Firewalls

- A firewall is a network element which tries to stop attackers from coming into the system.
- A firewall has (or should have) the following properties:
  - All traffic in either direction must pass the firewall.
  - Only traffic authorized by the local security policy can pass.
  - The firewall itself cannot be hacked.
- Is this so? Firewalls have been hacked (Example the Quake site at Crack dot Com, Texas).
- Passing a firewall is possible, e.g. a trapdoor can be opened with a virus.
- There is a claim that a stealth security scanner Jakal can obtain information from the network behind a firewall, depending on how the firewall blocks traffic (i.e., the hacker must look at the response from the firewall.)

Firewalls

- A firewall has two or more interfaces and it works either as a bridge on network or transport level, or as an application gateway.
- Some firewalls have one LAN interface card and a WAN interface card (maybe even not IP), but it is more common to have a firewall, which connects two LAN segments.
- One of these LANs is connected directly to the internal network and another to a LAN segment, where there is a router connecting it to the external Internet or extranet.
- This configuration is sometimes called bastion host.
- A intranet is the company IP-network protected by the firewall.
- Extranet is an IP-network, which is connected to the Internet with another firewall and meant as an IP-network for some set of users, typically business partners.

Firewalls

- In the bastion host configuration servers offering services for the external world are placed in the LAN segment separated from the internal network by the firewall.
- These servers typically offer HTTP, FTP and SMTP.
- For STMP the daemon on TCP port 25 in the external part is often a proxy, not the real sendmaild daemon.
- The firewall does not allow incoming connections to FTP or HTTP, but allows users of the internal network to have external connections through the firewall for FTP and HTTP.
- Some services, like DNS, must be allowed through a firewall.
- A firewall can be of basically two types:
  - a packet of circuit filter
  - an application level proxy
- There are other classifications, which identify more types.

Firewalls

- A simple packet firewall takes each IP-packet and looks at the fields: receiver address, sender address, transport protocol (TCP or UDP) and port numbers of sender and receiver.
- Then it makes a decision to pass the packet or to discard it, so a simple packet is a network level bridge (actually, a router).
- A simple packet firewall works on each IP-packet separately.
- A freeware simple packet filter is drawbridge. Karlbridge used to be another, now it is a product packed in hardware.
- A plain circuit level firewall decodes the protocol up to TCP or UDP level and looks at the address information in the transport protocol. It makes a decision to pass the transport level frame.
- In a circuit level firewall there is are proxies for different TCP and UDP port numbers, but the firewall does not decode the application level protocol data unit (PDU). So, a circuit level firewall is a transport level proxy.

Firewalls

- A stateful packet firewall is an automaton, which keeps a state for each incoming connection and combines information from IP-packets in each connection.
- It can also understand, that one logical connection may contain several connections to different port numbers, like FTP opens two TCP socket connections.
- A stateful packet firewall has some clever logic, which combines all the information and makes an intelligent decision.
- So, in fact a stateful packet filter understands relatively much of application level matters, though it does not decode application level PDUs.
- To conclude, the three types of network or transport level bridges: a (simple) packet filter, a stateful packet filter and a circuit level proxy

Firewalls

- An application level gateway looks at the application level PDU and can check any fields the designer though useful to check.
- A virus check is often added to application level firewalls.
- Application level firewalls are more safe than packet filters since there is no IP forwarding.
- There are disadvantages in application level firewalls:
  - There must be a proxy for each service. There are relay proxies for most common services (like HTTP, FTP, Telnet, RPC, rlogin, NFS, Gopher), but what to do when a new service is introduced?
  - A user must connect to the proxy, not to the application. This requires either changing the user behavior or changing the client side for some services, like Telnet, to do the connection to proxy transparently so that the user does not see it.

Firewalls in routers

- Many routers have some firewall capabilities. Mostly in the form of Network Address Translation (NAT) combined with a packet filter which allows setting filtering rules.
- CISCO routers have NAT and access control based on access lists. In the access lists you can specify IP-addresses of the receives and the sender, protocol (TCP or UDP) and port numbers for the receiver and the sender.
- In Linux router software there is an inbuilt firewall software called Netfilter. It offers hooks by which you can take any packet, investigate it, put it back to a queue in the router, or drop the packet.
- The Linux router software also has NAT.
- You can rather easily modify the Linux firewall.

Firewalls in routers

- The Network Address Translation is a facility, where a router changes an IP-address to another IP-address.
- Then you can use different address allocation schemes (address space) in the two networks connected by a router.
- Just to mention: NAT can be useful in other context, it is very fast in address translation. We have made a solution when NAT was used with the same address space in both sides. We reserved with ReSerVationProtocol a connection between two CISCO routers. The CISCO routers for IPv4 accept to the reserved flow only traffic with the same IP-addresses as the RSVP request used. We wanted to put some traffic with other addresses to this RSVP reserved connection and did it by changing the addresses with NAT and saving the original addresses to a padding field.

Firewalls in routers

- In NAT is used to connect two different addressing spaces, then connections from outside never see the internal addresses and cannot connect to them.
- In a simple usage of NAT you can have the internal and external address map one-to-one, then if is easy to make connections both way.
- Transport level firewalls use NAT so, that to the external word there is visible only one address (the firewall's IP-address) but inside in the network there are several IP-addresses from the inside address space.
- This works for outgoing connections (which the firewall supports). For incoming connections there would be needed some additional identifier to know to which host in the internal network the connection is going to.

Firewalls in routers

- There may be problems with this type of NAT usage. Some protocols, notably FTP, want to know the addresses on application level on both end systems.
- Then the external system would use the firewall's external IP-address and the internal end system would use its internal address. This could not work, therefore such applications are given a special application level proxy if NAT is in use.
- There are different ways to use NAT in the firewalls.
- One usage is that the end system trying to connect to another end system through the firewall user the end system's IP-address. the firewall intercepts the call and forma a new connection to the end system and makes a transparent communication between these two connections. Examples of this way are Centri, Eagle and Milkyway's Black Hole.

Firewalls in routers

- The other way is that the end system is connecting to the proxy with the proxy's IP-address and the proxy is connecting to the end system with another connection.
- Then both end systems see that there is a proxy. This can be hidden from the application by programming a browser to change the IP-address in the end system.
- Many WWW-browsers, like Netscape Navigator and MS Internet Explorer can be programmed to change the addresses.
- Firewalls working in this way include TIS Firewall Toolkit, TIS Gaunder, Digital’s AltaVista Firewall and LSLI’s PORTUS.
- There may be a problem in this way for using uncommon applications (RealAudio, RealVideo, LDAP etc.) through the firewall.

Firewalls in routers

- NAT solves one simple form of address spoofing.
- In packet level firewalls, if a hacker writes to an IP-packet a wrong address so that the address looks like an address from the internal network, it would pass the address check.
- This can be easily fixed so, that the address space is connected with the network interface card. Then it is not possible for internal traffic to come in to the firewall from an external port.
- A hacker may have an inside person, get a job in the company or in some way get around this problem.
- Notice, many firewalls have more than two ports. This is to allow extranets to be supported. (The extranet name is not standard Internet terminology, it is invented by one vendor, a good name anyway.)

Building a Firewall

- If you plan on building a firewall, there are several possibilities.
- If you only need to put some added security, it may be sufficient to use packet filtering capabilities of routers (CISCO, Linux) or to install a transport level proxy, like SOCKS.
- SOCKS is an example of an application level firewall. It intercepts the connection request and translates it.
- SOCKS is supported by many browser packages, like Netscape Navigator, which makes it easier to introduce.
- SOCKS is relatively easy to install, you can try it in the exercises.
- For better security you could consider building an application level firewall using TIS (Trusted Information Systems) Firewall Toolkit.

Building a Firewall

- TIS Firewall Toolkit was the first application level firewall. It is freeware. It is one of the most popular tools to build your own firewall.
- TIS Firewall Toolkit is not easy to use. It is a toolkit, not a ready plug-and-run program, so you must understand security issues. Sufficient time and effort must be spent on it to get a secure firewall.
- In many respect it is very good. It has a very good access control scheme: you can e.g. restrict access from a part of a network or even from a single address.
- Instructions on how to build a firewall using the TIS Toolkit are available. In the book Internet security Atkins et al. there is a whole chapter devoted for this. WWW material also exist.

Building a Firewall

- TIS Firewall Toolkit (TFWT) has a number of proxies:
- smap and smapd proxy for sendmail and sendmaild
- tn-gw proxy for Telnet
- rlogin-gw
- ftp-gw
- http-gw
- x-gw proxy for X window system
- plug-gw a proxy for other services (there is a configuration file where you set rules for all other protocols). If works for NNTP, POP etc., may not suit for all protocols.
- Configuring the proxies requires much work. There are tools (netscan, portscan) for checking the firewall and reporting functionalities in all proxies.

Building a Firewall

- There is a new CORBA (Common Object Broker Architecture) service CORBA Firewall standardized by OMG. It is one possible way to make a firewall in the future for CORBA-based systems.

- The firewall is configured by setting rules.
- General policies:

  Forbid everything that is not allowed. (recommended)

  Allow everything that is not forbidden. (not recommended)
- This is then simple. Allow separately outgoining and incoming connections for the applications. Or is it simple?
- FTP allow outgoing for all, incoming only to the FTP server in the bastion host.

Building a Firewall

- Telnet, rlogin - allow outgoing for all users, incoming not at all.
- SMTP - allow incoming and outgoing for all users.
- HTTP - allow outgoing for all users, incoming to the bastion host.
- DNS - domain name service, (also whois), allow completely
- PING - probably allow
- RSH, REXEC, TFTP, FINGER - forbid as too dangerous
- SNMP - forbid, no network management from the Internet
- NNTP - news, allow
- POP - Post Office Protocol, could be allowed if used
- NTP - network time protocol, forbid, setting time could be bad
- - - - continue in this manner

Building a Firewall

- With an application level firewall this went fine, we had the proxies for all the necessary services.
- With a packet level firewall we had one problem already: DNS had to be allowed but what about other applications on RTP (real Time Protocol). They are on UDP like DNS, but RTP gets a port from portmapper and there is no definite port to close.
- We could close all UDP ports on some range, but will DNS be then also closed?
- We have problems with services on RTP with an application level firewall as well. No ready proxies.

Building a Firewall

- FTP has some special features caused by how it works and what it does.
- FTP should be operated only in the passive mode. FTP works so, that there first comes a connection request from the sender. Then ftpd tries to open a new socket connection to data, i.e., data uses another connection. Usually this second connection is initiated by ftpd, but in the passive mode it is also initiated by the sender.
- Why the normal mode would not work through a firewall is that the firewall is usually configured not allow incoming connections for ftp.
- Web browsers have ftp working in the passive mode, so their ftp works. Some other ftp implementations then do not work through a firewall.

Building a Firewall

- Especially with services which fetch files, like ftp and tftp,it is important that the hacker cannot fetch a password file and do password cracking on it.
- Remember to chroot all directories correctly.
- chroot restricts applications access to the file system and in this way you can restrict TFTP (if you want necessarily to use it) to certain directories. The same goes for TFP.

- There are similar complicated problems with some other applications than FTP, so securing them requires special proxies for all of them.
- This is why a general plug-gw proxy of TIS Firewall Toolkit may not be sufficient for some new services.

Building a Firewall

- TCP Port Wrapper can be used to build a transport level firewall. There are port wrappers for several TCP ports and they can log information of incoming traffic and discard TCP frames.
- In one project we used the Netfilter for packet measurement purposes. It is quite simple to use, so making your self a packet filter with or without state information to Linux router is quite possible.
- We noticed one thing: the performance depended essentially on whether the code was run as a kernel module or as a user space module. If in the kernel, the code runs very fast. The relevance to a firewall is that probably the protocol level is not so important. The performance is determined by the implementation, mainly on whether the code can run in the kernel most of the time.

Buying a Firewall

- A firewall can be bought as a product.
- Many operators offer firewall service, when you rent a firewall located in the operator’s locations and you buy either 24 hour maintenance/assistance to it, or for a shorter time.
- The price of a firewall service is not negligible (it is rather high), but one should count the cost of maintenance and assistance if made by own company.
- A firewall may become a bottleneck to the network, so it must be selected so that it has sufficient performance.
- A typical complaint with firewalls is that some users cannot use their services through a firewall. These complaints are more difficult to solve if the firewall is a product and there is no way to add features.

Buying a Firewall

- Raptor's Eagle has application and transport level proxies. Several application protocols have proxies (such as HTTP, STMP, FTP) and there is a generic TCP-level proxy.
- Digital's AltaVista Firewall is similar to Eagle in its mode of operation.
- Check Point Software Firewall-1 is made by Israelian firm founded 1993 (is there a trapdoor for Israel intelligence?). Firewall-1 has both a packet filter and application level proxies. The application level proxies are of low performance, while the packet filter is very fast. The packet filter is stateful packet firewall.
- The user interface is nice and easy to use.
- Firewall-1 seems to be the best known product in Finland for commercial firewalls.

Buying a Firewall

- Global Internet's Centri is primarily a proxy firewall. It has a very simple packet filter additionally. The packet filter is not stateful.
- Network-1's Firewall/Plus is primarily a packet filter. It has stateful packet filtering technique.
- It is unique in starting filtering from Ethernet frames, not from IP level, so it can test non-IP protocols, such as IPX, NetBEUI, AppleTalk, DECnet.
- It is not a router but a bridge. It has transparent operation.
- In some configuration it is very slow, despite of operating on a very low protocol level.
- The user interface is difficult, but it enables a very precise investigation of packets and setting of decision rules.

Buying a Firewall

- There are many other firewall products. The following are mentioned in the book Maximum Security, but that information is rather old.
- CISCO PIX Firewall, not using proxies but based on a secure operating system within the hardware.
- Sun’s SunScreen is a series of products. Heavy -duty packet filtering. Special features like encryption.
- IBM Internet Connection Secured Network Gateway. For AIX, uses application proxies and has logging capabilities.
- Some other firewalls can be added:
- LSLI’s PORTUS
- TIS’s Gaunder
- Milkyway’s Black Hole

Does a firewall give safety?

- Trivial fact: A firewall is not really a wall, you must leave some holes to the wall, else your network is not connected to the Internet.
- Often workers in the company have a joint project and will want to open an access which does not go through the firewall and will not comply with the company security policy.
- For a security administrator it is easy to say that such cannot be allowed, but if the work is part of the main business of the company, so probably such holes will be opened, officially or not.
- Modem ports may also be installed or left there, they may be only for convenience and could be more easily forbidden.

Does a firewall give safety?

- An application proxy can be configured to filter Java applets, other executable content, and anti-virus software can be used.
- As long as the users do not want the benefits from mobile code, applets, etc. In general, the concept of a firewall protection may become outdated in the future.
- Anti-virus software does not stop all new viruses.
- Anonymous in Maximum Security book p. 653 hints that with the Jakal scanner and some suitable scripts one can break into some firewalls.
- One must remember that a hacker can get into the internal network by e.g. social engineering, so security based solely on firewalls is not advisable.

Does a firewall give safety?

- A firewall may make the system vulnerable to Denial of Service (DoS) attack.
- This can in principle be caused by checking being rather slow so that a firewall may become a performance bottleneck. Then it can be attacked.
- It can also be caused by a too simple proxy, which does not work properly. Many proxies have some simplifications in negotiating options and also errors in the protocol implementation which may enable DoS attack.
- In general one can say that firewall performance is good, but in some situations performance can be low. There is no way of saying anything general of the performance. A packet filter can be slow or fast, an application proxy can be slow or fast. Most commercial firewalls implement both proxies and packet filters.

Does a firewall give safety?

- Traditionally the Internet has been very unsecure because Unix networking has included a large set of unsecure services.
- Firewalls block most of the unsecure services and the traditional attacks become more difficult. Scanning for open unsecure ports may become rather useless.
- Traditional holes, like buffer overflows, may become rare cases. There will be such cases but they are not available all the time.
- If it would only be a question of securing email, Web, FTP, this could be done simply.
- However, there are the new services. Many of the new services will be on unknown UDP ports (using RTP, so the port numbers are dynamically allocated) and securing them would depend on security of the protocol implementation, not on a firewall.
- This is, there is no proxy for them and no well-known port.

Does a firewall give safety?

- Instead of writing a secure proxy for the new services, it is better to write the service to be secure itself.
- A firewall can be penetrated by a trapdoor inserted in a service, like email, which users want to pass.
- Therefore a firewall is no real protection.
- A firewall assumes that people outside can be hackers but people inside are trustable, this is a strong assumption.
- Firewalls have improved security quite tremendously.
- Still I would say that it is possible that a firewall as an idea will not be a permanent component in a solution to security of the Internet.
- It serves to block unsecure services, but why these services should exist in the intranet either without sufficient security level. A firewall creates inconvenience to users.