Network Security

What would you like to protect?

- Your data
  - The information stored in your computer
- Your resources
  - The computers themselves
- Your reputation
  - You risk to be blamed for intrusions or cyber crime

Security aspects for your data

- Confidentiality
- Integrity
- Availability

When communicating the other party's identity must be verified = >

- Authentication

Authentication

- How do you know with whom you are communicating?

Integrity and Confidentiality

- How do you know that the information has not been modified and/or intercepted?

"Man in the middle"

Availability

- Attack against availability is called ″denial of service″
- Extremely difficult to be protected against

Example

- ″SYN-flooding″
- ″Ping of death″
- ″Mail bombing″

NETWORK INSECURITY

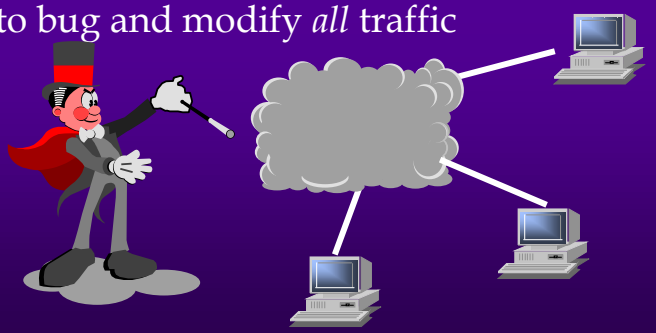
Network insecurity

Reasons for security problems in networks:

- Resource sharing
- Complexity, difficult to get an overview
- Difficult to define the boundary
- Several points of attack
- Anonymity
- Several routes between two nodes

Insecure Medium

- It is almost impossible to secure the network itself, i.e. the communication links
- You must always assume that attackers are able to bug and modify *all* traffic



Web-(in)security

Server-related risks

- The information is modified by un-authorized parties
- Internal information leaks out via the server
- The server is inaccessible
- The server is used for further intrusions

Client-related risks

- Trojan Horses (Java, PostScript etc)
- Viruses/Trojan horses in down-loaded programs and documents (macros)
- Tracing of habits
- The ”babbling” browser

FIREWALLS

Firewalls

- A firewall is an access control device between two networks.
- A firewall monitors all traffic (in both directions) and filters away (denies) unwanted traffic
- Thus it protects against attacks from outside

Firewalls

- The firewall determines which inside services may be accessed from outside and which outsiders that are allowed to access to those inside services.
- It determines which outside services may be accessed by insiders.

Firewall Capabilities and Limits

- capabilities:
  - defines a single choke point
  - provides a location for monitoring security events
  - convenient platform for some Internet functions such as NAT, usage monitoring, IPSEC VPNs
- limitations:
  - cannot protect against attacks bypassing firewall
  - may not protect fully against internal threats
  - improperly secure wireless LAN
  - laptop, PDA, portable storage device infected outside then used inside

Firewalls – basic functionality

A firewall implements an organization's security policy with respect to Internet

- The ***stance*** of a firewall describes the fundamental security philosophy of the organisation
- The ***default deny (discard)*** stance: everything is denied unless specifically permitted
- The ***default permit (forward)*** stance: everything is permitted unless specifically denied

Firewalls techniques

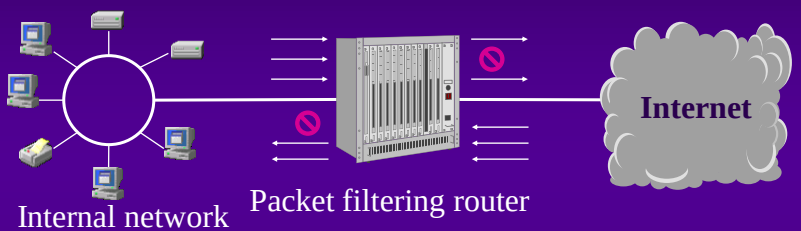
Basic principles:

- Packet filter
- Application-level gateway (proxy)
- Circuit-level gateway
- Stateful inspection (dynamic filtering)

Architectures:

- Packet filtering router
- Single-homed host
- Dual-homed host
- Demilitarized Zone (DMZ)

Firewalls, basic principles (and architecture): *Packet filter*



- Allows or denies a packet based on address, direction, port and protocol
- Does not understand the contents of the packet
- Advanced variation: dynamic filtering/stateful inspection

Packet Filter Rules

Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

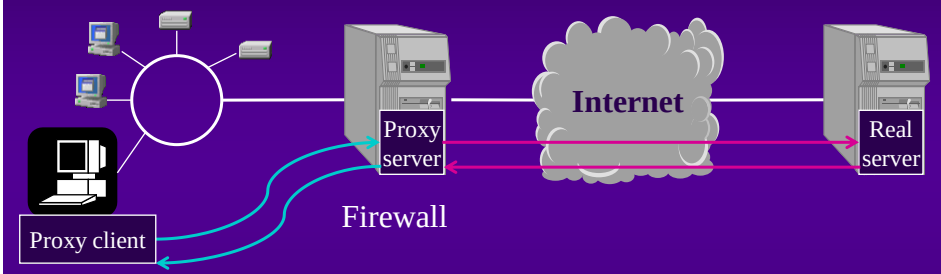
Rule Set D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Firewalls, basic principles: Application-level gateway (proxy)



- Offers transparent forwarding of services
- Connections terminate in the firewall
- Internal systems are not directly visible to the outside

Application-Level Gateway

- acts as a relay of application-level traffic
  - user contacts gateway with remote host name
  - authenticates themselves
  - gateway contacts application on remote host and relays TCP segments between server and user
- must have proxy code for each application
  - may restrict application features supported
- more secure than packet filters
- but have higher overheads

Circuit-level gateway

- A Circuit-level gateway sets up and relays 2 TCP connections, one to an internal host and one to an external host, without any further filtering
- Logically, it acts as a "wire". (Cp circuit-switched n/w)
- Can be implemented by an application-level gateway.
- Is often used for outgoing connections, where the internal user is trusted.

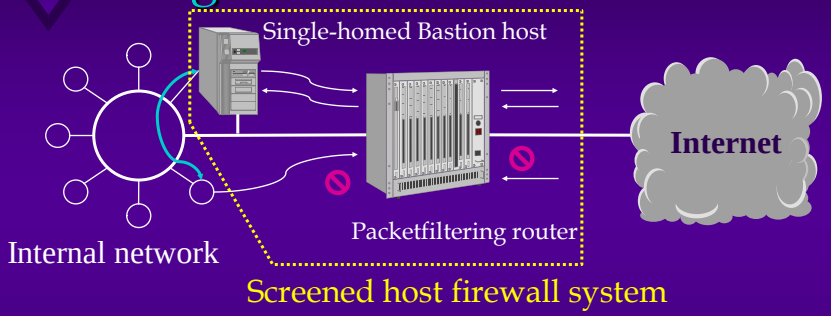
Host-Based Firewalls

- A software module used to secure an individual host
- available in (or as an add-on for) many O/S
- often located in servers
- advantages:
  - taylored filter rules for specific host needs
  - protection from both internal/external attacks
  - additional layer of protection to stand-alone firewall

Personal Firewall

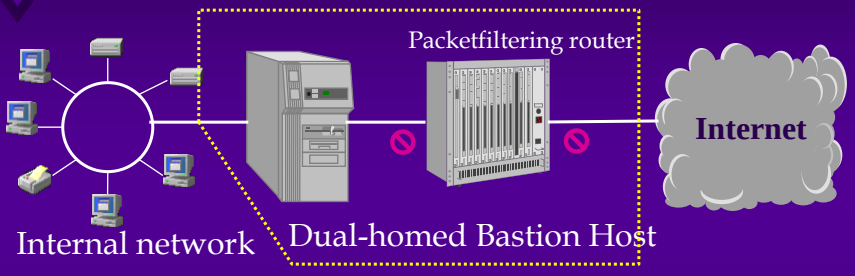
- controls traffic flow to and from a PC and external network (Internet)
- for both home or corporate use
- may be software module on PC
- typically much less complex
- primary role to deny unauthorized remote access to the PC
- may also monitor outgoing traffic to detect and block malware

Firewalls, architectures:
Single-Homed Bastion Host



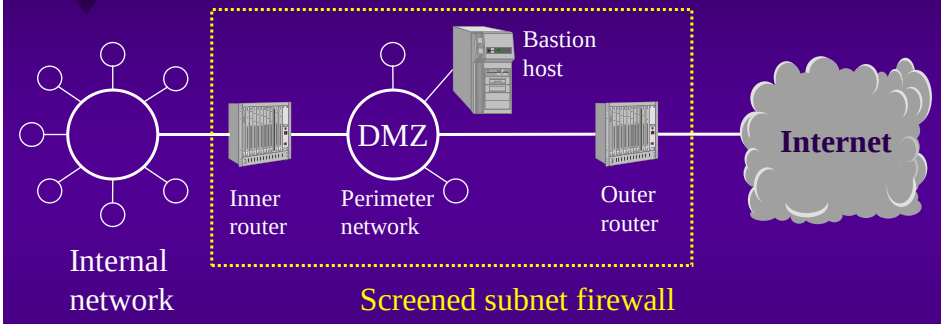
- The Bastion Host performs authentication and proxy functions
- The packet filter only accepts packets to/from Bastion Host

Firewalls, architectures:
Dual-homed Bastion Host



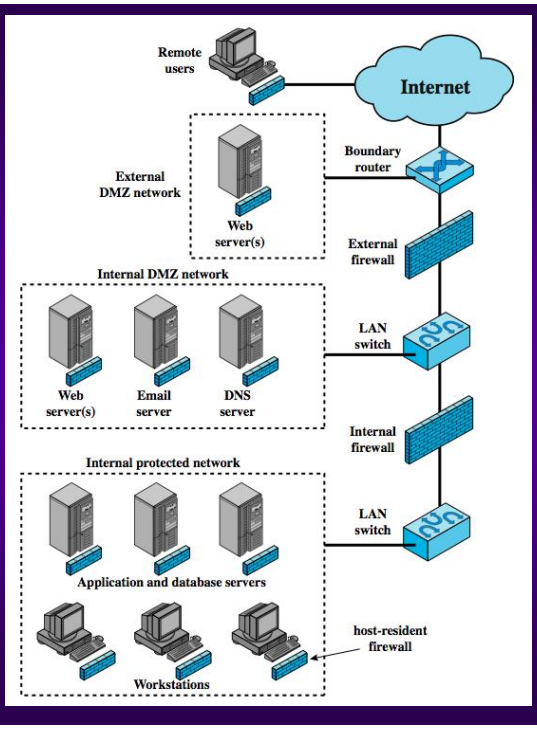
- A computer with two network interfaces
- Stops "pass-by" attacks, since the traffic must pass the Bastion Host

Firewalls, architectures:
Demilitarized Zone (DMZ)



- Web- and mail-servers etc are placed in DMZ
- Provides in-depth defence

Distributed Firewalls



Firewalls – functional limitations

- Protects only those connections that passes the firewall - is the firewall really the *only* connection to Internet?
- Does not protect against insiders
- Does not protect againts viruses
- Does not protect againts data-driven attacks
- Open for availability attacks
- Errors, weaknesses and deficient installations may impair functionality

Firewalls - problems

- Must be installed and adapted, which could be difficult
- Installation details may be important
- Must be maintained
- Difficult to test
- Affects the performance of the Internet connection?
- May be seen as a hindrance by the users

Virtual Private Networks