Firewall

Ge Zhang

What is Firewall?

- **Design goals**
  - All traffic from inside to outside and vice versa must pass through the firewall
  - A single checking point that filters unauthorized traffic (i.e., scanning)

Services by a firewall

- **Service control**
- **Direction control**
- **User Control (internal network)**
- **Behavior control (the firewall needs to know the application protocol)**
- **Logging flow information**
- **Hidden internal topology**

Capabilities and limitations

- **Capabilities**
  - Prevent unauthorized traffics
  - Monitoring security-related events
  - The platform for Network address translator (NAT)
  - The platform for IPSec tunnel mode
- **Limitations**
  - Attacks the bypass the firewall (over other channels)
  - Internal threats (internal employees cooperate with external attackers)
  - Prevent transferring virus-infected programs

Types of firewalls

- **Packet-Filtering router**
- **Application-level gateway**
- **Circuit-level gateway**

Packet-Filtering router (1)

- **Packet-Filtering Firewall**
  - Applies a set of rules
  - Decides forwarding or discarding the packet
  - Only examine the *header*, do not “see inside” a packet
Packet-Filtering router (2)

<table>
<thead>
<tr>
<th>source</th>
<th>destination</th>
<th>protocol</th>
<th>dest. port</th>
<th>action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ane_home</td>
<td>Ane_work</td>
<td>any</td>
<td>any</td>
<td>Allow</td>
</tr>
<tr>
<td>any</td>
<td>SIP proxy</td>
<td>Tcp, udp</td>
<td>5060, 5061</td>
<td>Allow</td>
</tr>
<tr>
<td>any</td>
<td>Mail server</td>
<td>Tcp, udp</td>
<td>25</td>
<td>Allow</td>
</tr>
<tr>
<td>any</td>
<td>Web server</td>
<td>tcp</td>
<td>80, 8080</td>
<td>Allow</td>
</tr>
<tr>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Requirements on rule set design

- **Consistency**: The rules are ordered correctly
- **Completeness**: every packet satisfies at least one rule in the firewall
- **Compactness**: firewall has no redundant rules

An example

- **Consistency error**
- **Compactness error**
- **Completeness error**

Improvement

<table>
<thead>
<tr>
<th>Interface</th>
<th>source</th>
<th>destination</th>
<th>protocol</th>
<th>dest. port</th>
<th>action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>any</td>
<td>Web server</td>
<td>tcp</td>
<td>80</td>
<td>Allow</td>
</tr>
<tr>
<td>0</td>
<td>any</td>
<td>Web server</td>
<td>any</td>
<td>any</td>
<td>Deny</td>
</tr>
<tr>
<td>0</td>
<td>malicious</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Deny</td>
</tr>
<tr>
<td>1</td>
<td>host</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Allow</td>
</tr>
<tr>
<td>1</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Efficiency of rule set

<table>
<thead>
<tr>
<th>source</th>
<th>destination</th>
<th>protocol</th>
<th>dest. port</th>
<th>action</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.163.0.1</td>
<td>any</td>
<td>tcp</td>
<td>80, 8080</td>
<td>Deny</td>
</tr>
<tr>
<td>192.163.0.2</td>
<td>any</td>
<td>tcp</td>
<td>80, 8080</td>
<td>Deny</td>
</tr>
<tr>
<td>192.163.0.3</td>
<td>any</td>
<td>tcp</td>
<td>80, 8080</td>
<td>Deny</td>
</tr>
<tr>
<td>10.1.1.2</td>
<td>any</td>
<td>tcp</td>
<td>80, 8080</td>
<td>Allow</td>
</tr>
<tr>
<td>10.1.1.3</td>
<td>any</td>
<td>tcp</td>
<td>80, 8080</td>
<td>Allow</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>source</th>
<th>destination</th>
<th>protocol</th>
<th>dest. port</th>
<th>action</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.163.0.*</td>
<td>any</td>
<td>tcp</td>
<td>80, 8080</td>
<td>Deny</td>
</tr>
<tr>
<td>10.1.1.*</td>
<td>any</td>
<td>tcp</td>
<td>80, 8080</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Stateful PF

- **For TCP connections**
  - Server ports are mostly fixed (<1024)
  - Client ports are dynamically used (from 1024 to 65535)
- **Stateful**: tightens up the rules for TCP traffic by creating a directory of outbound TCP connections

<table>
<thead>
<tr>
<th>src</th>
<th>Src port</th>
<th>des</th>
<th>Des port</th>
<th>state</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.100</td>
<td>1030</td>
<td>210.9.88.29</td>
<td>80</td>
<td>established</td>
</tr>
<tr>
<td>192.168.1.102</td>
<td>3331</td>
<td>216.32.1.122</td>
<td>25</td>
<td>established</td>
</tr>
</tbody>
</table>
**Pro and cons in PF**

- **Pro:**
  - Simple, high efficient
  - Transparent to users

- **Con:**
  - Does not work with application-specific vulnerabilities
  - Limited log information
  - No user authentication
  - Difficulty to configure rulesets

**Attacks on a PF**

- **IP address spoofing:** (use spoofed IP address which can be trusted)
- **Fragment attacks**
  - Tiny fragment
  - Overlapping fragment

**IP fragment**

- A firewall only inspects the first fragmented one.

**Tiny fragment attack**

**Overlapping fragment**

**Application-level Gateway (mainly for inbound requests)**

- Have more checking parameters (user names, message format, client software version, etc)
- Only deal with allowable applications
- More useful log information
- Con: high processing overhead
Circuit level gateway (mainly for outbound requests)
- Based on connections instead of packets
- Similar to stateful PF
- Perform authentication
- Implementations: Socks server

Bastion Host
- A secure version of its operating system
- A platform for an application-level gateway or circuit-level gateway
- Only support allowed applications
- Only support a subset of the standard applications
- Needs additional authentication

Demilitarized Zone (DMZ)
- **Demilitarized zone** is a subnet that contains and exposes an organization's public services to an external network
- DNS, web server, VoIP server
- Internal network, workstations

Setup Firewalls in a network
- Screened host firewall (single-homes bastion)
- Screened host firewall (dual-homed bastion)
- Screened subnet firewall
<table>
<thead>
<tr>
<th>Practical experiences on firewall itself</th>
<th>Key points</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Stealth rule</strong>: drop any packet from outside to the firewall</td>
<td>• Types of firewall</td>
</tr>
<tr>
<td>• <strong>Insecure firewall management</strong>: drop packets to the firewall over insecure protocols (telnet, ftp, x11)</td>
<td>• Pros and cons of the three types</td>
</tr>
<tr>
<td>• <strong>Limited management machines</strong>: firewalls should be managed from a small number of machines</td>
<td>• Ruleset of PF (consistency, completeness, compactness, efficiency)</td>
</tr>
<tr>
<td></td>
<td>• Stateful PF</td>
</tr>
<tr>
<td></td>
<td>• Attack on PF</td>
</tr>
<tr>
<td></td>
<td>• Bastion host</td>
</tr>
<tr>
<td></td>
<td>• DMZ</td>
</tr>
<tr>
<td></td>
<td>• Setup firewalls in a network</td>
</tr>
</tbody>
</table>