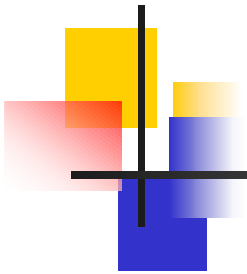
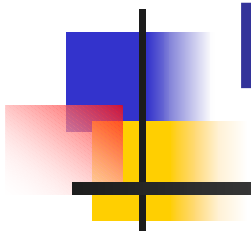
Agenda of today's lecture



- **Firewalls in General**
- Hardware Firewalls
- Software Firewalls
- Building a Firewall

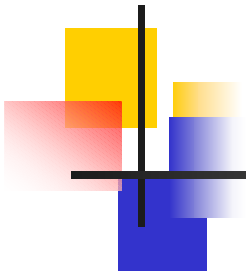


Firewalls in General

S-38.153 Security of Communication Protocols

Antti Lehtonen

29.4.2003

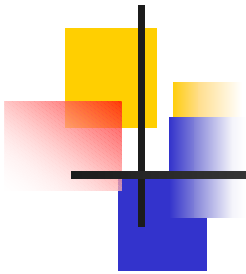


firewalls

- systems designed to prevent unauthorised access to or from a private network
- data security gateway
- usually between local network and Internet
- hardware or sotfware or combination of both
- transparent to the users

why do we need firewalls?

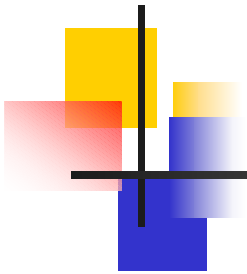
- protection of
  - information/knowledge
    - secrecy, integrity, accessibility
  - resources
    - servers, computers
  - reputation
    - identity, confidence, privacy
- against several kinds of attacks and threats



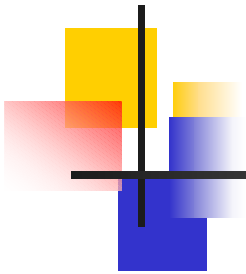
firewall types

- generally fall into two categories:
  - network-level firewalls ("packet-filtering" firewalls)
  - application-level firewalls ("proxy" firewalls)
- stateful vs. stateless inspection
  - state table of established connections in stateful solution
- there are also many other classifications

firewall techiques (1/4)

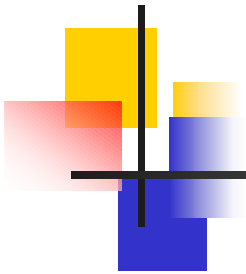


- packet filtering
  - filters IP packets based on IP addresses and port numbers
  - available in Linux (Netfilter) and in routers
  - usually compined with NAT (network address translation)
  - effective and easy to implement
    - can stop e.g. IP spoofing and DOS attacks
  - can be defeated by a number of tricks (for example with packet fragmentation)



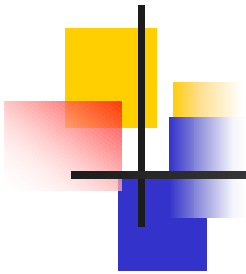
firewall techiques (2/4)

- circuit gateways
  - located at the OSI layer 5 (session layer)
  - reassembles and examines all packets in each TCP circuit
  - provides some added functionalities
    - VPN over the Internet by doing encryption from firewall to firewall
    - filtering of web sites or newsgroups
  - can’t protect against e.g. malicious code



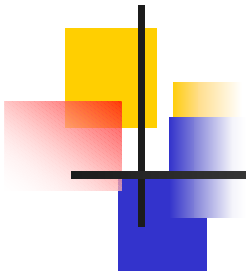
firewall techiques (3/4)

- application-level gateways
  - looks at the application level PDU (Protocol Data Unit)
  - acts as a proxy for specified services
    - proxy servers are application specific
  - all traffic goes through firewall proxy
    - direct communication between Internet and local network is not allowed
    - logging and examination of traffic



firewall techiques (4/4)

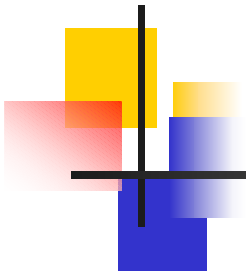
- can also be easily used as network address translators (NAT)
- slower and less flexible than packet filtering but also more secure
- virus check may be included
- users can not connect to the application but they must connect to the proxy
  - transparency?



security policies and firewalls (1/2)

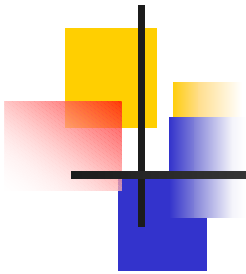
- before you can deploy a firewall you need to have network security policy
  - software vs. hardware
  - simple router vs. complex system
  - security vs. performance
  - own vs. service provider's
  - Forbid everything that is not allowed vs. Allow everything that is not forbidden

security policies and firewalls (2/2)



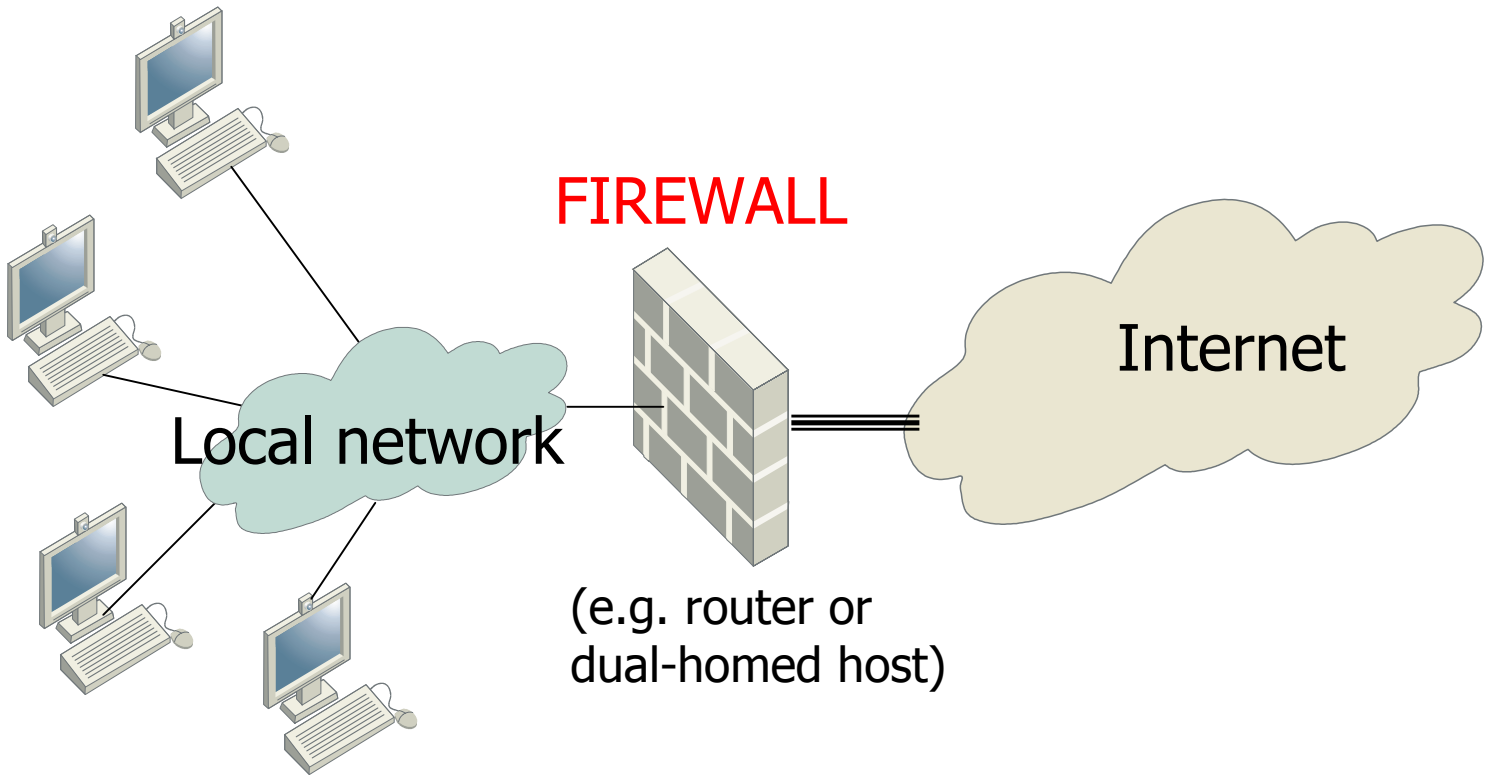
- firewall policy: allow/deny?
  - IP addresses, ports, MAC addresses, domains
- NAT and NAPT (network address and port translation) are basic methods provided by routing firewalls to the protected networks and they are relatively easy to deploy

DMZ (demilitarized zone)

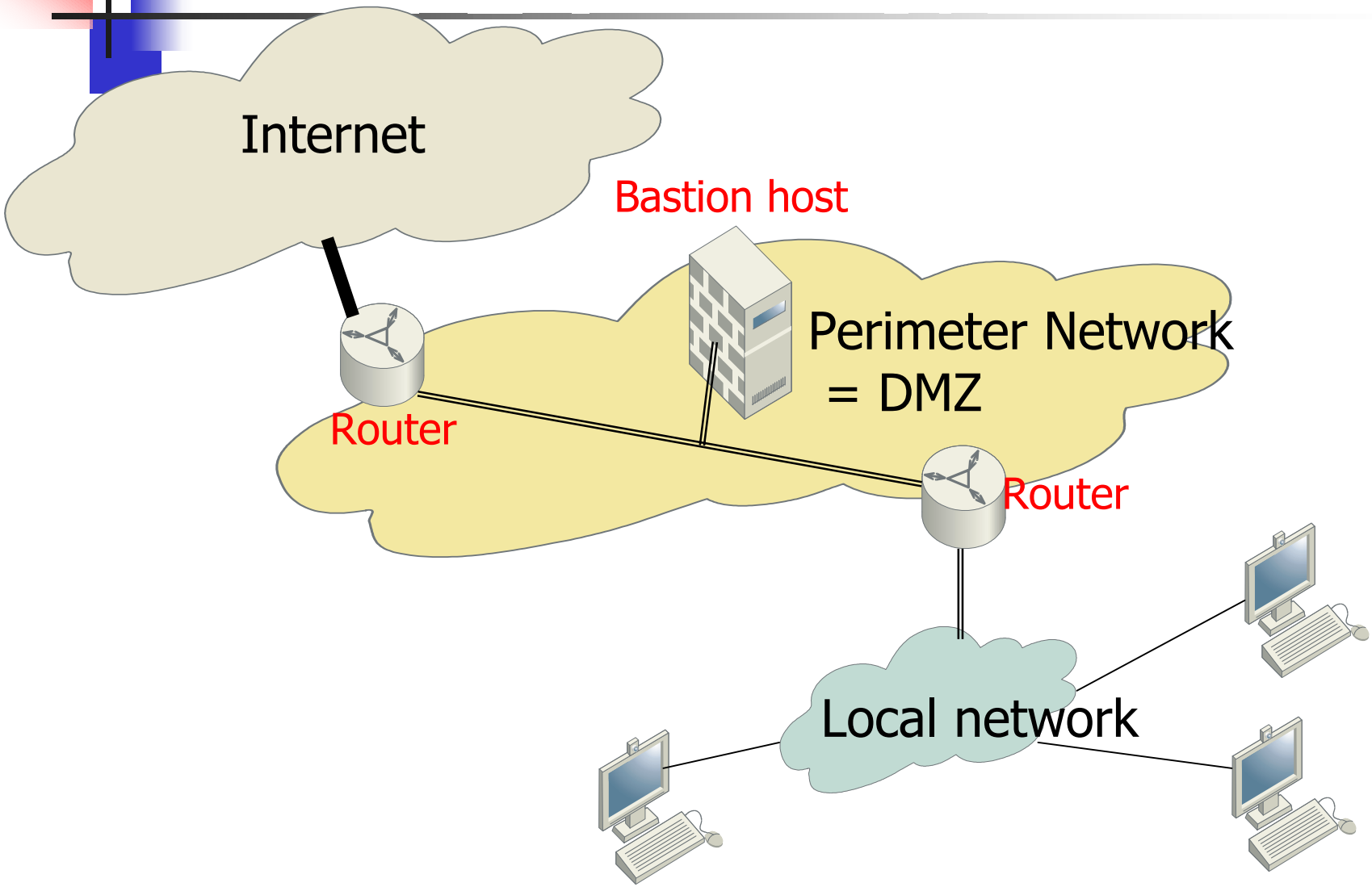


- part of the network that is neither part of the internal network nor directly part of the Internet
- can be between any two policy-enforcing components of your architecture
- breaking DMZ into several ”security zones” (having different networks within the DMZ)

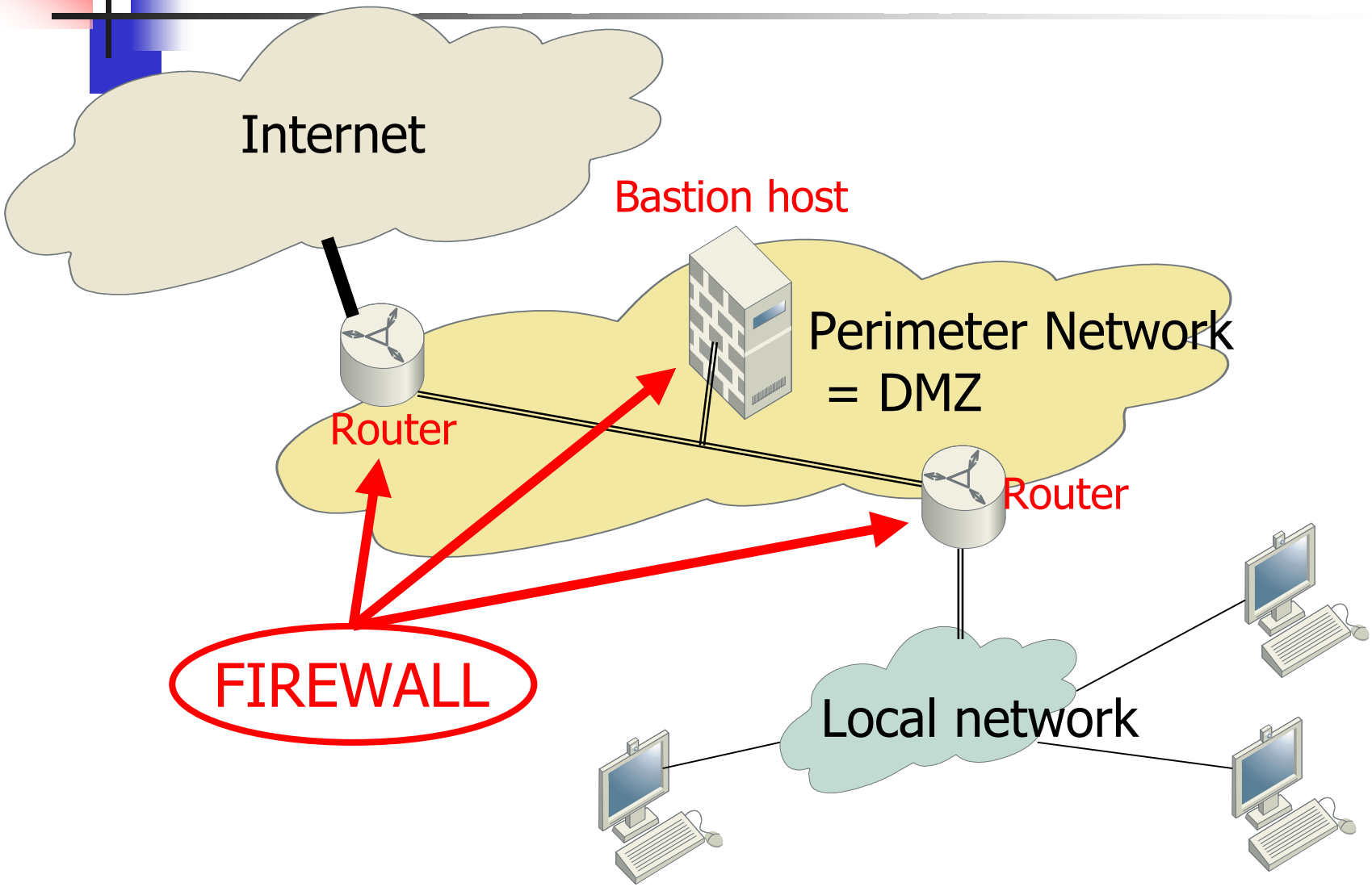
Example simple topology

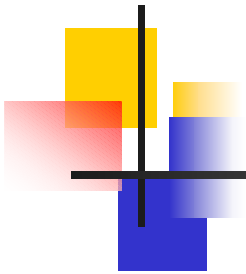


Example DMZ topology



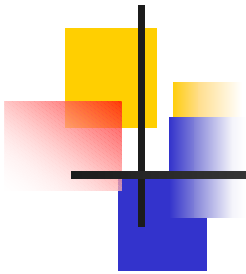
Example DMZ topology





with firewalls you can

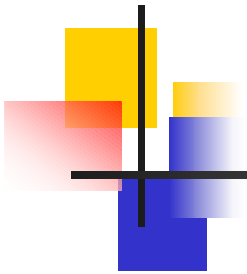
- concentrate network protection to one point (”choke point”)
- enforce the use of security policies
- logging and auditing of Internet traffic
- restrict the visibility of your network topology (NAT, network address translation)
- perform access control



firewalls cannot protect against

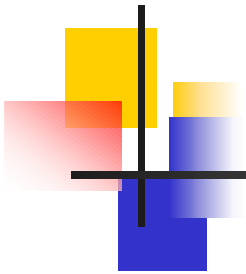
- malicious people inside
- connections that do not go through the firewall
- viruses
- data-driven attacks (something is mailed or copied to an internal host where it is then executed)
- new or unknown threats

other weaknesses



- configuration can be quite complex: ”The firewall is only as good as its configuration”
- needs active, skillful and up to date administration and control
- may prevent users to access some services they might need
- may give to an excessive feeling of safety

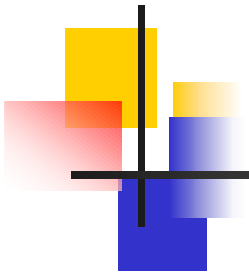
encryption vs. firewalls



- supports each others by solving different kinds of security problems
- one will not eliminate the need for the other

- IPSEC: integrity and privacy of the information flowing between hosts
- Firewall: what kinds of connectivity is allowed between different networks

Agenda of today's lecture



- Firewalls in general
- **Hardware firewalls**
- Software firewalls
- Building a firewall