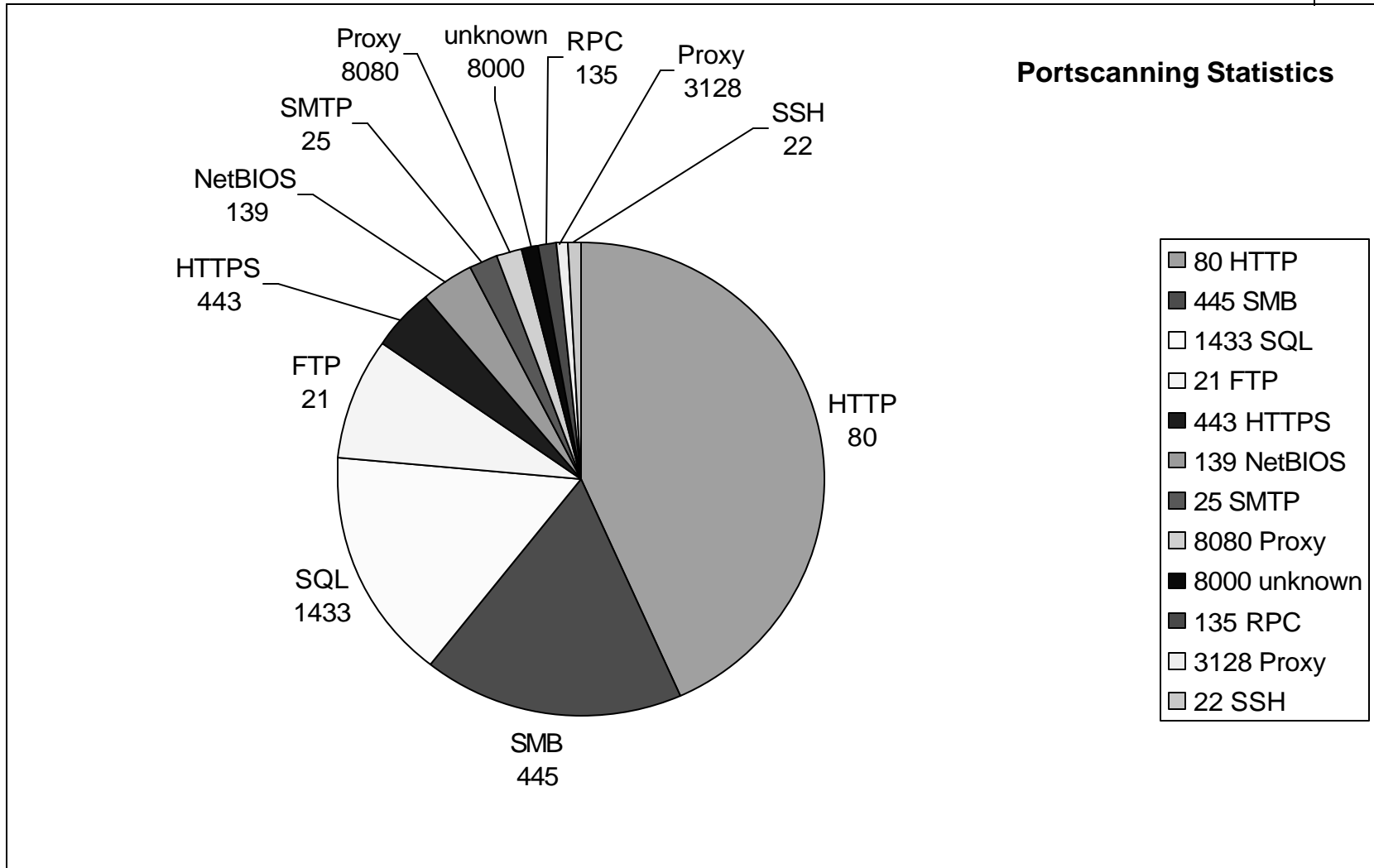
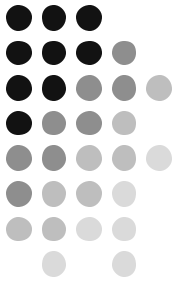
- What to do with ALL that data.....Graph It!
- Shows trends, what people are looking for
 - Helps prioritize security tasks
- Occasionally you may want to block portscans

Firewalls as IDS

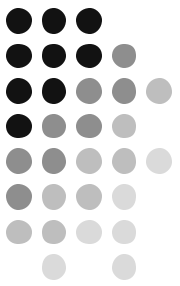


Data collected from July – August 2002, Brown University Network

Firewalls as IDS

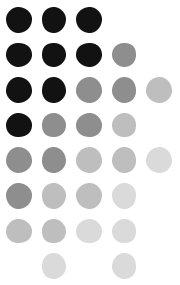


Data collected from October – November 2002, Brown University Network



Firewall as IDS

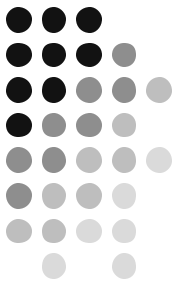
- Pay close attention to traffic leaving DMZ
- Often the first sign of a compromise
- Low traffic rules, so logs aren't as enormous
- Email is nice, provided you're the only one reading it



Firewalls as IDS

- Ways to accomplish alerting:
 - Swatch
<http://www.oit.ucsb.edu/~eta/swatch/>
 - Logsentry
<http://www.psionic.com/products/logsentry.html>
 - Alert.sh (Firewall-1)
<http://www.enteract.com/~lspitz/intrusion.html>

Firewall as IDS



Date: Wed, 31 Dec 1997 15:40:01 -0600 (CST)
From: ids@example.net To: fwadmin@example.net
Subject: ##### Firewall ALERT #####

You have received this message because someone is potentially scanning your systems. The information below is the packet that was denied and logged by the Firewall. This is email alert number 3, with a limit of 5 from evil.example.org.

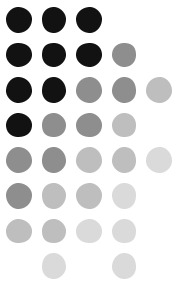
----- CRITICAL INFORMATION -----

Date: 31Dec1997 Time: 15:39:59 Source: evil.example.org
Destination: ns1 Service: domain-tcp

----- ACTUAL LOGENTRY -----

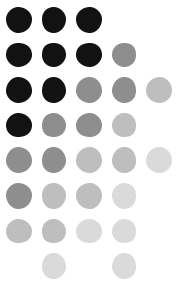
31Dec1997 15:39:59 drop fw1 >elx0 mail proto tcp src
evil.example.org dst ns1 service domain-tcp s_port 37401 len 44
rule 6

Configuring VPN For Management

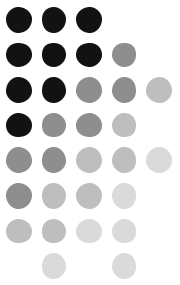


- VPN is far more secure than other management methods:
 - SSL and SSH are vulnerable to Man-In-The Middle Attacks
 - Telnet and SNMP are clear text
 - There are no known MIM attacks against IPSEC (Yet)

Configuring VPN For Management



- VPN clients are supported on most platforms
- Most firewalls will work with most clients
- Netscreen now officially supports FreeSwan
- Mac OS X is now supporting VPN



Useful Links

- <http://www.enteract.com/~lspitz/> - Lance Spitzner's Web Site
- http://rr.sans.org/firewall/blocking_ipchains.php - Guide to blocking ports
- <http://rr.sans.org/firewall/index.php> - All sorts of good stuff