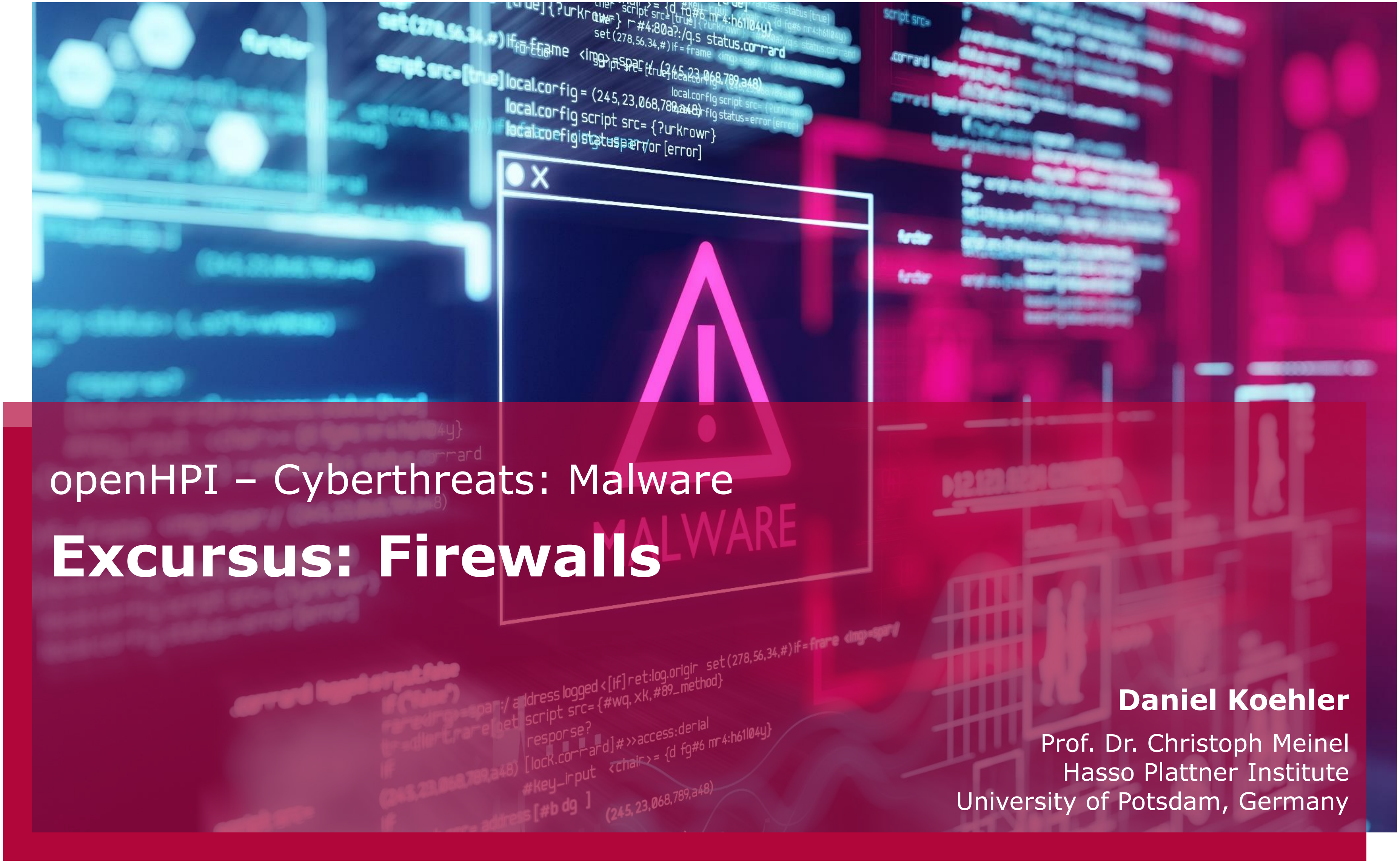


openHPI – Cyberthreats: Malware

Excursus: Firewalls

Daniel Koehler

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

Firewalls

Firewalls are security measures / systems that **protect** individual computer or full networks from **unwanted network traffic**

- Monitoring of incoming and outgoing connections
- Can deny / block unauthorized connections
- Improved security against attacks, e.g
  - Attacks by **botnets** or **backdoors**
    - Attacks need connection to / from attacker in advance
    - Such connections can then be blocked, or alarms can be raised

Firewall Rules (1/3)

Firewall-Rules define, which connections / what network traffic is allowed or not allowed

- Rules can be specific to…
  - Protocols
  - Ports
  - Clients
  - Sources
  - Destinations
  - … or a combination of the above

Firewall Rules (2/3)

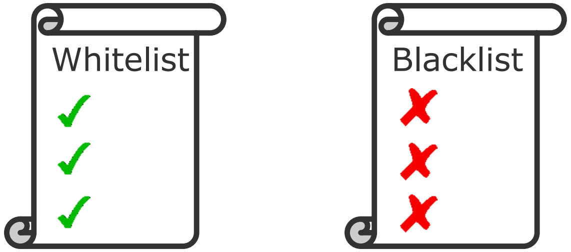
Firewall-Rules define, which connections / what network traffic is allowed or not allowed

- Whenever a network packet matches a rule, it can be decided what to do with the packet:
  - **Accept**
  - **Aeject / Deny**
  - Forward
  - Monitor
  - Modify
  - ...

Firewall Rules (3/3)

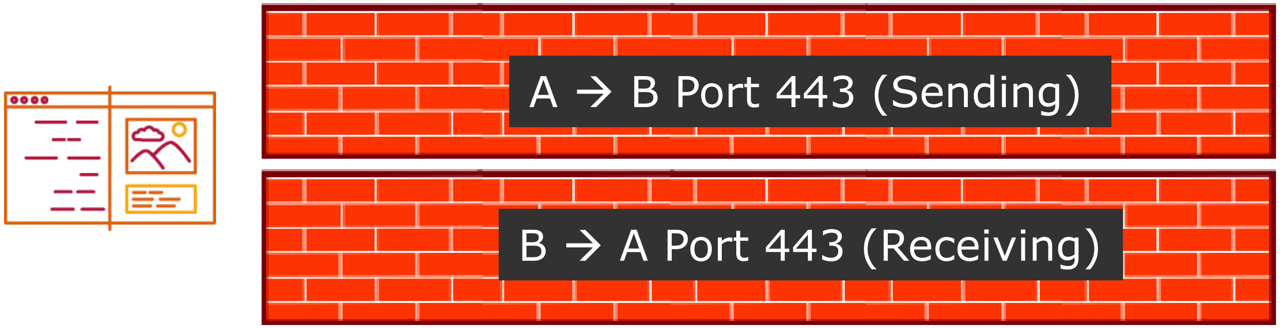
If no other Firewall rules are applicable, packages will be treated based on the **Standard Policy**.

- **Whitelist**: Allowed connections are listed explicitly, everything else will be rejected
- **Blacklist:** Disallowed connections are listed explicitly, everything else will be accepted.



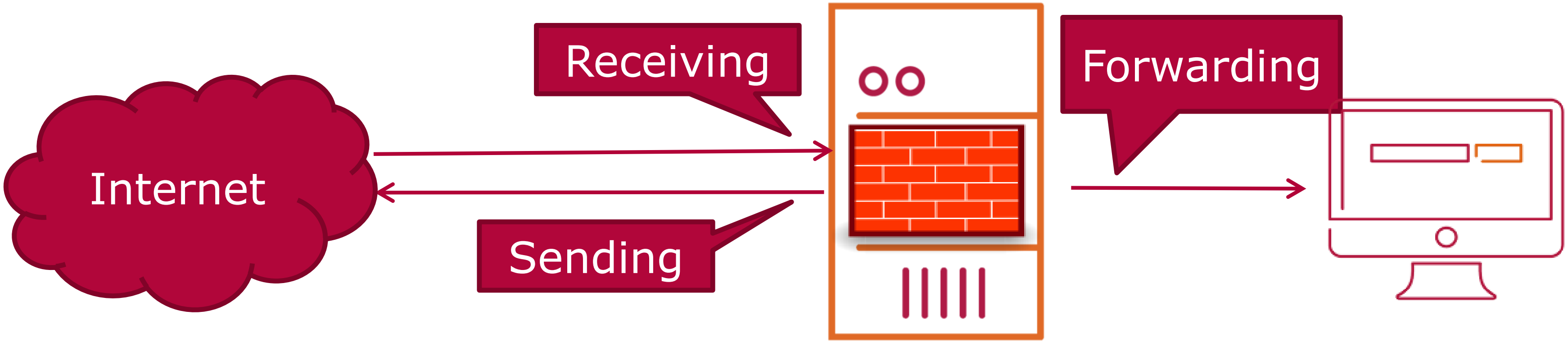
Firewall – States (1/2)

- **Rules** can be applied at different stages of the packet processing
- In the definition of the rule, the state of the connection has to be defined



A → B Port 443 (Sending)

B → A Port 443 (Receiving)



Receiving

Forwarding

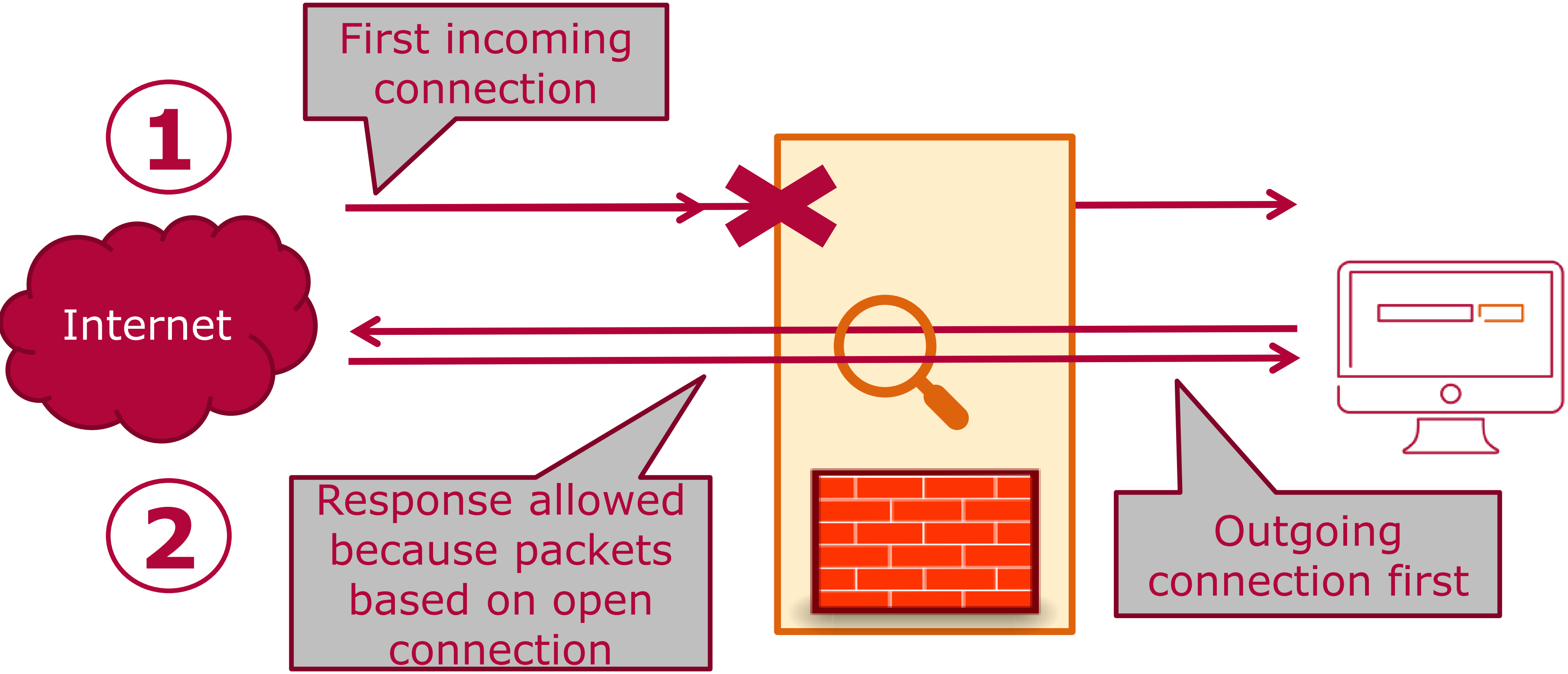
Internet

Sending

Firewall – States (2/2)

Stateful packet inspection

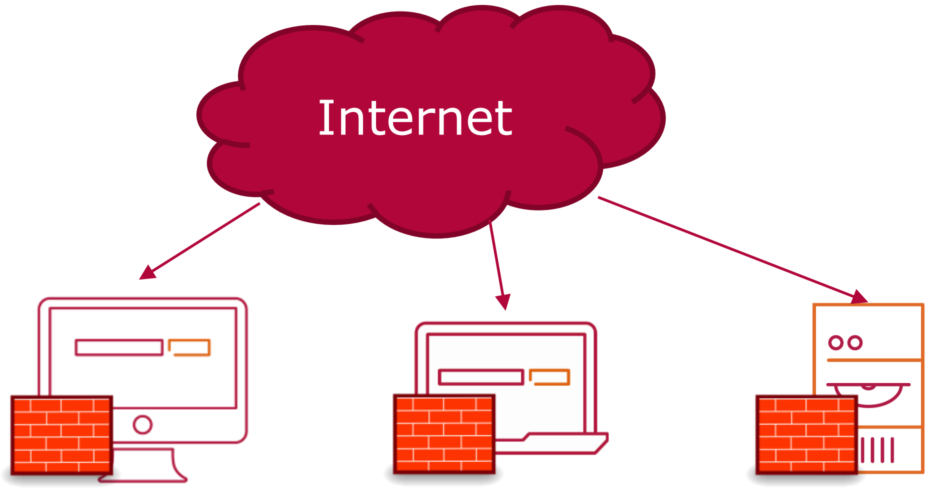
- **Rules** can be dependent of the state of the connection
- In general, this configuration is easier and more secure


First incoming connection
1
Internet
2
Response allowed because packets based on open connection
Outgoing connection first

Local Firewalls

Local Firewalls run only on the System on which they are installed

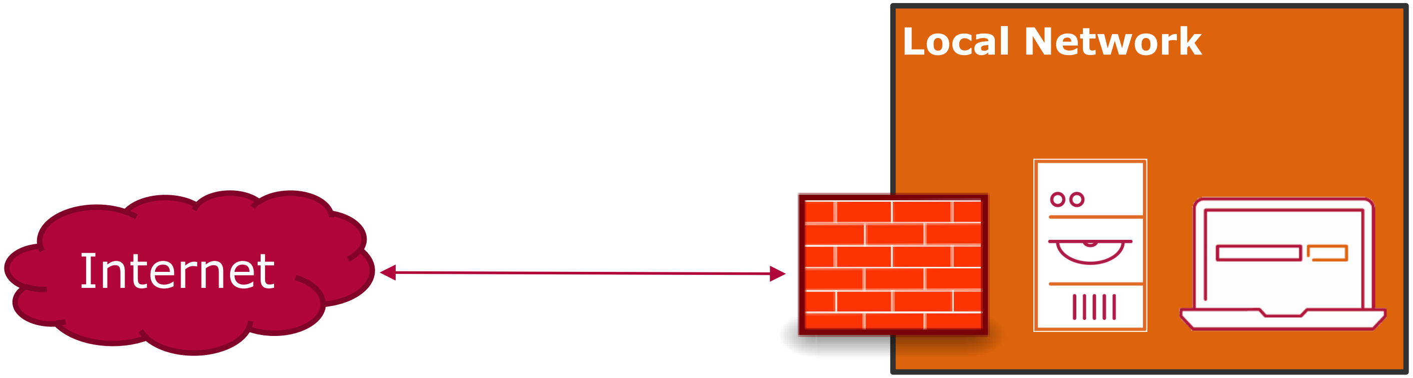
- Monitors all incoming and outgoing connections of the device at hand
- Possibility for system-specific detailed setting



Network-Based Firewalls

Network-Based Firewalls monitor all connections going through the network.

- Typically installed on central network-components such as the Gateway (connection to the Internet)
- Can also be installed on internal network components to monitor internal connections
- Settings „aplly" to all Network-Devices
- Security of each individual device simplified


Local Network
Internet