



openHPI – Internet Security Excursion: Firewalls

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

Firewalls

Firewalls are security systems that protect a single computer or network from **unwanted network accesses**

- Monitor incoming and outgoing connections and the network traffic
- Can prevent unauthorized connection attempts
- Provide additional protection against attacks such as
 - Attacks by backdoors and botnets
 - Each of these attacks requires a connection from/to the attacker, which must be created without an authorization
 - Such attacks can be prevented or an alarm can be triggered

Firewall – Rules (1/2)

Firewall rules define the circumstances in which certain connections or network traffic is permitted or disallowed

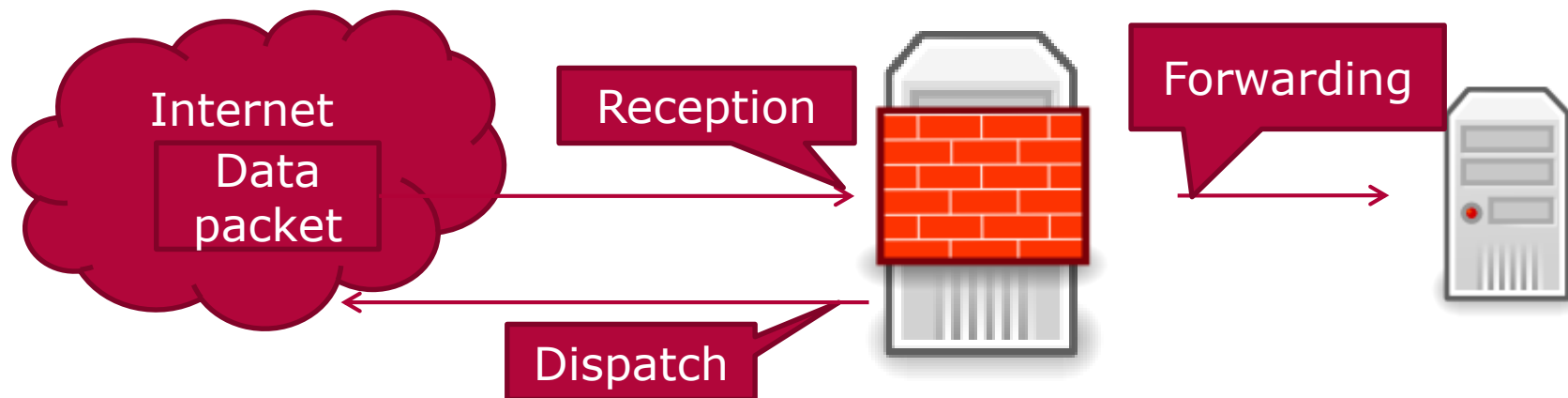
- Rules can be formulated specifically for individual protocols, ports, destination and source addresses or programs
- A check is made to see if a rule fits and needs to be applied for each incoming and outgoing network packet
- If a rule applies to a network packet, various actions can be performed
 - Package can be allowed, redirected, modified, discarded or blocked, a warning can be displayed, ...
- Defining the rules requires knowledge of the computer's connections
- Incorrect definitions can block valid connections

Firewall – Rules (2/2)

- In the case of missing definitions or unsuitable rules, the **general policy** of the system is applied
 - Security guidelines dictate whether other connections are blocked or allowed, or whether a user's confirmation is required
- Firewalls can store all explicitly permitted connections and automatically set the rules for them
- **Local firewall** only implements the defined firewall rules for the computer on which it is installed
- **Network firewall** checks all network traffic and is typically installed on the connection node between a local network and the Internet

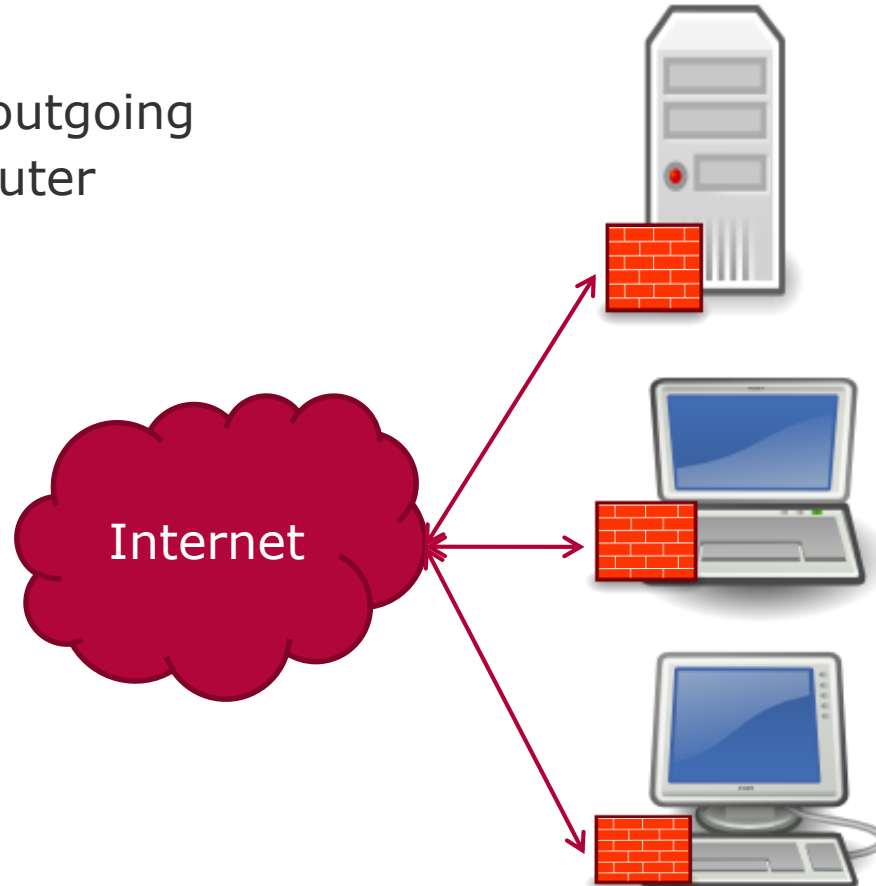
Firewall – Stages

- Rules can be applied at different stages of the packet processing
- When defining the rules, the stage in which the rule applies is specified, e.g.
 - when receiving, dispatching, forwarding, before routing, ...
- Defined actions are executed at the respective stages



Local Firewalls

- **Local firewall** acts only on the system on which it is installed
- Checks all incoming and outgoing connections on this computer
- Allows system-specific fine-granular settings
 - Warnings and packet blocking apply only to the respective system



Network-Based Firewalls

- **Network firewall** checks all incoming and outgoing network traffic and is typically installed on the connection node between a local network and the Internet
- Connections within the network are not checked, unless the firewall acts as a central connection node
- Settings affect all clients in the network
- Administration of firewall rules for the local network is simplified

