Firewalls

Security threats and network

- As we have already discussed, many serious security threats come from the networks;
- The firewalls implement hardware or software solutions based on the control of network connections between local network and other networks.

Hardware firewall

Software firewall
Layers in network connections (OSI model)

![Layers in network connections (OSI model)](image)

Firewalls work at these layers

Messages in OSI model

![Messages in OSI model](image)

Firewall characteristics

- All traffic from inside to outside, and vice versa, must pass through the firewall. All access to the local network is blocked except via firewall.
- Only authorized traffic, defined by the local security policy is allowed to pass in either direction.
- The firewall itself can not be penetrated.

Types of control used by firewalls

- **Service control**: determines what types of services can be accessed;
- **Direction control**: determines in which direction particular service request may be initiated;
- **User control**: determines access to a service according to a user;
- **Behaviour control**: controls how particular services are used.
Limitations of the firewalls

• Cannot protect against attacks that bypass the firewall.

• Does not protect against internal threats.

• Cannot protect, in general, against transfer of virus-infected programs or files.

Types of firewalls

• **Packet filtering router** (works at the network layer, IP)

• **Circuit-level gateway** (works at the transport layer, TCP)

• **Application-level gateway** (works at higher layers)

Packet-filtering router

A packet-filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet.

Filtering is based on information contained in a network packet.

Filtering rules

Filtering rules are based on

• **Source IP address**

• **Destination IP address**

• **Source and Destination transport-level address**: transport level port number

• **IP protocol field**: defines the transport protocol
Default policies

One may apply rules following two different default policies:

- **Discard**: that which is not explicitly permitted is prohibited.
  - More conservative. At the beginning everything is forbidden. Then permitting rules must be added on a case-by-case basis.

- **Forward**: that which is not explicitly prohibited is permitted
  - More convenient to use, but less secure. Once security threat is recognized, specific forbidding rule(s) must be added

Packet-filtering examples

**(Default=discard)**

<table>
<thead>
<tr>
<th>action</th>
<th>src</th>
<th>dest</th>
<th>port</th>
<th>protocol</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>*</td>
<td></td>
<td>25</td>
<td>SMTP</td>
<td>*</td>
</tr>
<tr>
<td>Allow</td>
<td>*</td>
<td>*</td>
<td></td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>action</th>
<th>src</th>
<th>dest</th>
<th>port</th>
<th>protocol</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>*</td>
<td>*</td>
<td>25</td>
<td>SMTP</td>
<td>*</td>
</tr>
</tbody>
</table>

Pros and cons of packet filtering

**Pros:**

- Simple;
- Transparent for users;
- Very fast.

**Cons:**

- Lack of upper-layer functionality;
- Do not support advanced user authentication schemes;
- Cannot block specific application commands: either the application is disallowed, or all its functions are permitted;

Circuit-level gateway

Outside host

Outside connection

Outside host

Inside connection

Inside host

(c) Circuit-level gateway
Circuit-level gateways

- Traffic is filtered based on specified session rules, like:
  - a session is initiated by a recognized computer;
- A circuit-level gateway sets up two connections:
  - One between itself and a TCP user on the inner host;
  - One between itself and a TCP user on the outer host;
- Once connections are established and security criteria are met, both connections are linked by the gateway;

Pros and cons of circuit-level gateways

Pros:
- Circuit-level gateways are relatively inexpensive;
- have the advantage of hiding information about the private network they protect.

Cons:
- do not filter individual packets.

Application-level gateway

Application layer gateways (proxies)

- They can filter packets at the application layer of the OSI model.
- Incoming or outgoing packets cannot access services for which there is no proxy:
  - for example, an application level gateway that is configured to be a web proxy will not allow any ftp, telnet or other traffic through.
- They can filter application specific commands such as http:post and get, etc.
Pros and Cons of Application-Level Gateways

- **Pros:**
  - They offer a high level of security;
  - Application specific protection;

- **Cons**
  - significant impact on network performance;
  - are not transparent to end users; and
  - require manual configuration of each client computer.

Firewalls: benefits and problems

**Benefits:**
- firewalls protect private local area networks from hostile intrusion from the Internet;
- flexibility in implementation of security policies;
- relatively inexpensive solution.

**Possible problems:**
- Possible traffic bottleneck;
- Security concentrated in one spot;