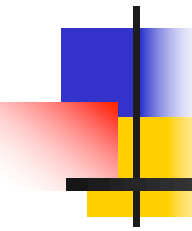
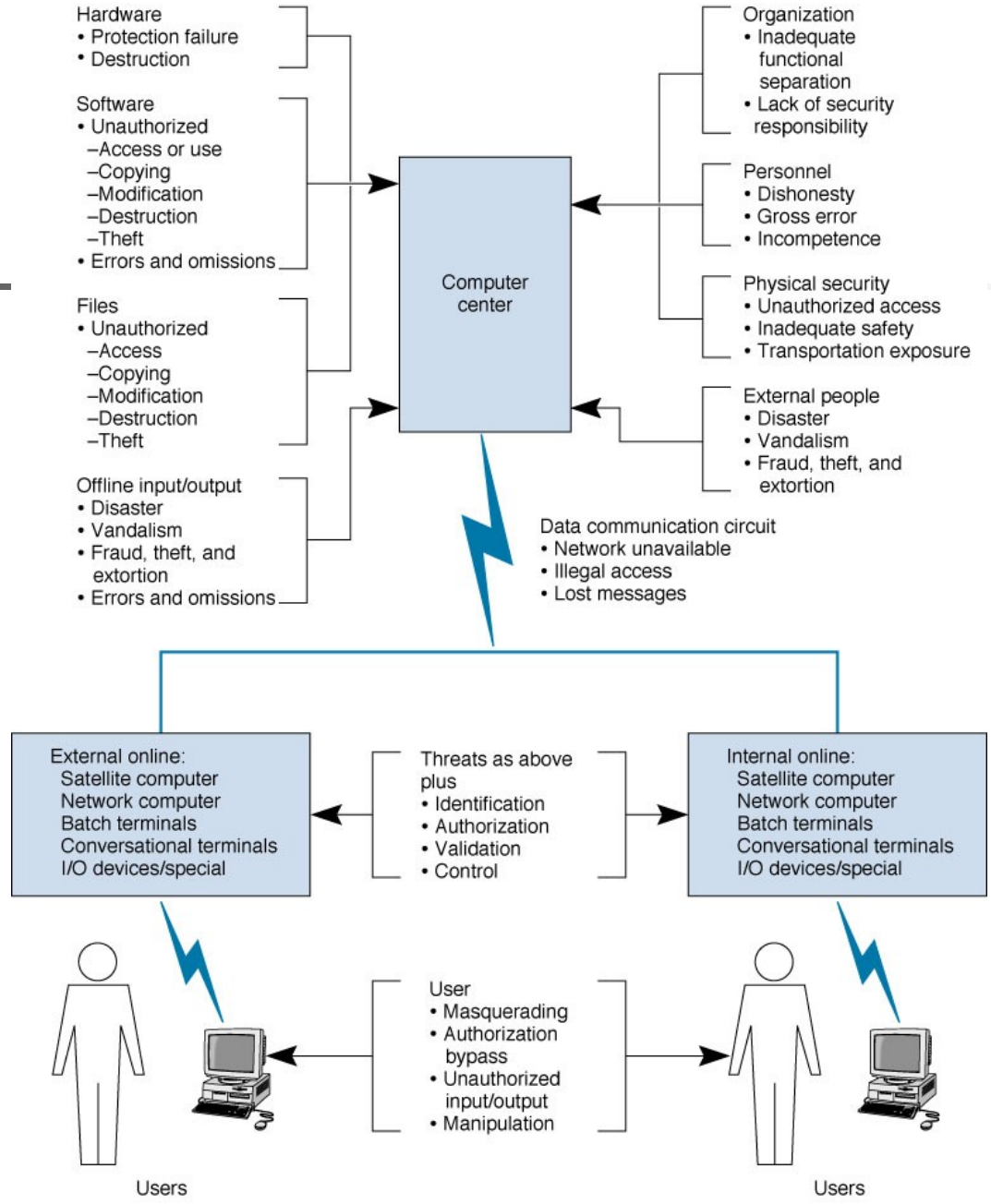
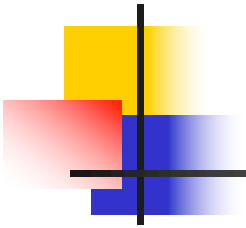


Network Security

Firewall

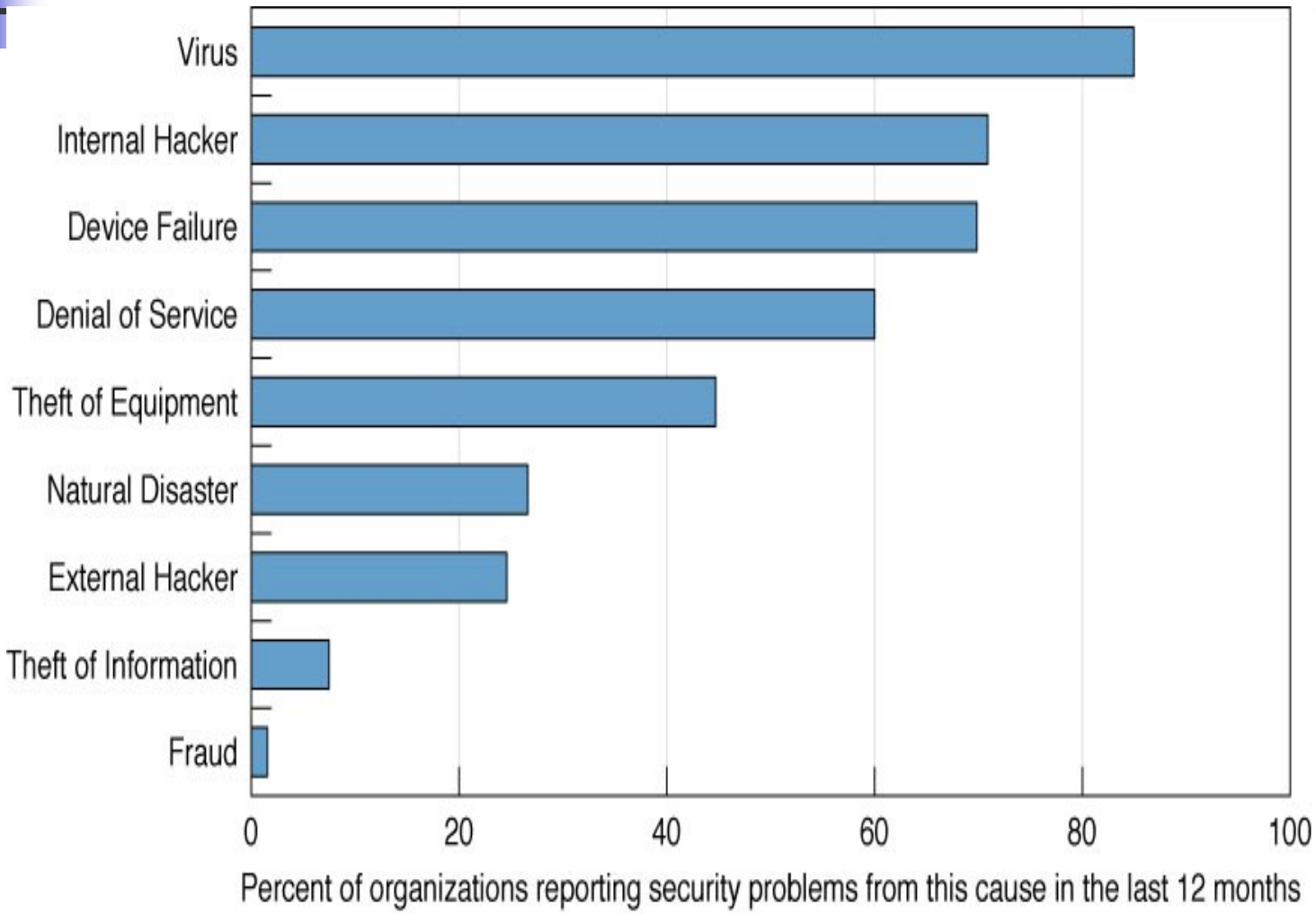

Hardware
• Protection failure
• Destruction
Software
• Unauthorized
–Access or use
–Copying
–Modification
–Destruction
–Theft
• Errors and omissions
Files
• Unauthorized
–Access
–Copying
–Modification
–Destruction
–Theft
Offline input/output
• Disaster
• Vandalism
• Fraud, theft, and extortion
• Errors and omissions
Computer center
Organization
• Inadequate functional separation
• Lack of security responsibility
Personnel
• Dishonesty
• Gross error
• Incompetence
Physical security
• Unauthorized access
• Inadequate safety
• Transportation exposure
External people
• Disaster
• Vandalism
• Fraud, theft, and extortion
Data communication circuit
• Network unavailable
• Illegal access
• Lost messages
External online:
Satellite computer
Network computer
Batch terminals
Conversational terminals
I/O devices/special
Threats as above plus
• Identification
• Authorization
• Validation
• Control
Internal online:
Satellite computer
Network computer
Batch terminals
Conversational terminals
I/O devices/special
User
• Masquerading
• Authorization bypass
• Unauthorized input/output
• Manipulation
Users
Users



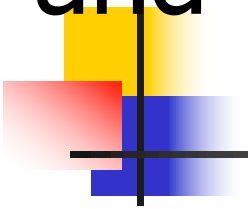
Security Threats

- A network security threat is any potentially adverse occurrence that can harm or interrupt the systems using the network, or cause a monetary loss to an organization.
- Once the threats are identified they are then ranked according to their occurrence.
- The next slide summarizes the most common threats to security.

Common Security Threats



Preventing Disruption, Destruction and Disaster



- Preventing disruptions, destructions and disasters mean addressing a variety of threats including:
  - Creating network redundancy
  - "Preventing" natural disasters
  - Preventing theft
  - Preventing computer virus attacks

Network Redundancy

- The key to in preventing or reducing disruption, destruction and disaster - is **redundancy**.
- Examples of components that provide redundancy include:
  - Uninterruptible power supplies (UPS)
  - Fault-tolerant servers
  - Disk mirroring
  - Disk duplexing
- Redundancy can be built into other network components as well.

Preventing Natural Disasters

- Disasters are different from disruptions since the entire site can be destroyed.
- The best solution is to have a completely redundant network that duplicates every network component, but in a different location.
- Generally speaking, preventing disasters is difficult. The most fundamental principle is to decentralize the network resources.
- Other steps depend on the type of disaster to be prevented.

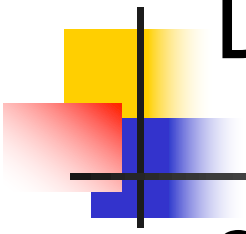
Preventing Theft

- Equipment theft can also be a problem if precautions against it are not taken.
- Industry sources indicate that about $1 billion is lost each year to theft of computers and related equipment (USA statistic).
- For this reason, security plans should include an evaluation of ways to prevent equipment theft.

Preventing Computer Viruses

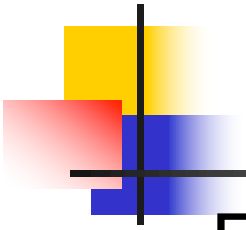
- Special attention must be paid to preventing **viruses** that attach themselves to other programs and spread when the programs are executed.
- **Macroviruses** attach themselves to documents and become active when the files are opened are also common. Anti-virus software packages are available to check disks and files to ensure that they are virus-free.
- Incoming e-mail messages are the most common source of viruses. Attachments to incoming e-mail should be routinely checked for viruses - ref University Policy
- The use of filtering programs that 'clean' incoming e-mail is also becoming common.

Detecting Disruption, Destruction & Disaster



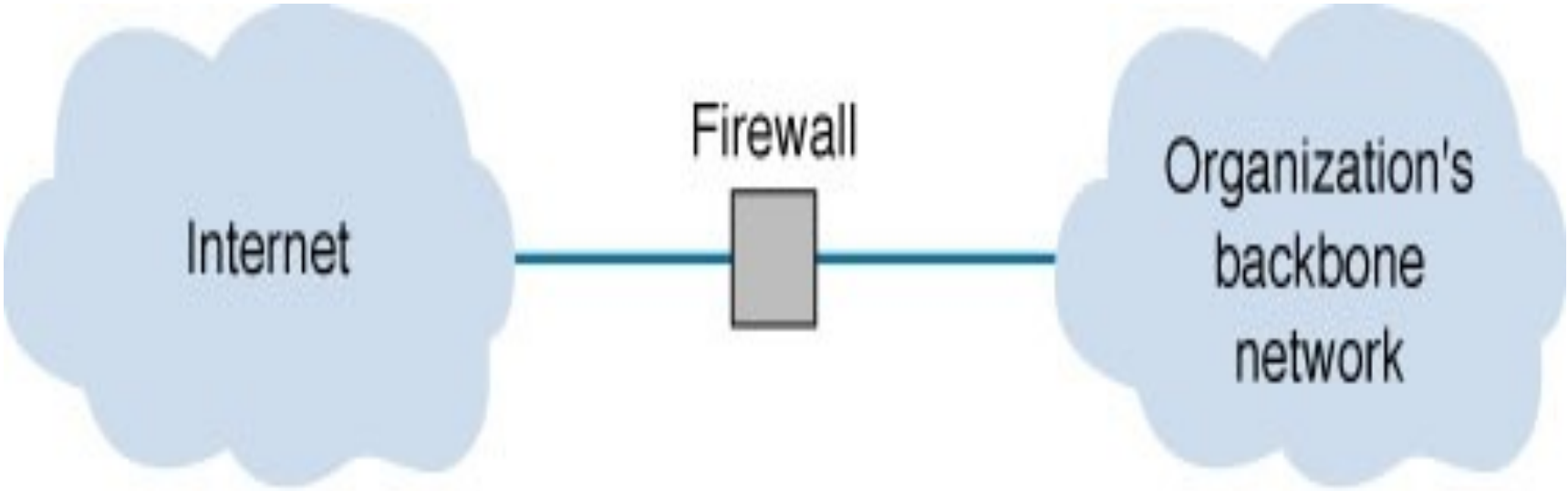
- One function of network monitoring software is to alert network managers to problems so that these can be corrected.
- Detecting minor disruptions can be more difficult.
- The network should also routinely log fault information to enable network managers to recognize minor service problems.
- In addition, there should be a clear procedure by which network users can report problems.

Firewalls

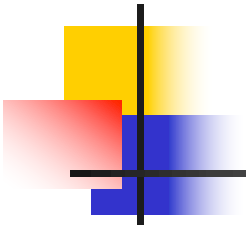


- Firewalls are used to prevent intruders on the Internet from making unauthorized access and denial of service attacks to your network.
- A **firewall** is a router, gateway, or special purpose computer that examines packets flowing into and out of the organization's network (usually via the Internet or corporate Intranet), restricting access to that network.
- The two main types of firewalls are packet level firewalls and application-level firewalls.

Using a firewall to protect networks.



Packet Filters

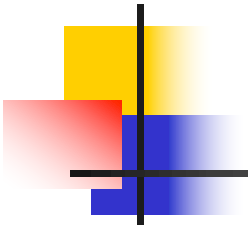


- A packet-level firewall (or **packet filter**) examines the source and destination address of packets that pass through it, only allowing packets that have acceptable addresses to pass.
- ***Since each packet is examined separately, the firewall can't understand what the sender's goal is***.
- Packet filters may be vulnerable to **IP spoofing**, accomplished by changing the source address on incoming packets from their real address to an address inside the organization's network.
- While packet filters have strengthened their security since the first cases of IP spoofing, IP spoofing remains a problem.

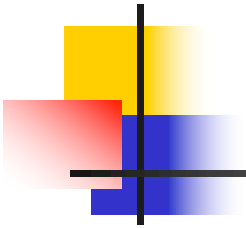
Application-Level Firewalls

- An **application-level firewall** or application gateway acts as an intermediate host computer, separating a private network from the rest of the Internet, but it works on specific applications, such as Web site access.
- The application gateway acts as an intermediary between the outside client making the request and the destination server responding to that request, hiding individual computers on the network behind the firewall.
- Because of the increased complexity of what they do, application level firewalls require more processing power than packet filters which can impact network performance.
- Some call IDS/IPD now a day.

Security Holes



- Security holes are made by flaws in network software that permit unintended access to the network. Operating systems often contain security holes, the details of which can be highly technical.
- Once discovered, knowledge about the security hole may be quickly circulated on the Internet.
- A race can then begin between hackers attempting to break into networks through the security hole and security teams working to produce a patch to eliminate the security hole.

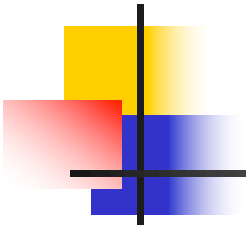


policy

- You need to decide what you want to protect and
  - Inventory what you are doing
  - (Email, Web/ Modems/ Database, etc.)
- Then design how to protect it
  - Wall (Firewall), IDS/IPS
  - Throw it away
  - Improve authentication, i.e. one time keys
  - …

Security is base on trust and risk

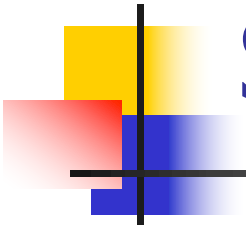
- Assume: perfect Inet-wide IPSEC
- Does this mean “perfect security”
- No… you still have to trust the other side or the other network (Engineers) or ou employees



Firewall not enough because

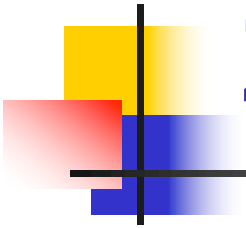
- Social engineering attacks
  - I’m from IT and I need Boss’s password
  - Lack of physical security for computer console
  - Secret in the dumpster
  - Secret in the floppies, flash drive
  - Etc.

So, what firewall does



- Firewalls control access – on one more machine that constrain access to an internal network
- Firewall may allow you to implement rule-based policies and act as
- … “Chock point”

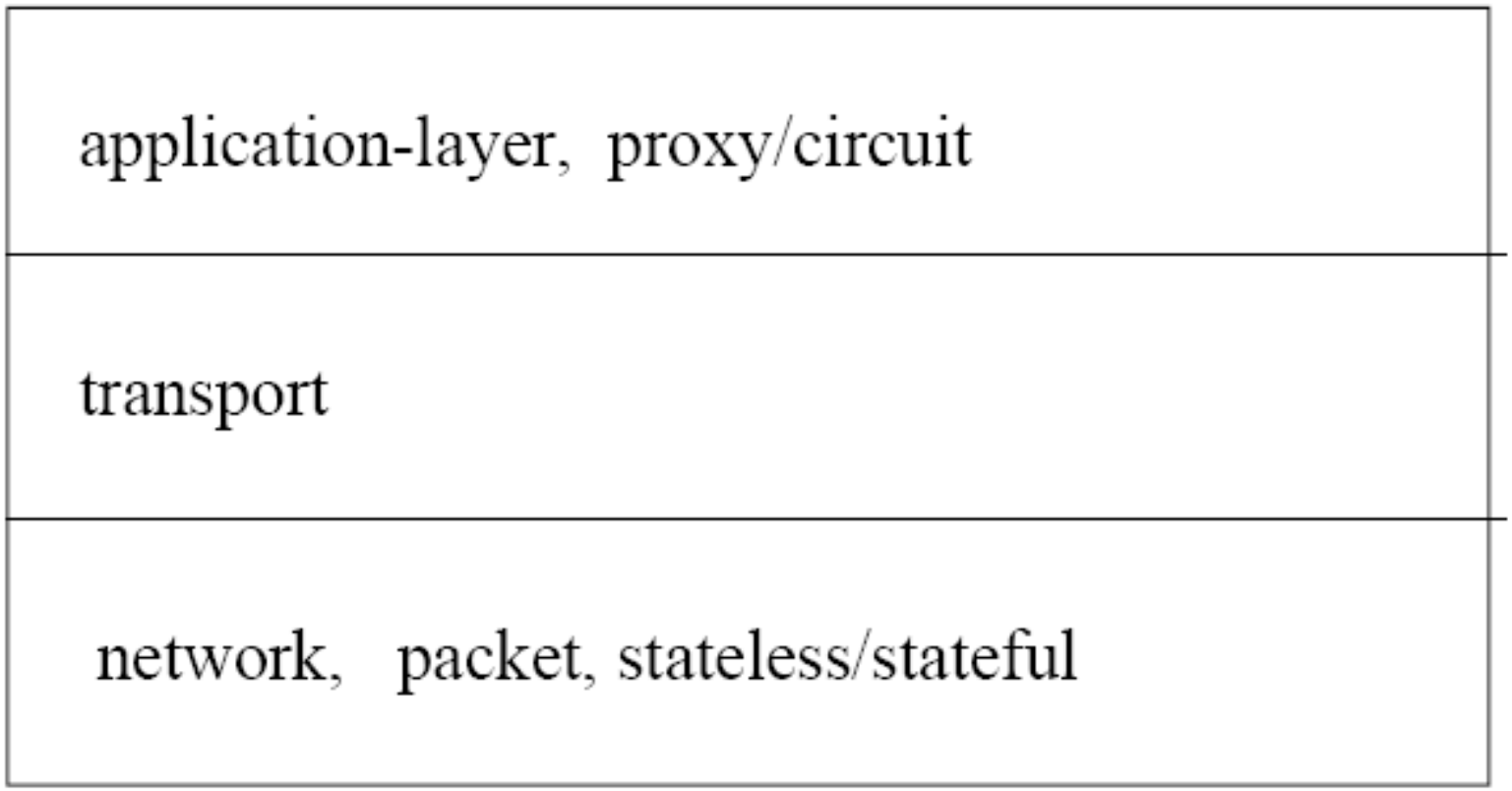
2+2 Kinds of firewall

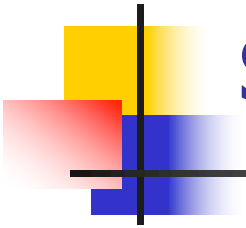


- **Access control list**; i.e. Packet Filters
- **Application Level Gateway**, Proxy Server
- two more possible forms (subforms)

- **Stateful packet systems**
- **Circuit proxy** – use TCP, and talk to server that turns around and acts as client

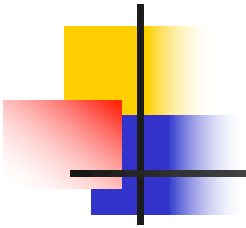
In General


application-layer, proxy/circuit
transport
network, packet, stateless/stateful

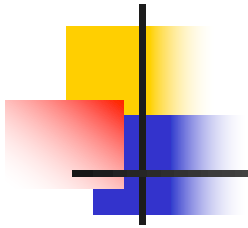


some buzzwords

- **bastion host** - system that is made more secure due to Internet exposure, typically workstation
- **screened host/network** - host or network behind firewall/router, amount of protection depends on rules in firewall. said router is a screening router.
- **perimeter network/DMZ** - network (often internal) between internal secure nets and outside world
- **defense in depth** - the notion that in addition to firewall one, you have host protection and internal firewalls, etc.

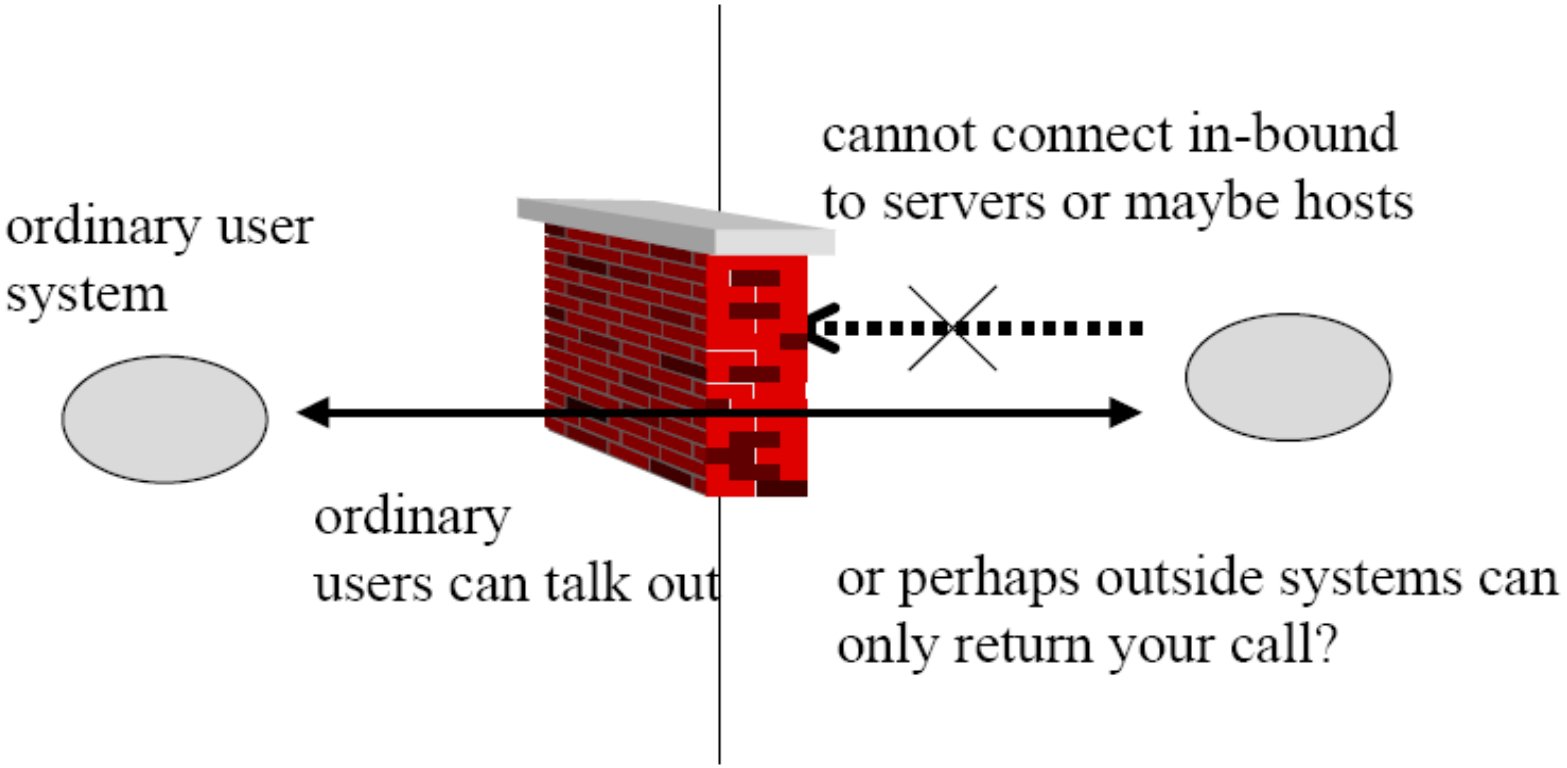


- **victim system** or **goat system**
  - – experimental and sacrificial
  - – maybe they are all victim systems?
- **intrusion detection** - looking for bad guys having landed (or little people?)
  - – may take a number of forms
  - » packet analysis, tripwire, log scanning, virus scans
  - – may be regarded as defense in depth technique
  - – may be regarded as internal defense technique

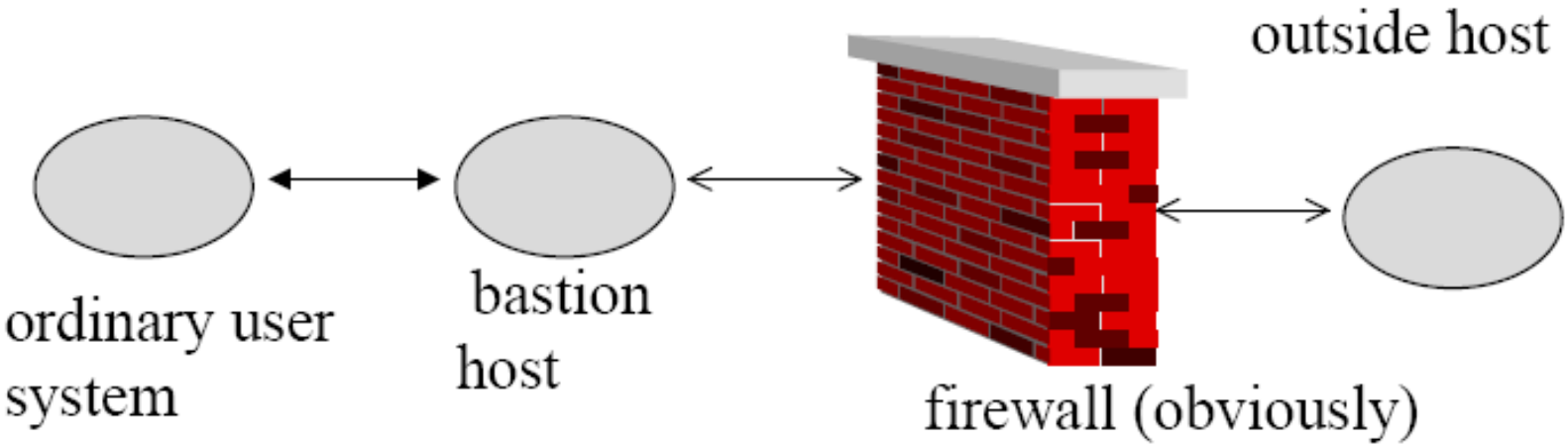


some possible firewall architectures follow

user systems can get out but bad guys are restricted getting in

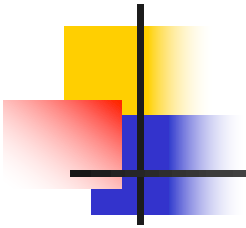


users cannot get out period and vice versa



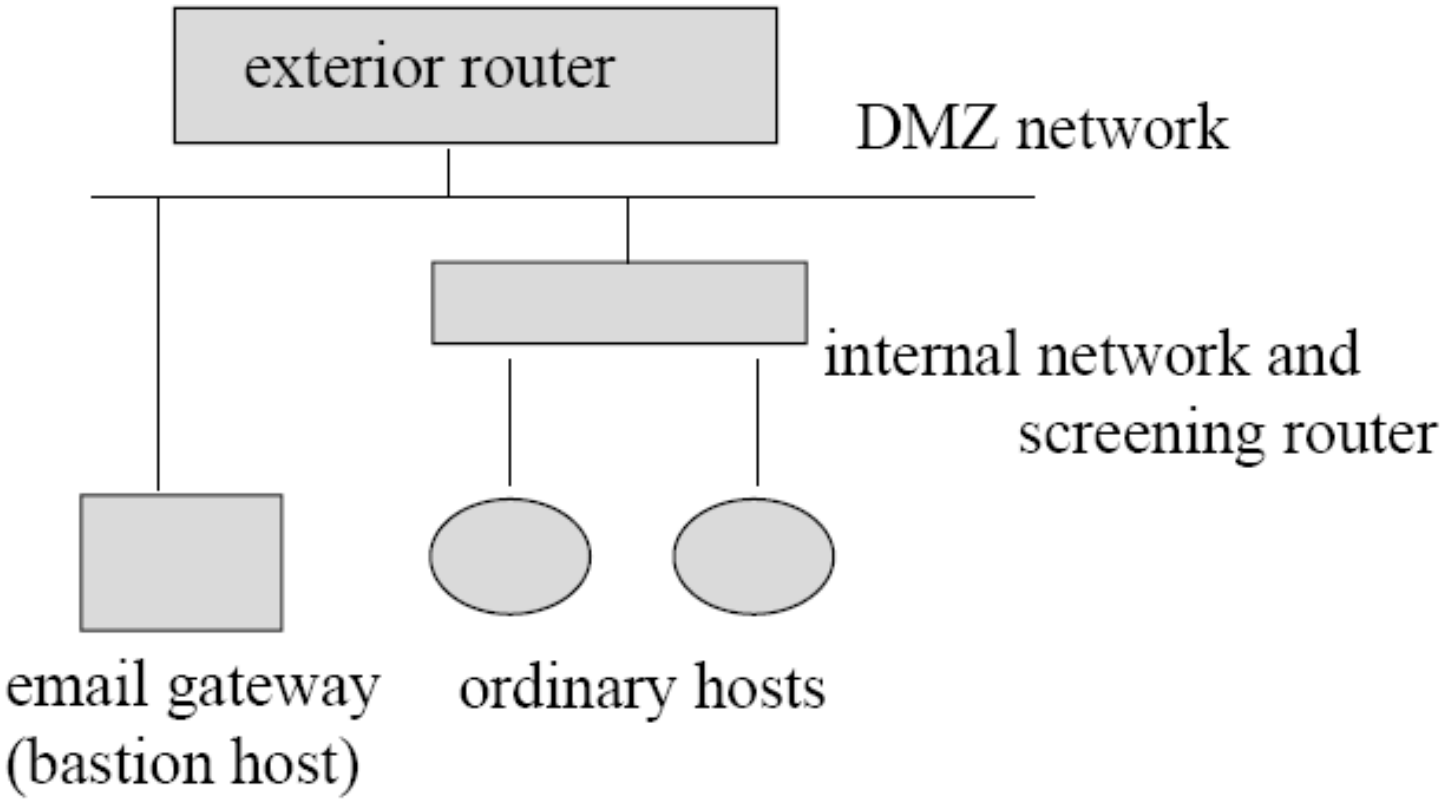
internal user systems cannot talk or be talked to
from outside world - only through intermediary

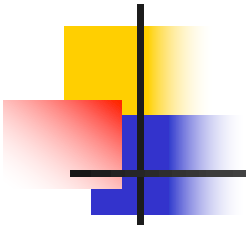
note to network engineers !!!



- **the infrastructure has to be protected too**
  - the routers/switches
  - snmp writes ...
  - the firewall is part of the infrastructure
    - if compromise succeeds on cisco router/switch or
    - brand X firewall
    - that is not a GOOD thing ...

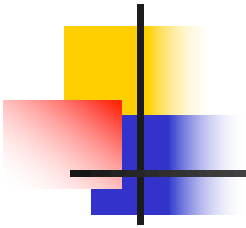
Classic arch model





Packet filters ---

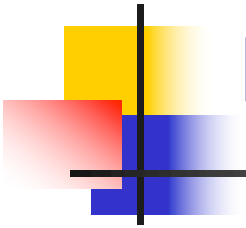
- typically associated with network layer/routing function (but peek at transport headers)
- use IP src/dst, protocol type, tcp/udp src/dst ports, IP encapsulation types (ICMP, IPIP)
- router knows i/f packet arrived on or is trying to escape on
- can understand IP networks as well as IP host addresses
- should be able to log “denys”



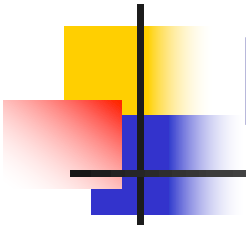
Pros and Cons

- **pros**
  - large scale tool - can turn off all telnet access or all access to subnet X or to proto Y
  - can deal with NEW service because it doesn't know about it
  - more efficient than application gateway
- **cons**
  - logging is harder because you may not have app/protocol knowledge (no state machine)
  - getting rule base right for ALL protocols is tricky
  - especially if accept all, deny some is policy basis

new kid on the block



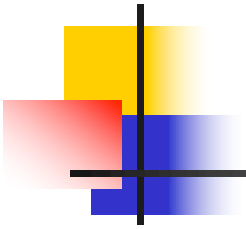
- **stateful inspection**
- basically packet filters that are smarter and look at "connection" state (tcp or udp)
- e.g., can easily setup so that no internal access is allowed outside in
- *external access is allowed inside out*
- *state: TCP out means expect TCP back in*
- perhaps easy to teach about new protocols



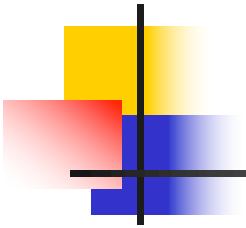
policy considerations

- start with: **deny all, permit a few**
  - pro: most paranoid/proscriptive/most secure
  - con: cost to getting anything accomplished is the most high
  - **pro: less need to react to latest hacker discovery**
- start with: **allow all; deny a few** (known bad)
  - pro: least impact on Internet traffic
  - con: least secure, + need to stay up to date on hackerdom

Example: deny all; allow a few

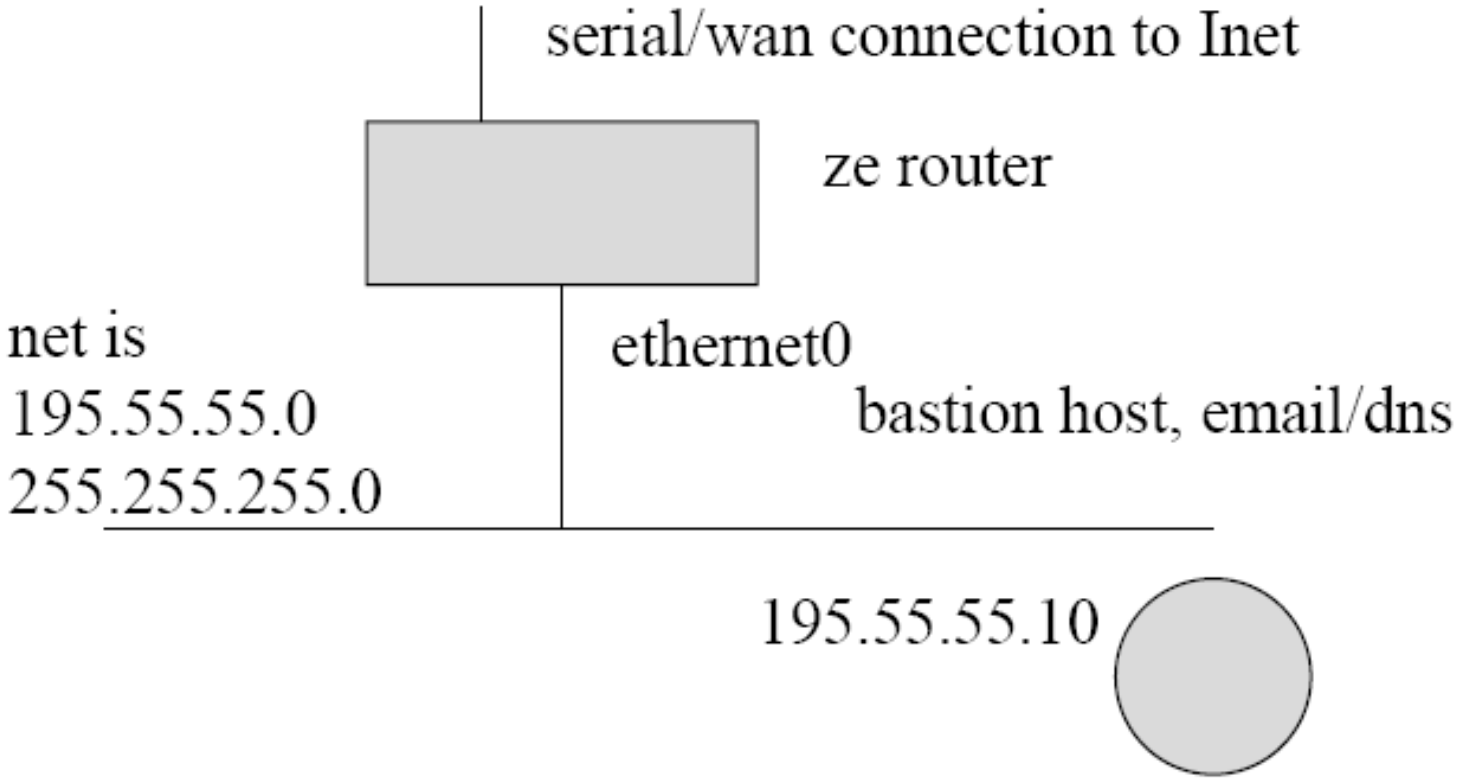


- no Internet traffic allowed to/from internal hosts except for proxies (application control gates)
- proxies include:
  - – web proxy (easy/apache)
  - – email proxy (easy/sendmail by definition)
  - – telnet proxy
  - – ftp proxy



- no IP spoofing (pkts leaving/entering must have IP src that make sense)
- no private IP addresses
- no directed broadcast 192.128.1.255
- no IP authentication-based protocols
  - lpr, X, nfs, rlogin, rsh
- no Microsoft TCP/NetBEUI (137-139)

ACL Example (Cisco)



Acl basic first….

- executed in order of list entries on a packet
- default deny at end
- basic form:
  - permit ip src-net src-mask dst-net dst-mask eq port
- permit or deny, log may appear at end
- access-list 101 permit ip 172.16.0.0 0.0.255.255 172.17.0.0 0.0.255.255
- *mask sets bits for bits to ignore*, therefore above means 172.16.X.X (any hosts in 172.16)
- net/mask may be replaced with **any** or **host 1.2.3.4**

Cisco deny all ACL example

- no ip source-route
- interface ethernet0
  - ip address 195.55.55.1
  - no ip directed-broadcast
- interface serial0
  - ip access-group 101 in
- ◆ access-list 101 deny ip 195.55.55.0 0.0.0.255
- ◆ access-list 101 permit tcp any any established
- ◆ access-list 101 permit tcp any host 195.55.55.10 eq smtp
- ◆ access-list 101 permit tcp any host 195.55.55.10 eq dns
- ◆ access-list 101 permit udp any host 192.55.55.10 eq dns