

The need for an information policy

- very important for an organisation to assess risks
 - develop a clear policy regarding information access and protection

- policy to specify who is granted access to which information
 - the rules an individual must follow in disseminating the information to others
 - a statement of how the organisation will react to violations

- may seem obvious many organisations attempt to make the network secure before deciding what security really means

- establishing an information policy is crucial as humans are usually the most susceptible point in any security scheme

An information policy

- employees should know the answers to some basic questions:
 - how important is information to your organisation?
 - what does copyright mean and what is your organisation's policy to photocopying and copying data onto floppy-disk?
 - how much of the information to which you have access to may you discuss with other employees?
 - do you or your organisation work with information belonging to other organisations?
 - what information may you import to the company?
 - may you use a personal computer at work to access any outside data?
 - what are intellectual property rights, and how do they affect what you do at work?

Answers to questions might be complex

- for example consider three organisations A, B and C
 - the policy at A allows information to travel to B but not C
 - the policy at B is to allow information to travel to C

- a problem!
 - although the end effect might compromise security no employee would be violating their organisations policy!

Firewalls and Internet access

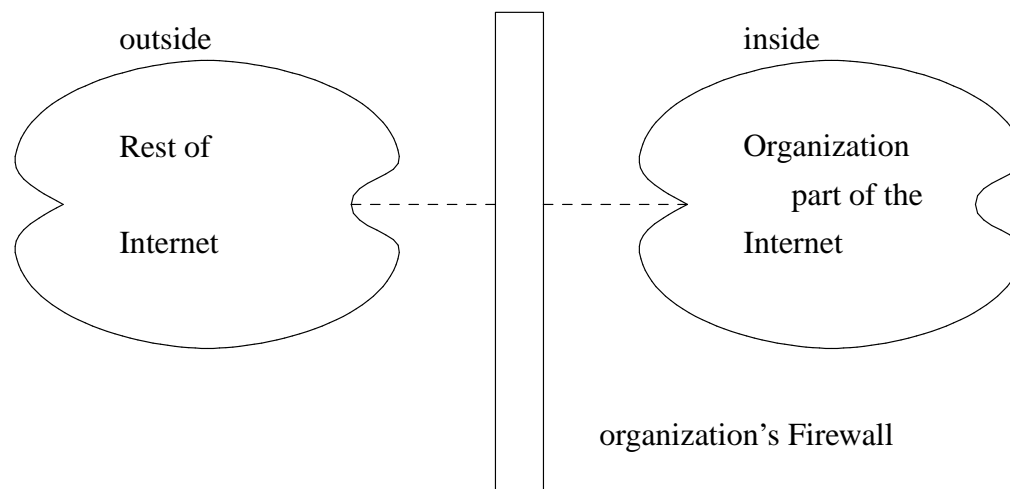
- having an organisation attached to the Internet can prevent security problems
 - may need to screen the network or organisation from unwanted communication

- need a mechanism to prevent outsiders from:
 - obtaining information,
 - changing information or disrupting information

- a single technique has emerged as the basis for Internet access control,
 - an Internet firewall

Firewall concept

- firewalls essentially control the entrance to a network from the global Internet
- partitions an Internet into two regions, the *inside* and *outside*



Firewalls

- an organisation that has multiple external connections
 - must install a firewall on each external connection
 - must coordinate all firewalls

- failure to restrict access identically on all firewalls can leave the organisation vulnerable

Simplest Firewall: Packet level filters

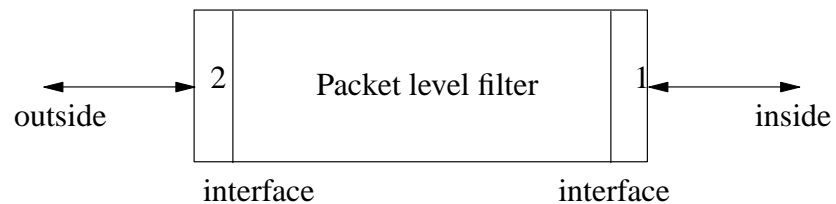
- can be as simple as one machine
 - two network cards
 - some protocol software

- throws away unwanted packets and passes wanted packets from one network card to another

- TCP/IP does not dictate a standard for packet filters
 - each vendor is free to choose the capabilities of their packet filter as well as the interface that the manager must operate

Packet level filter

- simple firewall
 - single machine with two interfaces
 - filters on IP datagram dest/src addresses
 - and TCP/UDP port numbers



Example firewall software configuration display

- default deny



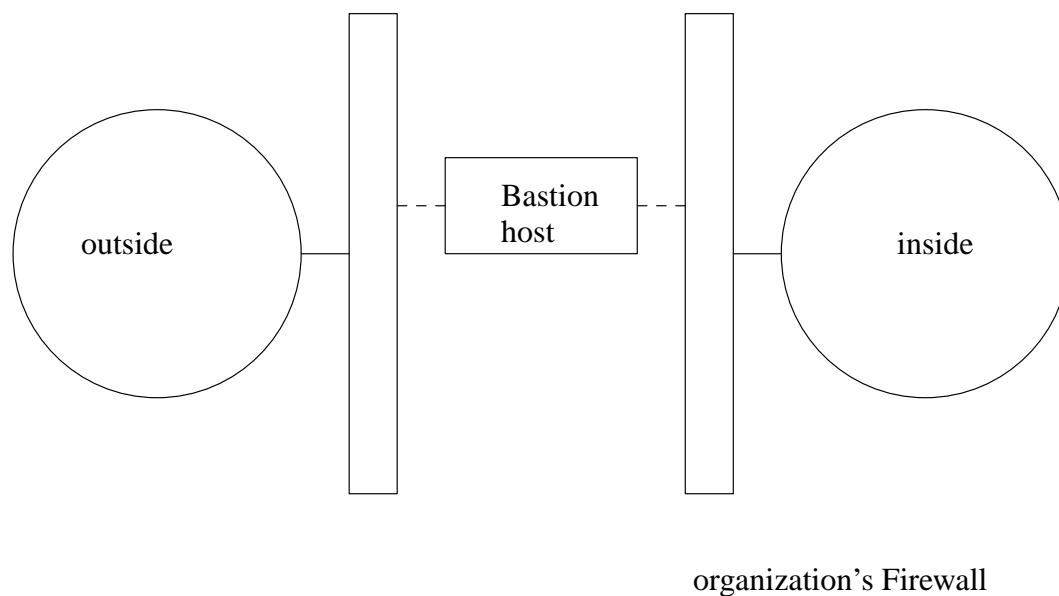
arrival i/f	ip src	ip dst	protocol	src port	dst port
2	*	*	tcp	*	22
2	*	*	tcp	*	25
1	128.5.*.*	*	tcp	*	22
1	128.5.*.*	*	tcp	*	80

- here the manager has chosen to block all packets
 - except those incoming datagrams (ssh = 22) and (smtp = 25)
 - allows access to external (http = 80) and (ssh = 22) from the inside

Accessing services through a firewall

- not all organisations want to use packet level filtering
 - perhaps employees on the inside need to have access to some of the services outside
- make one computer secure and assume that all the other computers in your organisation are insecure
- this one computer must be strongly fortified to serve as a secure communication channel and is termed a *bastion host*

Bastion hosts



- the outer barrier blocks all incoming traffic except:
 - datagrams destined for services on the bastion host that the organisation chooses to make available externally
 - datagrams destined for clients on the bastion host

Bastion hosts

- inner barrier blocks all incoming traffic except datagrams coming from the bastion host

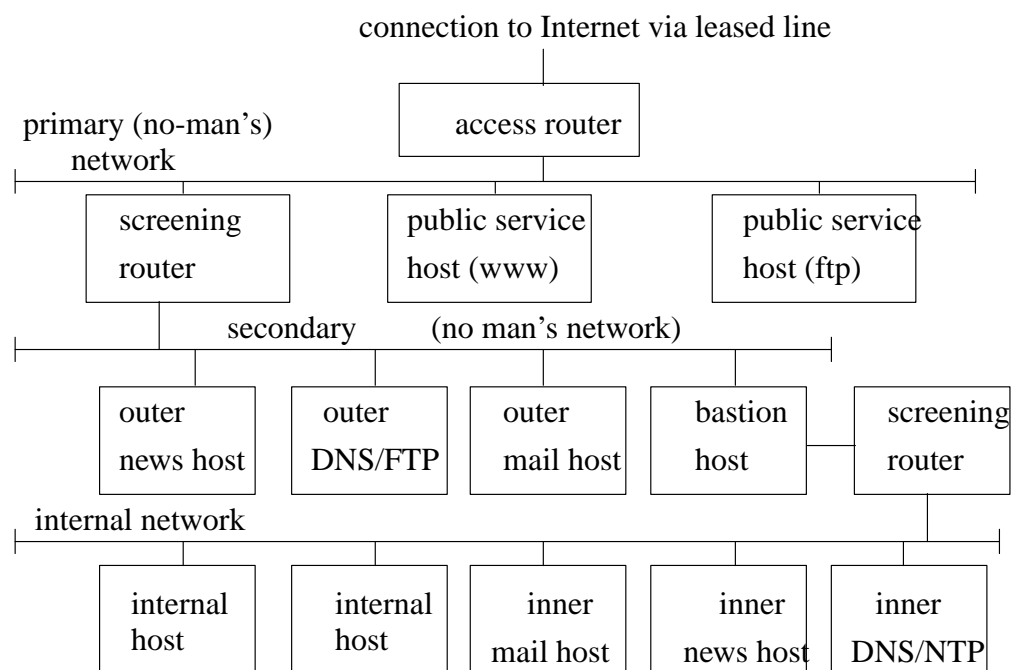
- consider the sftp service
 - if someone in the organisation needs to use sftp
 - the user cannot run sftp client software directly
 - must run the sftp client on the bastion host

- once the file has been retrieved
 - on the bastion host

- it is transferred to the users machine

Recommended firewall architecture

- try and link together TCP/IP services and support protocols together with firewall structure



Topological justifications: access router

- leased line and Internet provider outside our control

- however it might provide basic security via filtering, typically it:
 - prevent incoming IP datagrams with same src address as internal hosts
 - prevent remote management requests to either itself or any part of firewall
 - for example: ssh and SNMP from outside
 - prevent an attacker from forcing a particular route to be chosen for communications using incorrect src datagrams
 - for example: falsifying ICMP routing packets

Primary (no-man's) network

- acknowledging that the ftp and www servers are extremely vulnerable to attack
 - they are placed in the primary network
 - often termed the de-militarised zone (DMZ)

- obviously efforts are made to make these machines as secure as possible
 - but sensible precaution to keep them safely isolated from internal hosts

- screening router is particularly hardened
 - remember access router maybe owned by someone else

Primary (no-man's) network

- our screening router is configured to restrict communication between certain hosts
 - uses specific filter rules
 - example: only bastion host can ssh to www server

Secondary (no-man's) network

- this network contains machines which are not as vulnerable as those providing public services
 - but are visible from the rest of the Internet

- screening router #1 filters incoming packets to protect these machines from external users
 - allows specific TCP ports access, for example:
 - NNTP allowed into outer news host
 - SMTP allowed into outer mail host

Secondary (no-man's) network

- bastion host
 - stripped to the core!
 - built up again
 - extensive auditing and services kept to absolute minimum
 - provides a proxy service (it relays requests)
 - effectively an application level filter

Internal network

- internal hosts are in theory protected by the bastion host
 - bastion host can translate IP datagram headers so that the outside world does not know the IP address of inner hosts
 - inner hosts are invisible to the Internet
 - a machine that is not known is less likely to be attacked

- services such as email and news are handled internally by relevant servers
 - external email is passed by an internal email server
 - through the bastion host
 - and then through the proxy server to the Internet

Applications of firewalls

- an obvious use is to place a firewall between organisation and Internet
- can also be used to guard separate components of a LAN
- can deny certain protocols between departments
 - example: University of Glamorgan could install firewalls between departments
 - to stop departmental server traffic migrating into different departments