ELEN 689: Topics in Network Security: Firewalls

Ellen Mitchell
Computing and Information Services
20 April 2006

© Ellen Mitchell, 2006
Firewall

• Historically: a wall constructed to prevent the spread of fire
Firewall Function

• Used on computer networks to protect one area from another

• Permits or denies access to computer services
Security “Stances”

- Deny-Based (deny by default)
- Allow-Based (allow by default)
Protocols

• Generally TCP/UDP IP (v4), ICMP
Types of Firewalls

Generally correspond to a layer in the ISO model

<table>
<thead>
<tr>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation</td>
</tr>
<tr>
<td>Session</td>
</tr>
<tr>
<td>Transport</td>
</tr>
<tr>
<td>Network</td>
</tr>
<tr>
<td>Data Link</td>
</tr>
<tr>
<td>Physical</td>
</tr>
</tbody>
</table>
Hardware/Software

• Dedicated hardware is fast, though may not be as flexible as software firewalls

• Software firewalls tend to run on top of or as part of an operating system (needing security updates)
Host-based/Network-based

- Protect one computer?
- Protect many?
- Recommend layers of protection
Firewalls

• Packet Filter
• Stateful Packet Filter
• Proxy
• Hybrids
Packet Filters

- Work at layers 3 and 4
- Make packet-level decisions
- Simple, powerful, fast
Packet Filter Decisions

• Source or destination host
• Source or destination port
• Protocol (TCP/UDP/ICMP)
Three-way handshake

Host 1

SYN

SYN/ACK

ACK

Host 2
Stateless Firewalls

- No knowledge of previous traffic is used to make decision on whether to permit/deny the next packet
Stateful Firewalls

- Firewall keeps a record of previous traffic
- Permits traffic if it belongs to the current “session”
- Flags (SYN, FIN, RST; ECHO REQ/REP, etc.)
Stateless/Stateful Trade-offs

- Speed
- Additional security
Proxy Firewall

- Application-level decisions
- Applies to protocols such as HTTP, rather than TCP
- Protects computers because they don’t receive traffic directly
Before Proxy Firewall

Inside Firewall

Server

... 

Outside Firewall

Bad Guy >:[

Firewall

© Ellen Mitchell, 2006
Using Proxy Firewall

Inside Firewall

Server

Proxy

Outside Firewall

Bad Guy >:[

Firewall

© Ellen Mitchell, 2006
Hybrids

• Combinations and customization are possible
Response when traffic’s denied

- Drop packets (TCP RST) or time out?
- People tend to prefer one or another
- Some firewalls offer configuration options for this
Personal Firewalls

• Many available at reasonable cost

• BlackIce -- http://www.netice.com/ ($39.95)

• ZoneAlarm -- http://zonelabs.com/ (Free)

• ConSeal -- http://www.signal9.com/ ($49.95)

• IPChains -- linux kernel (Free)
Securing Hosts

- Eliminate Extra Services
- Educate Users
- Use good passwords
Firewall Weaknesses

- Misconfiguration
- Misunderstanding
Network Address Translation (NAT)

- Process that maps addresses between an external network and (hides the addresses on) the internal network
- One to one, one to many
- Increase in “security” is debatable
Virtual Private Networks (VPN)

- Allows people outside the firewall to authenticate and connect to the inside of the firewall
- Permissions are configurable
- Removes the need to open ports through the firewall
VPN Implementation

- Students, Faculty, Staff
- No additional cost
- “neo” login/password
VPN Implementation continued

• Client software at
  http://www.net.tamu.edu/network/vpn.html

• Not all hand-helds are supported, but we’re trying to improve that
Technical Overview

Drivers
- Shim
- OS
- RADIUS Database
- LDAP
- Key Negotiation (IKE) via UDP
- IPSEC (IP+AH & ESP)
- Regular IP
  - (Address Translation is performed)
  - (Address Translation Not Done)
  - Non-TAMU traffic

Campus machine

VPN Server

Firewall

Drivers Shim

OS

Home machine
Firewalls on Campus

- Campus Firewall
- NetSQUIP
- F-boxes
- Departmental firewalls
- Government Regulations
- Credit Card Industry
- Equipment Protection
TAMU Firewall

• History
  - Implemented in 1992
    • Assembly, DOS, Unix
    • “Drawbridge” freely available (http://drawbridge.tamu.edu/)

• Supports our Gig connection to the Internet

© Ellen Mitchell, 2006
NetSQUID

- “Network Security Quarantine and Isolation Device”
- Used in Residence Halls + some departments
- Linux-based
- Uses “iptables” + snort
- Intrusion detection + firewall
F-boxes

• These firewalls enforce our policy that wireless traffic must be authenticated and encrypted

• Permit only IPSEC traffic to cross the Access Point to reach the Rest Of The World

• (Forcing VPN enforces our policy)
Departmental Firewalls

• Some departments on campus want to further protect themselves from, say, the Residence Halls 😊
Government Regulations

• Some research areas are regulated and must meet federal guidelines... Patriot Act, Office of the State Chemist, etc.
Credit Card Industry

• VISA/MasterCard have regulations on how credit card transactions may be done using computers

• Requires NAT
Equipment Protection

• Some vendors’ products are based on old, vulnerable operating systems
Summary

• Types of firewalls
  - Packet filter, proxy,
  - Stateful/stateless
  - Host-based, network-based

• Security stances
  - Allow-based, deny-based
Local resources...

- TAMU firewall papers
  - ftp://net.tamu.edu/pub/security/TAMU/tamu-security-overview.ps and tamu_summary.txt

- TAMU firewall change request information
  - http://net.tamu.edu/network/tcpip.html#Firewall

- Choose a firewall based on your needs
Resources continued...

- TAMU VPN information page
  - http://net.tamu.edu/network/vpn.html

- TAMU ISF page
  - http://cis.tamu.edu/security/isf/

- My team’s page
  - http://security.tamu.edu/
Questions?