FIREWALL

- An integrated collection of security measures designed to control traffic flow into and out of a network.
- Similar to firewalls in building construction:
  - Both are intended to isolate one "network" or "compartment" from another.
- Firewall protects from general probes and many attacks.
FIREWALL POLICIES

- To **protect** private networks and individual devices from the **dangers** of the **Internet**
- To filter incoming or outgoing traffic based on a predefined set of rules called **firewall policies**
FIREWALL POLICIES: APPROACHES

- Two approaches to creating firewall policies
- Blacklist approach (default-allow)
  - All packets are allowed except those that satisfy rules defined specifically in a blacklist
  - **Pros:** Flexible in ensuring that service to the internal network is not disrupted by the firewall
  - **Cons:** Unexpected forms of malicious traffic could go through
- Whitelisted approach (default-deny)
  - Packets are dropped or rejected unless they are specifically allowed by the firewall
  - **Pros:** A safer approach to defining a firewall ruleset
  - **Cons:** Must consider all possible legitimate traffic in rulesets
FIREWALLS

- Firewall types based on system
  - Network
  - Personal
NETWORK FIREWALLS

Internet

25 80 445

25 80

Slide title 40 pt
Slide subtitle 24 pt
Text 24 pt

5 20 pt
PERSONAL FIREWALLS

- Run on the computer of the user
- Could provide filtering capabilities like network firewalls
- Distinguish between computer programs
FIREWALLS

- Firewall types based on protocol level
  - Network level
  - Transport level
  - Application level
NETWORK LEVEL FIREWALLS

- Filter on IP header fields
  - Source IP address
  - Destination IP address
  - Type of transport protocol
TRANSPORT LEVEL FIREWALLS

- Filter additionally on TCP header fields
  - Source port
  - Destination port
  - Flags (SYN, ACK)
APPLICATION LEVEL FIREWALLS

- Inspect contents of packets
- May filter certain websites
- Firewall may accept only trusted connections
- Logging of accepted connections is easy
- Performance may be problematic
- Since this type of firewall is quite complex, it may become a security risk itself
FIREWALLS

- Firewall types based on state knowledge
  - Stateless
  - Stateful
STATELESS FIREWALLS

- Treat each packet in isolation
- Has no memory of previous packets
- For each packet, check firewall rules again
- Easy to implement
- Very efficient

Issue: Can not easily handle protocols that use random ports
  - For instance, FTP
<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>allow</td>
<td>{our-host}</td>
<td>*</td>
<td>*</td>
<td>25</td>
<td></td>
<td>Our packets to their SMTP port</td>
</tr>
<tr>
<td>allow</td>
<td>*</td>
<td>25</td>
<td>*</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>deny</td>
<td>{ATTACK}</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
<td>Deny traffic from this address</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>allow</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>&gt;1024</td>
<td></td>
<td>Traffic to non servers</td>
</tr>
</tbody>
</table>
STATEFUL FIREWALLS

- Can tell when packets are part of legitimate sessions originating from a trusted network
- Maintain tables containing
  - Active connections
    - IP addresses
    - Ports
    - Sequence numbers
- Using these tables, stateful firewalls can allow only inbound TCP packets that are in response to the internal network initiated connections
STATEFUL FIREWALLS

- IF (packet belongs to an existing “association”)
- THEN {accept packet}
- ELSE {check firewall rules;
- IF (packet may pass)
- THEN {store “association” in state table}
- ELSE {discard packet}}

- Time-out inactive connections
- Connections may send “keep alive”
STATEFUL FIREWALLS

- Associations may be
  - TCP connections
  - UDP flows
  - ICMP request/response pairs

- Stateful firewalls can, for example, be configured to
  - Allow “associations” initiated by internal systems
  - Deny “associations” initiated by external systems

- Stateful firewalls can easily deal with protocols such as FTP
LOCATIONS OF FIREWALLS

- Internet
- Mail
- WEB
- DMZ
- Critical systems
FIREWALLS VS NAT

- NAT modifies IPs while firewalls do not
- In general, NATs do not inspect application data
- NATs can be compared to transport level firewalls
- Like certain firewall configurations, certain types of NATs accept incoming data only after an external “connection” has been established
FIREWALL AND NAT TOOLS

▪ For *nix users (for both firewall and NAT)
  – iptables
VIRTUALBOX

- A hypervisor

- It can be installed on a number of host operating systems including
  - Linux, OS X, Windows, Solaris, and OpenSolaris

- It supports creation and management of guest virtual machines running versions and derivations of
  - Windows, Linux, BSD, OS/2, Solaris, and others

- Download from: https://www.virtualbox.org
SUMMARY

- Firewall blocks unauthorised network access

- Firewall is not a standalone solution
  - Combined with anti-virus software and IDS

- Firewalls are effective only if configured correctly

- Use several different firewall configurations to protect a network
RESOURCES

- Read Chapter 11 of *Network Security Essentials – Applications and Standards* Fourth Edition
  William Stallings
  Prentice Hall
Questions?

Thanks for your attention!