**IS ZA Firewalls**

Firewall => device that sits between two or more networks to control the **packet flow** between them

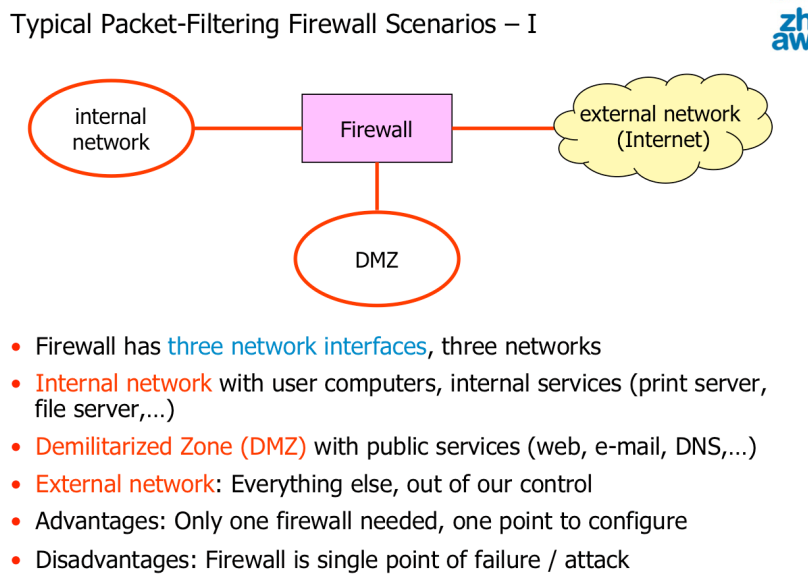
* Basis for usage => security policy => human-readable description
* Based on security policy => one or more firewalls are installed and configured
* Operating at the network layer
* Inspect headers of network and transport layer protocols

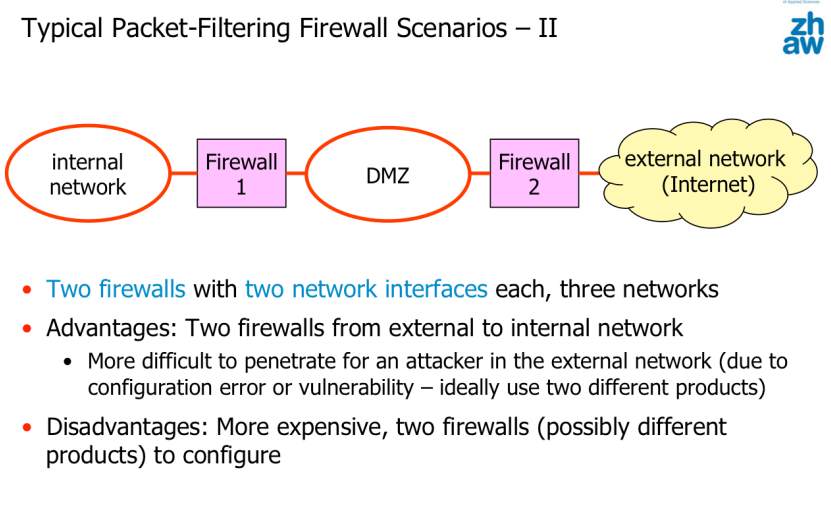
Firewall capabilities:

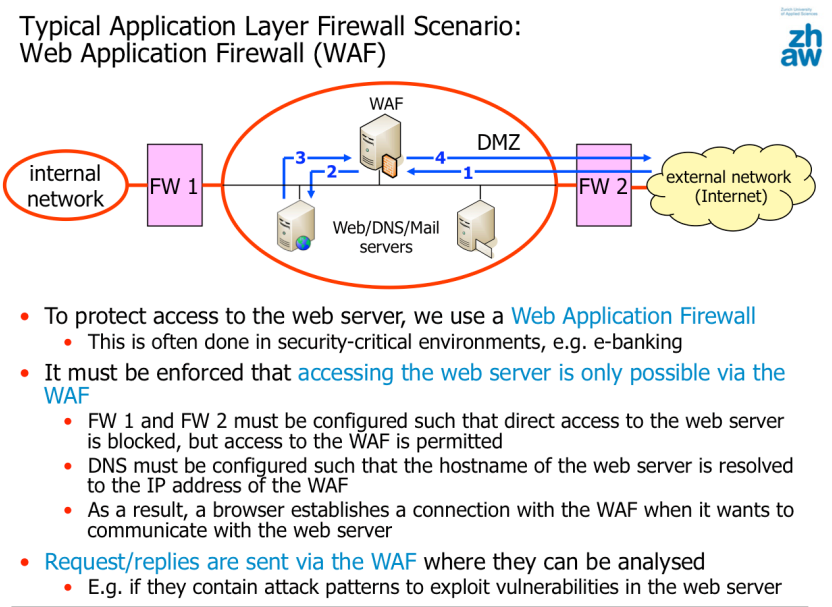
* **Control access from the internal** (company) network to the Internet
  + E.g allow only access to web and FTP servers
* **Control access from the internet** to internal computers and services
  + E.g only to web server (port 80, 443) and SMTP server
* Block malicious incoming web traffic

Firewall Types :

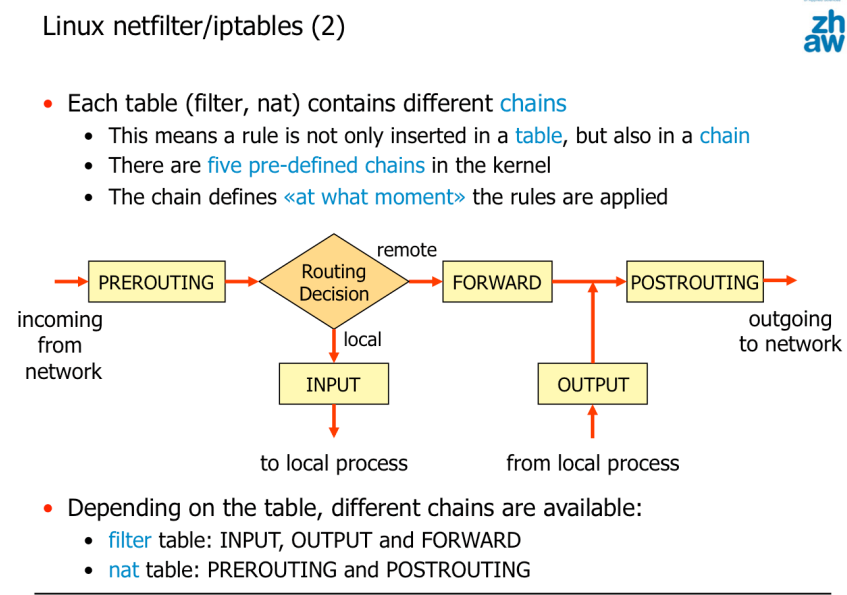
* **Packet-Filtering Firewalls:** 
  + Advantages:
    - **Very fast** => only have to check layer 3 and 4 protocol headers
  + Limitations:
    - Control only “**who is allowed to talk to whom**”, but they do not control the content that is exchanged
  + Basically “**extended routers**”
    - Must have also routing capabilities
* **Application Layer Firewalls** (**Proxy** Firewalls)
  + **Inspect application layer data** according to rules and => if the data is legitimate => relay it between client and server
  + Advantage
    - **Allows deep inspection of all data exchanged**
  + Limitation:
    - **Relatively slow**
      * Limitations with encrypted data
      * Can usually not handle many different application layer protocols
      * But are optimized for one type of application

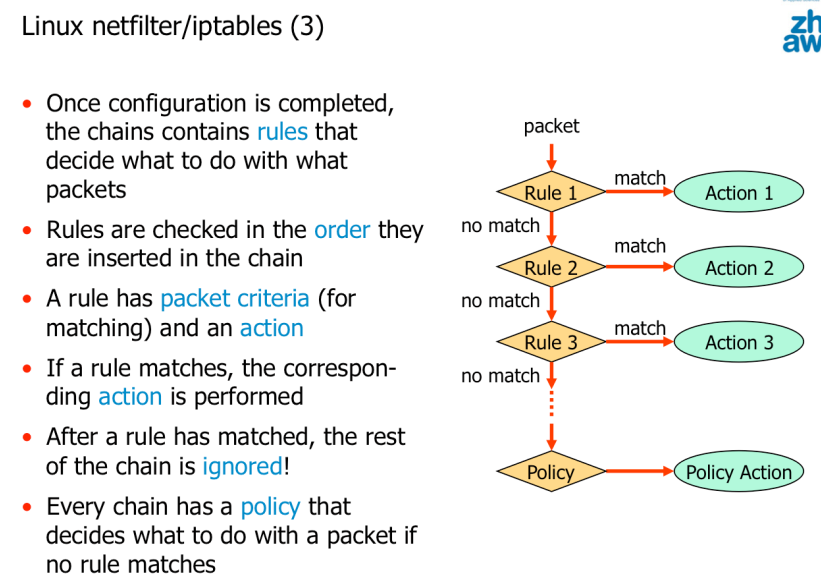


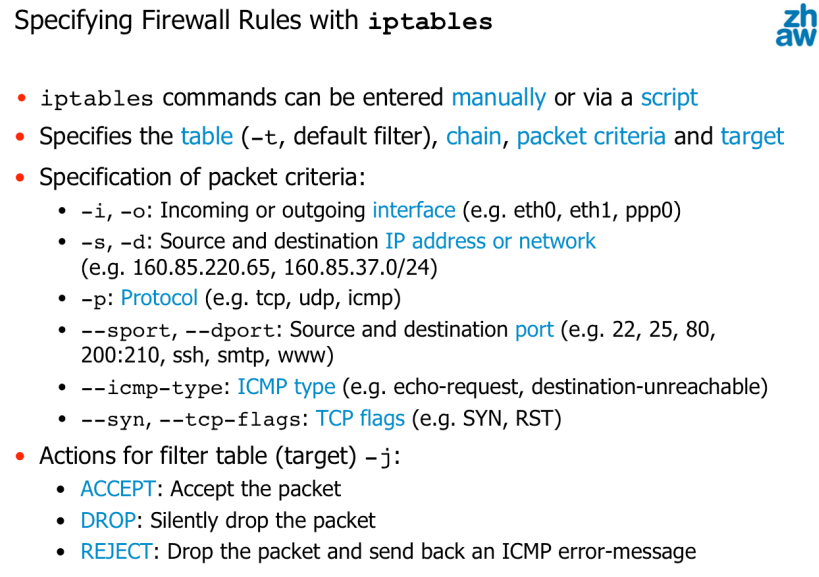


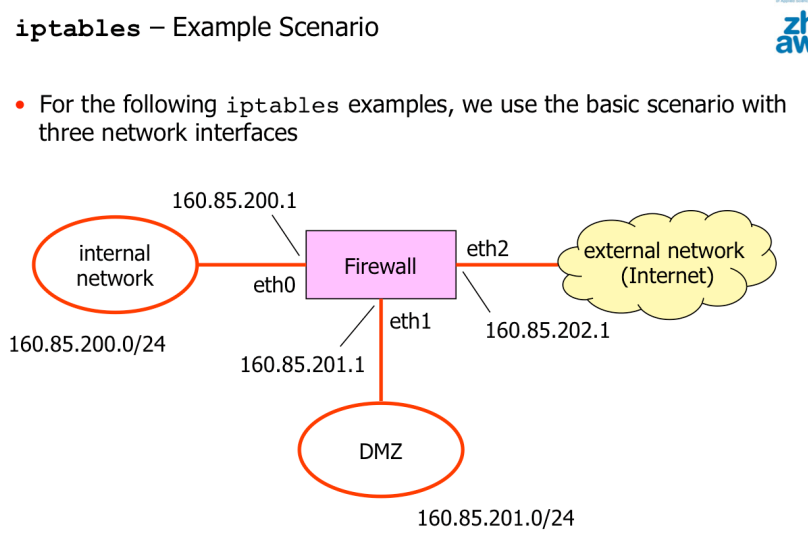


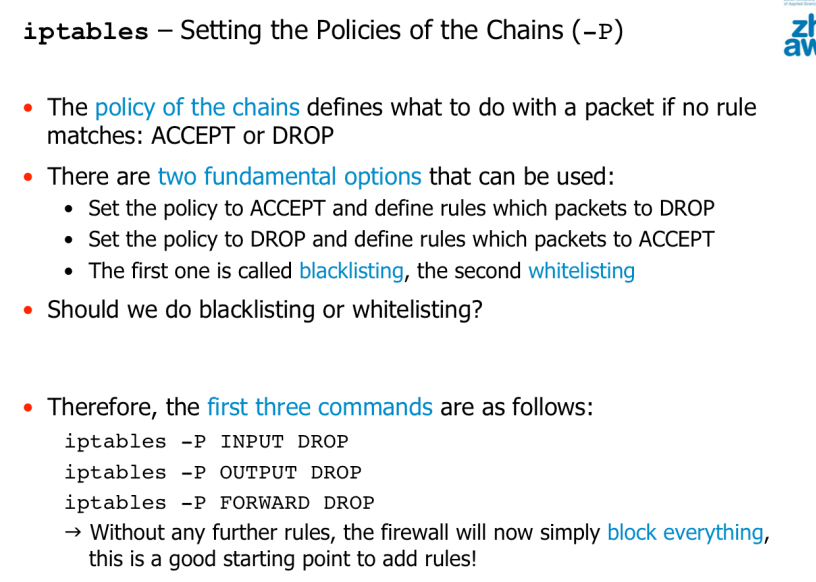
Linux netfilter => mechanism that allows to access the packets in the network stack to analyze, modify, extract and delete theme











**Firewalls should be configured to deny everything by default and only allow through what is needed**

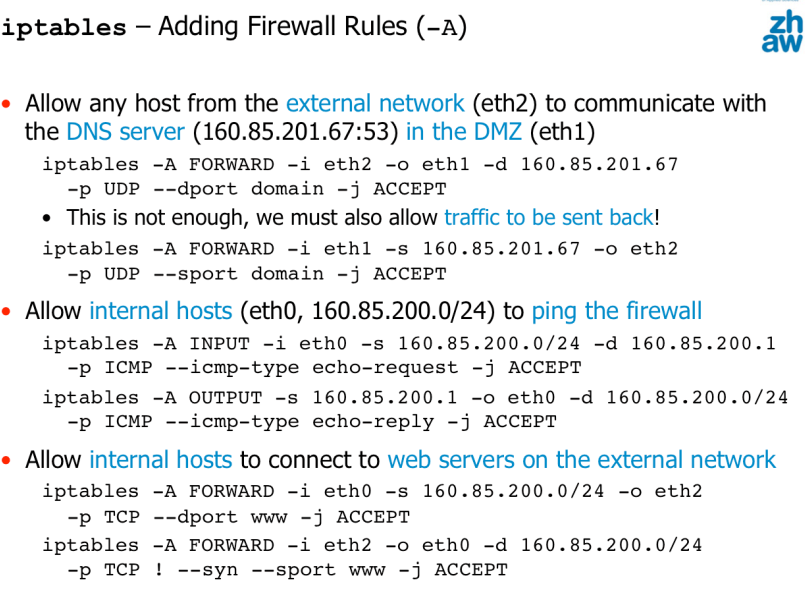
* Minimises the probability that unwanted traffic is accidentally allowed.

**Flushing (emptying) a/all chain(s), should be done before adding the firewall rules**

* iptables -F [chain]

Listing the rules (of a chain)

* iptables -L [chain]



**Including the network interface is crucial! => otherwise external network attacks are possible** => e.g gain access to the firewall

* avoid that hosts on the external network to be able to ping the firewall

**Stateless Firewalls**

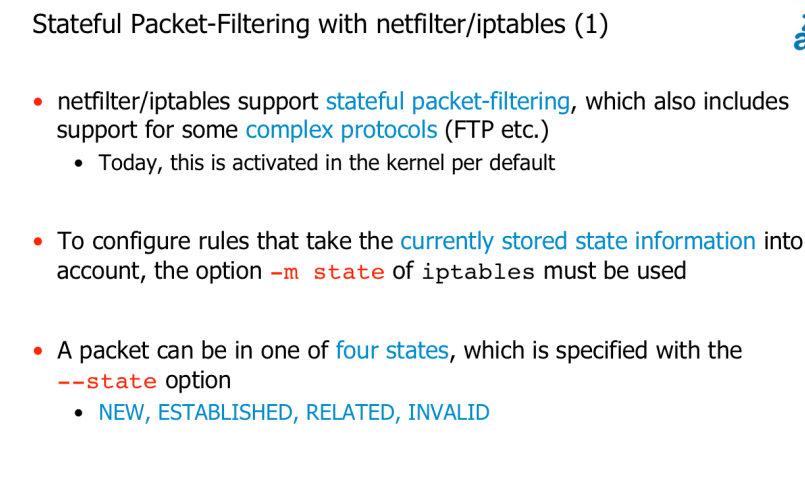
* **always configure a rule for both directions**

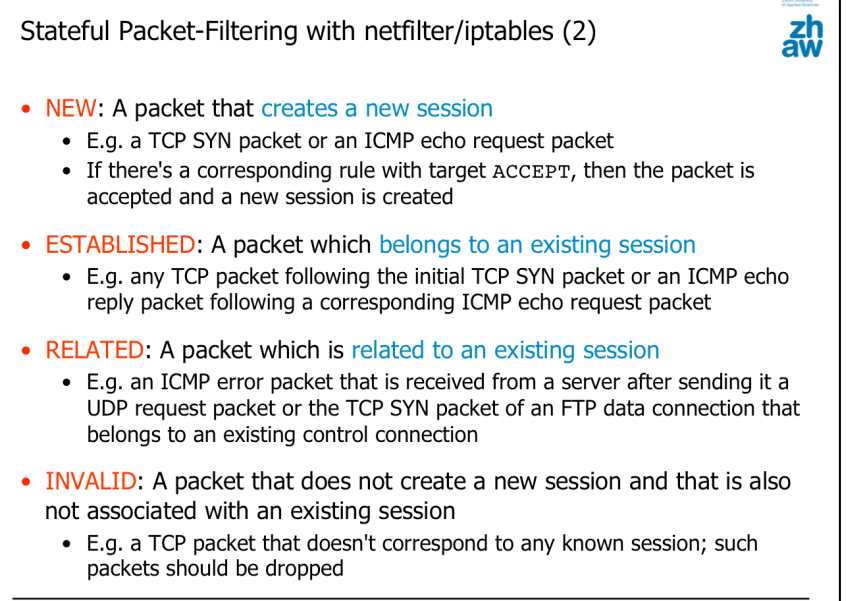
Stateless packet-filtering firewalls have additional limitations

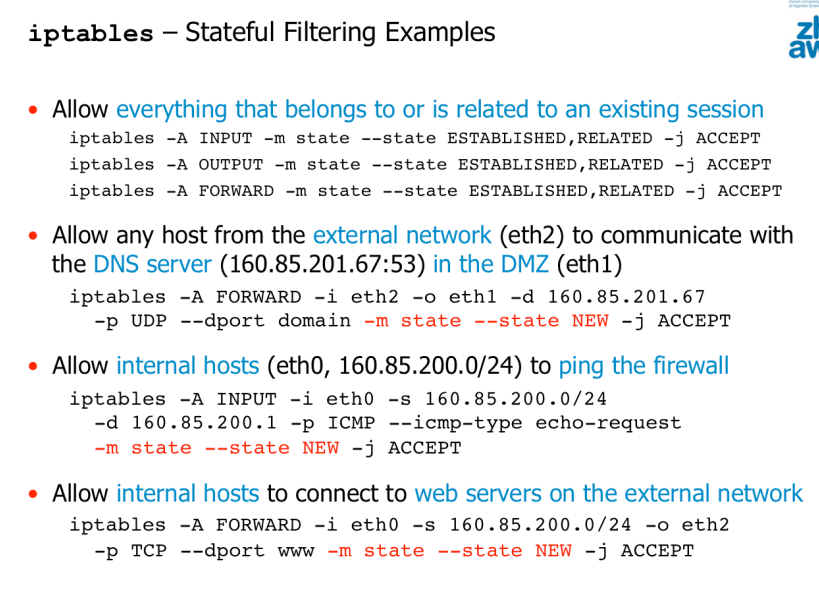
* Firewalls are more open than needed: Replies from a server are allowed without a previous request from a client
* **Limited support for complex protocols (FTP, multimedia protocols) where a control connections opens additional data connections**

**Stateful packet-filtering firewalls**

* Firewall not only checks individual packets, but tracks communication relationships (sessions) and maintains state information
* Typical state information: protocol, source/destination IP addresses, ports, session duration, protocol phase (TCP)
  + TCP sessions are easy to track: from SYN to FIN
  + There are no UDP/ICMP sessions!! But requests/replies can be associated (IP addresses, ports with UDP),
    - Timeout to remove state information
* **Significant advantages:** 
  + **Easier to configure** 
    - fewer rules needed
  + **Return traffic is only allowed on demand** 
    - No static rules for return traffic
    - Return traffic holes must not be always kept on but are closed per default
  + **Allows supporting compley protocols such as FTP**
    - The firewall monitors the FTP control connection and when it sees a Port command, it dynamically opens exactly that port

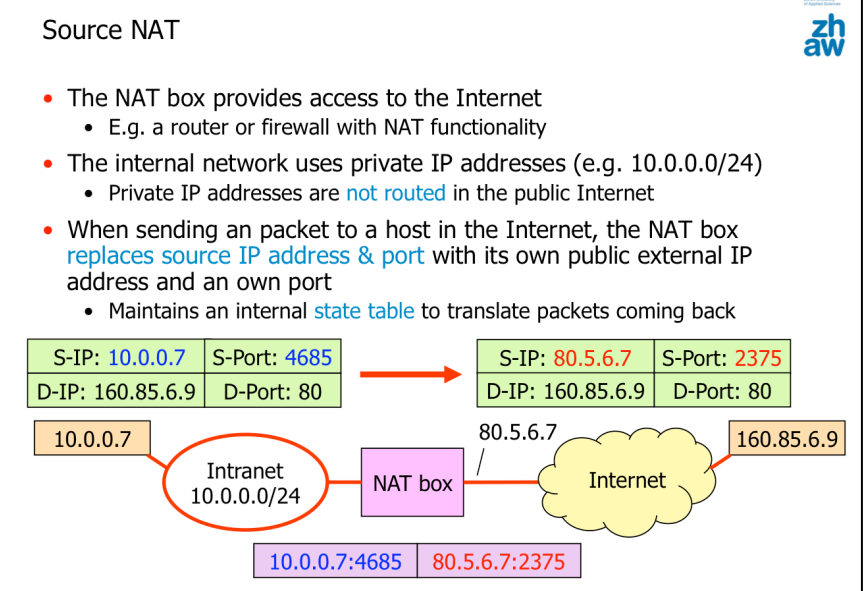


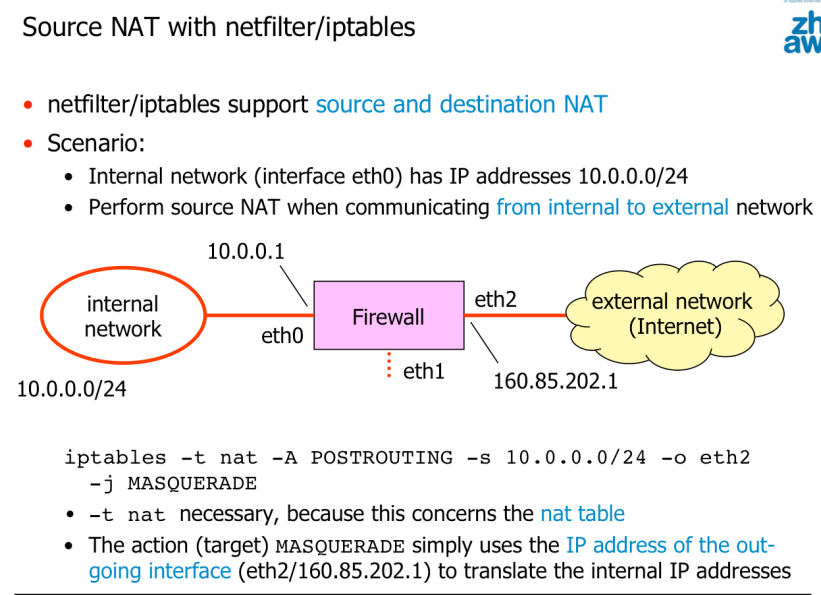




**NAT (Network Address Translation)**

* Source or destination addresses of packets are rewritten as they travel through a NAT-enabled router or a firewall
* Allows to access the internet with several host while having only one public IP address
* Traditionally used to save IP addresses
* Hides internal network structure from the outside
* Prevents internal hosts/services from being accessed from the outside

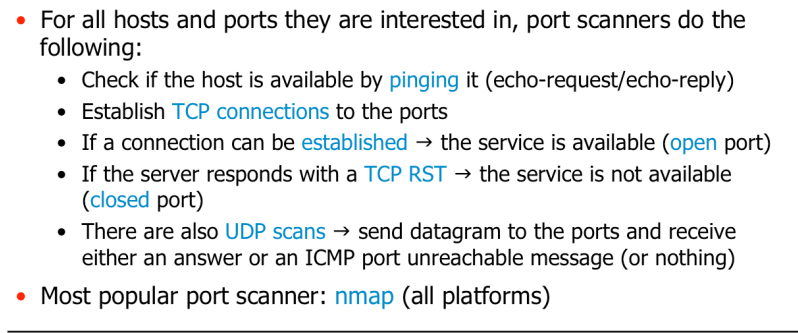


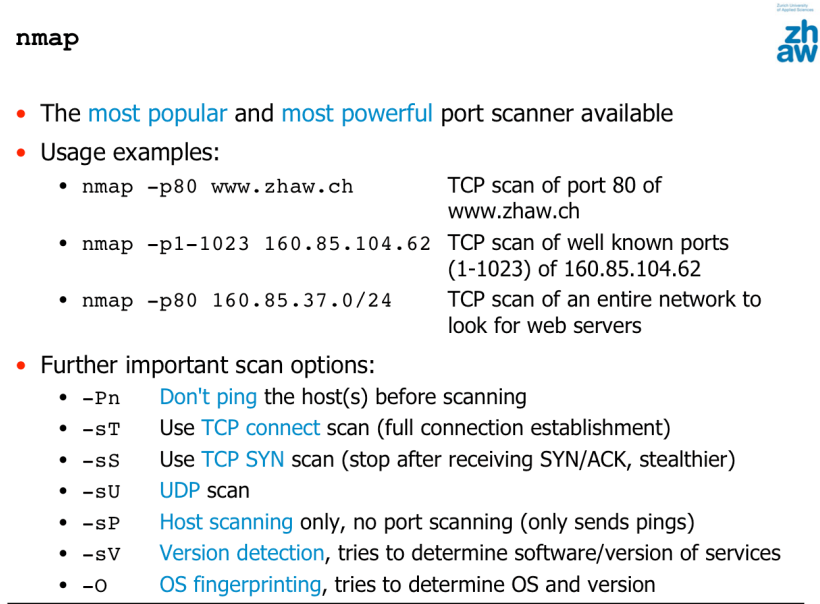


**Packet-filtering firewalls don’t protect from attacks on the application layer**

Port scanning

* **Technique to determine the services that run on a host**





**Firewalls (quiet ones => silently dropping packets) make port scanning much more difficult**