Chapter 20 – Firewalls

The function of a strong position is to make the forces holding it practically unassailable

—On War, Carl Von Clausewitz
Introduction

- seen evolution of information systems
- now everyone want to be on the Internet
- and to interconnect networks
- has persistent security concerns
  - can't easily secure every system in org
- typically use a **Firewall**
- to provide **perimeter defence**
- as part of comprehensive security strategy

What is a Firewall?

- a **choke point** of control and monitoring
- interconnects networks with differing trust
- imposes restrictions on network services
  - only authorized traffic is allowed
- auditing and controlling access
  - can implement alarms for abnormal behavior
- provide NAT & usage monitoring
- implement VPNs using IPSec
- must be immune to penetration
What is a Firewall?

Firewall Limitations

- cannot protect from attacks bypassing it
  - eg sneaker net, utility modems, trusted organisations, trusted services (eg SSL/SSH)
- cannot protect against internal threats
  - eg disgruntled or colluding employees
- cannot protect against access via WLAN
  - if improperly secured against external use
- cannot protect against malware imported via laptop, PDA, storage infected outside
Firewalls – Packet Filters

- simplest, fastest firewall component
- foundation of any firewall system
- examine each IP packet (no context) and permit or deny according to rules
- hence restrict access to services (ports)
- possible default policies
  - that not expressly permitted is prohibited
  - that not expressly prohibited is permitted
Firewalls – Packet Filters

Attacks on Packet Filters

- **IP address spoofing**
  - fake source address to be trusted
  - add filters on router to block

- **source routing attacks**
  - attacker sets a route other than default
  - block source routed packets

- **tiny fragment attacks**
  - split header info over several tiny packets
  - either discard or reassemble before check

Table 20.1 Packet-Filtering Examples

<table>
<thead>
<tr>
<th>Action</th>
<th>src</th>
<th>port</th>
<th>dest</th>
<th>port</th>
<th>flags</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>block</td>
<td>*</td>
<td>*</td>
<td>SPGOT</td>
<td>*</td>
<td>don’t trust these people</td>
</tr>
<tr>
<td></td>
<td>allow</td>
<td>OUR,GW</td>
<td>25</td>
<td>*</td>
<td>*</td>
<td>connection to our SMTP port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>src</th>
<th>port</th>
<th>dest</th>
<th>port</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>block</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>default</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>src</th>
<th>port</th>
<th>dest</th>
<th>port</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>allow</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>src</th>
<th>port</th>
<th>dest</th>
<th>port</th>
<th>flags</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>allow</td>
<td>{our hosts}</td>
<td>*</td>
<td>*</td>
<td>25</td>
<td>our packets to their SMTP port</td>
</tr>
<tr>
<td></td>
<td>allow</td>
<td>*</td>
<td>25</td>
<td>*</td>
<td>ACK</td>
<td>their replies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>src</th>
<th>port</th>
<th>dest</th>
<th>port</th>
<th>flags</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>allow</td>
<td>{our hosts}</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>our outgoing calls</td>
</tr>
<tr>
<td></td>
<td>allow</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>ACK</td>
<td>replies to our calls</td>
</tr>
<tr>
<td></td>
<td>allow</td>
<td>*</td>
<td>*</td>
<td>&gt;1024</td>
<td></td>
<td>traffic to non-servers</td>
</tr>
</tbody>
</table>
Firewalls – Stateful Packet Filters

- traditional packet filters do not examine higher layer context
  - i.e. matching return packets with outgoing flow
- stateful packet filters address this need
- they examine each IP packet in context
  - keep track of client-server sessions
  - check each packet validly belongs to one
- hence are better able to detect bogus packets out of context
- may even inspect limited application data

Firewalls - Application Level Gateway (or Proxy)

- have application specific gateway / proxy
- has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
  - can log / audit traffic at application level
- need separate proxies for each service
  - some services naturally support proxying
  - others are more problematic
Firewalls - Application Level Gateway (or Proxy)

- relays two TCP connections
- imposes security by limiting which such connections are allowed
- once created usually relays traffic without examining contents
- typically used when trust internal users by allowing general outbound connections
- SOCKS is commonly used
**Firewalls - Circuit Level Gateway**

- **Circuit Level Gateway**
  - Highly secure host system
  - Runs circuit / application level gateways
  - Or provides externally accessible services
  - Potentially exposed to "hostile" elements
  - Hence is secured to withstand this
    - Hardened O/S, essential services, extra auth
    - Proxies small, secure, independent, non-privileged
  - May support 2 or more net connections
  - May be trusted to enforce policy of trusted separation between these net connections

---

**Bastion Host**

- Highly secure host system
- Runs circuit / application level gateways
- Or provides externally accessible services
- Potentially exposed to "hostile" elements
- Hence is secured to withstand this
  - Hardened O/S, essential services, extra auth
  - Proxies small, secure, independent, non-privileged
- May support 2 or more net connections
- May be trusted to enforce policy of trusted separation between these net connections
Host-Based Firewalls

- s/w module used to secure individual host
  - available in many operating systems
  - or can be provided as an add-on package
- often used on servers
- advantages:
  - can tailor filtering rules to host environment
  - protection is provided independent of topology
  - provides an additional layer of protection

Personal Firewalls

- controls traffic between PC/workstation and Internet or enterprise network
- a software module on personal computer
- or in home/office DSL/cable/ISP router
- typically much less complex than other firewall types
- primary role to deny unauthorized remote access to the computer
- and monitor outgoing activity for malware
Personal Firewalls

Firewall Configurations

(a) Screened host firewall system (single-homed bastion host)
Firewall Configurations

(b) Screened host firewall system (dual-homed bastion host)

(c) Screened-subnet firewall system
**DMZ Networks**

- **Internal DMZ network**
  - Web server(s)
  - Email server
  - DNS server

- **Internal protected network**
  - Application and database servers
  - Workstations

**Virtual Private Networks**

- Users system with IPSec
- Ethernet switch
- Firewall with IPSec
- Ethernet switch
- Firewall with IPSec
- Public (Internet) or Private Network
- IPSec Encapsulator
- IKE Encapsulator
Distributed Firewalls

Summary of Firewall Locations and Topologies

- host-resident firewall
- screening router
- single bastion inline
- single bastion T
- double bastion inline
- double bastion T
- distributed firewall configuration
Summary

- have considered:
  - firewalls
  - types of firewalls
    - packet-filter, stateful inspection, application proxy, circuit-level
  - basing
    - bastion, host, personal
  - location and configurations
    - DMZ, VPN, distributed, topologies