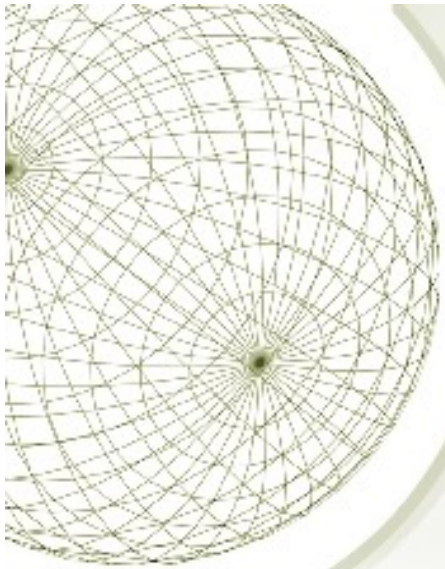


Firewalls

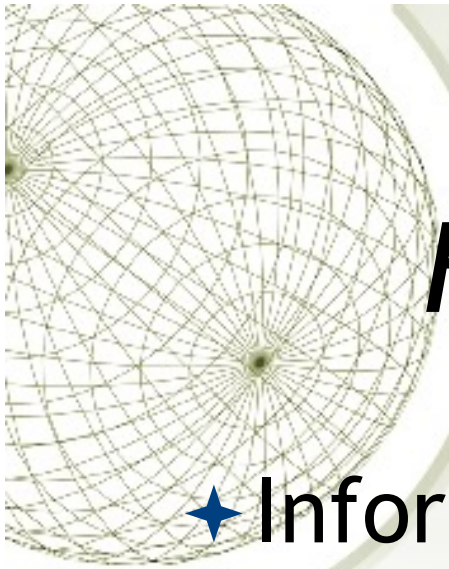
Ola Flygt
Linnaeus University, Sweden
http://homepage.lnu.se/staff/oflmsi/
Ola.Flygt@lnu.se

Outline

- Firewall Design Principles
  - Firewall Characteristics
  - Types of Firewalls
  - Firewall Configurations
  - Firewall Testing (extra material)

Firewalls

- Effective means of protecting a local system or network of systems from network-based security threats while affording access to the outside world via WAN's or the Internet



Firewall Design Principles

- Information systems undergo a steady evolution (from small LAN's to Internet connectivity)
- Strong security features for all workstations and servers not established

Firewall Design Principles

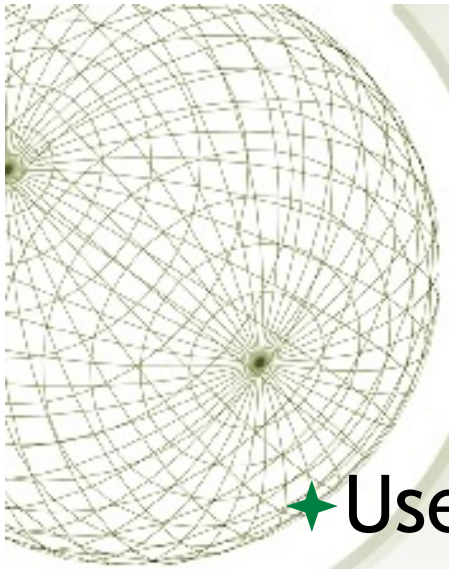
- The firewall is inserted between the premises network and the Internet with the aims:
  - Establish a controlled link
  - Protect the premises network from Internet-based attacks
  - Provide a single choke point
- The firewall itself is immune to penetration (use of trusted system with a secure operating system)

Firewall Limitations

- cannot protect from attacks bypassing it
  - eg sneaker net (the act of physically transporting data between computers), utility modems, trusted organisations, trusted services (eg SSL/SSH)
- cannot protect against internal threats
  - eg disgruntled or colluding employees
- cannot protect against access via WLAN
  - if improperly secured against external use
- cannot protect against malware imported via laptop, PDA, storage infected outside

Firewall Characteristics

- Four general techniques:
  - Service control
    - Determines the types of Internet services that can be accessed, inbound or outbound
  - Direction control
    - Determines the direction in which particular service requests are allowed to flow

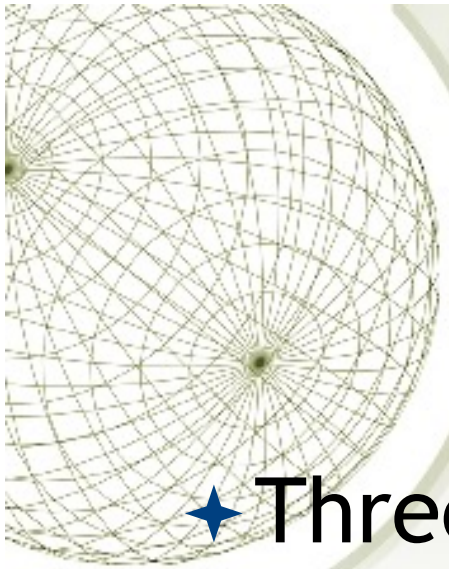


Firewall Characteristics

- User control
  - Controls access to a service according to which user is attempting to access it
- Behaviour control
  - Controls how particular services are used (e.g. filter e-mail)

Firewall Types

- Different scopes
  - Personal - a single host is protected
    - Typically implemented in software run as an application under a host OS
  - Site - the firewall protects an entire site
    - Typically a dedicated hardware device with hardened software
- We will mainly discuss the latter type in the rest of this presentation

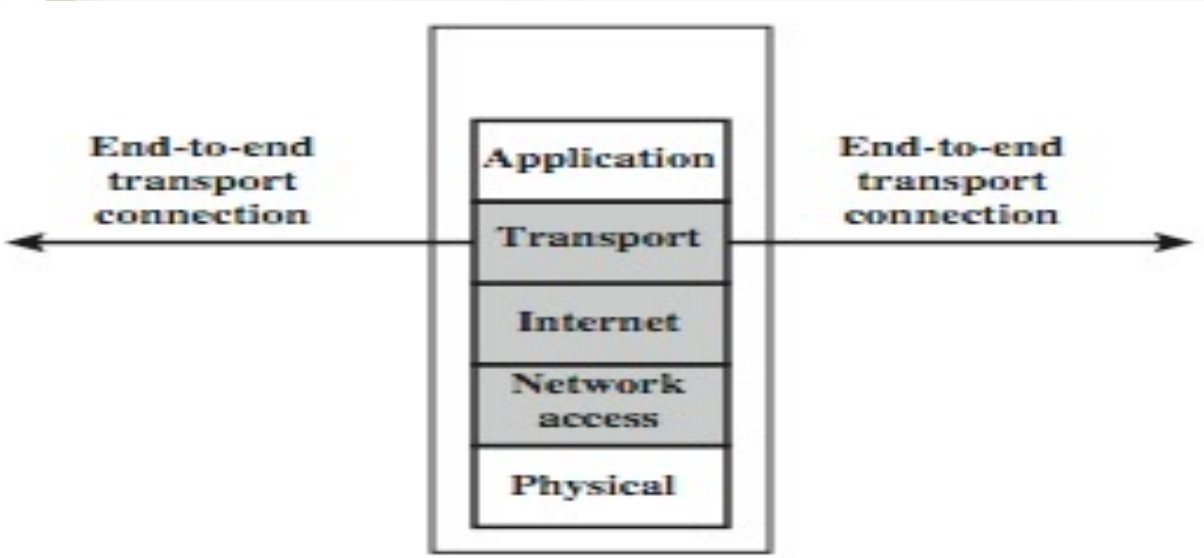


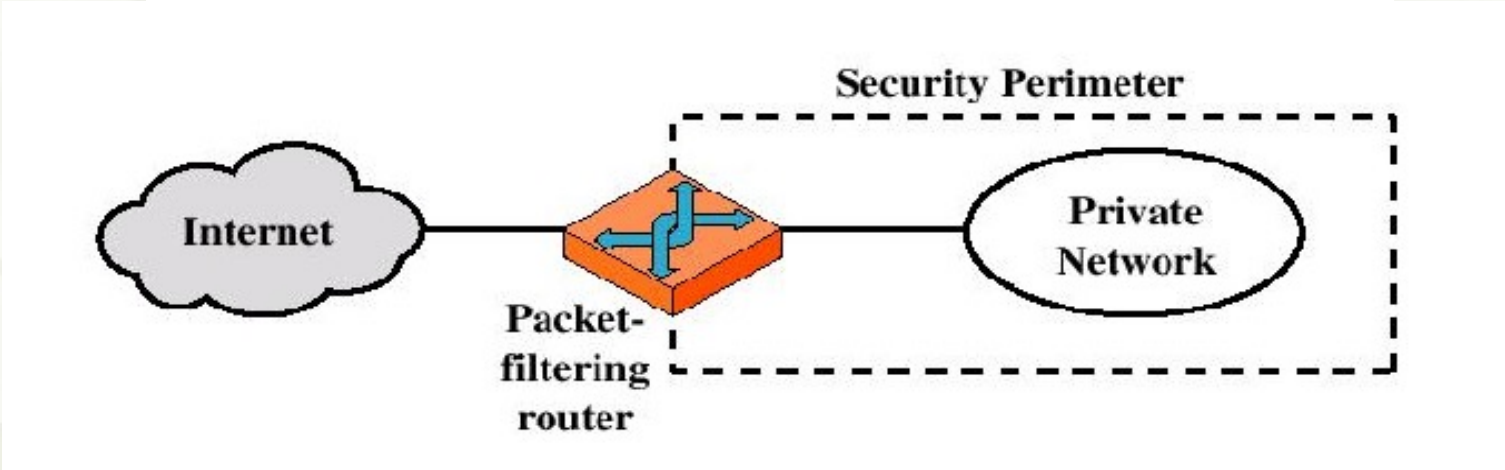
Types of Firewalls

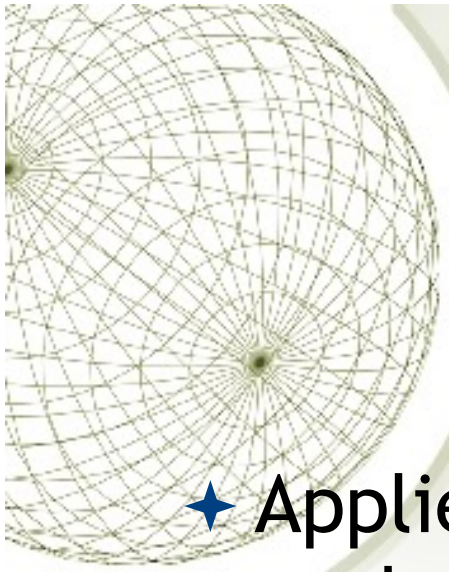
- Three common types of Firewalls:
  - Packet-filtering routers
  - Application-level gateways
  - Circuit-level gateways

  - (Bastion host)

Packet-filtering Router







Packet-filtering Router

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet
- Filter packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- Two default policies (discard or forward)

Filtering rule examples

Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
Outside connections to public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a Smurf DoS attack.	Drop all ICMP packets going to a “broadcast” address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP

Filtering rule examples

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Attacks on Packet Filters

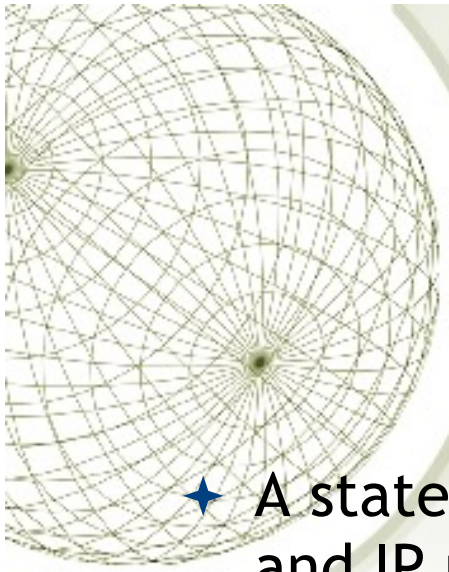
- IP address spoofing
  - fake source address to be trusted
    - ➔ add filters on router to block
- source routing attacks
  - attacker sets a route other than default
    - ➔ block source routed packets
- tiny fragment attacks
  - split header info over several tiny packets
    - ➔ either discard or reassemble before check

Packet-filtering charateristics

- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of authentication

Stateful vs. Stateless Firewalls

- A stateless packet filtering FW is investigating each packet on its on merits
- A stateful firewall is an advanced packet filter that keeps track of the state of the network connections going through it
- Whenever a packet arrives to the stateful firewall, it checks whether it matches an on-going connection. If a match is found the packet can pass through



Stateful Firewalls

- A stateful inspecting firewall is not limited to the TCP and IP protocols.
- For known applications it looks at the application protocol as well.
- This enables the firewall to detect when a communication link does something out of the ordinary
- It also enables the firewall to filter out certain parts of the data transmitted.
- For the HTTP protocol it may filter out java scripts
- For the SMTP protocol it may filter out certain types of attachments.

Stateful Filtering rule example

- Log each TCP connection initiated through firewall: SYN segment
- Timeout entries which see no activity for, say, 60 seconds

source address	dest address	source port	dest port	time
222.22.1.7	37.96.87.123	12699	80	14.23.35,6
222.22.93.2	199.1.205.23	37654	80	14.22.58,3
222.22.65.143	203.77.240.43	48712	80	14.23.38,0

- If rule table indicates that stateful table must be checked:
- check to see if there is already a connection in stateful table
- Stateful filters can also remember outgoing UDP segments

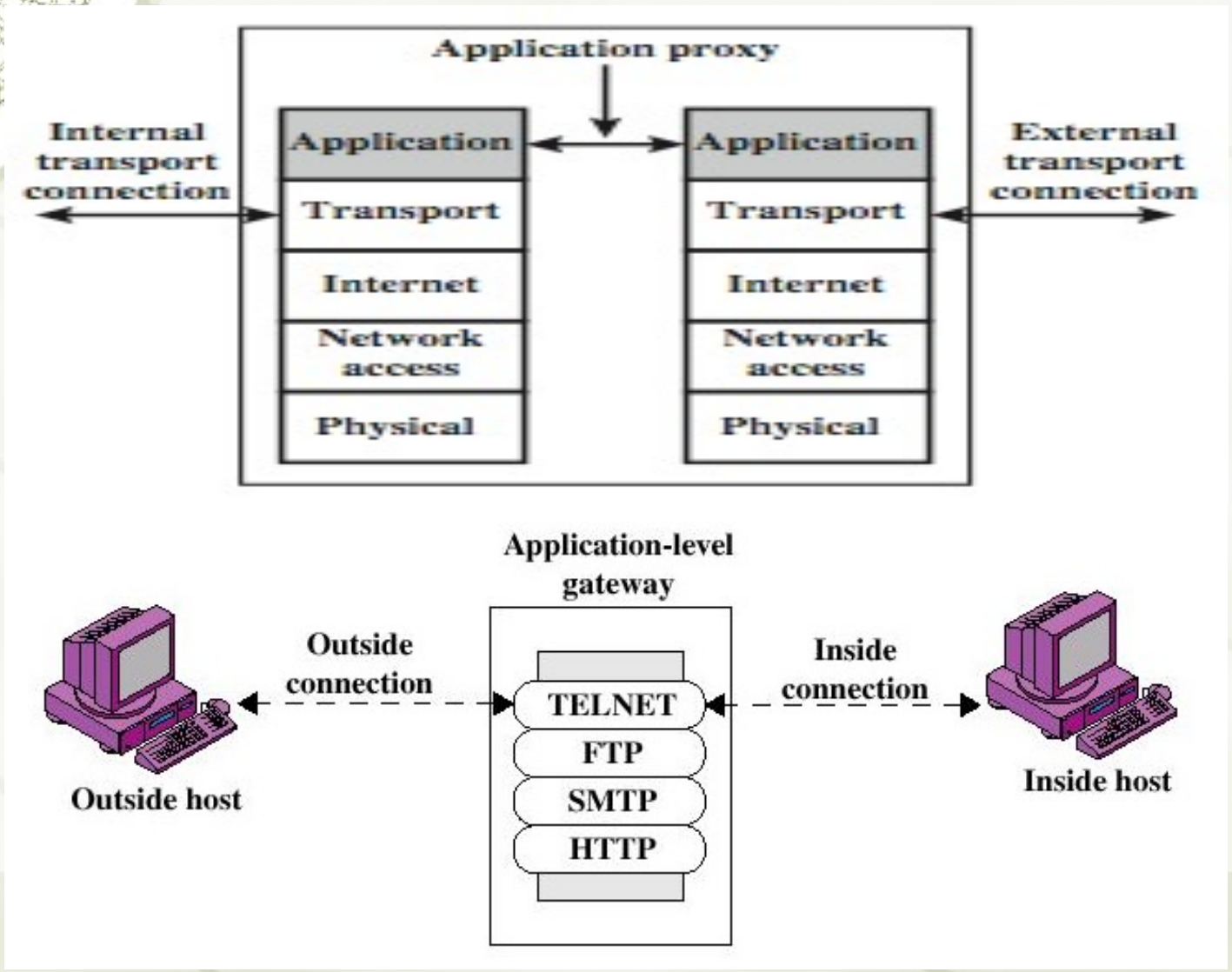
Stateful Filtering rule example

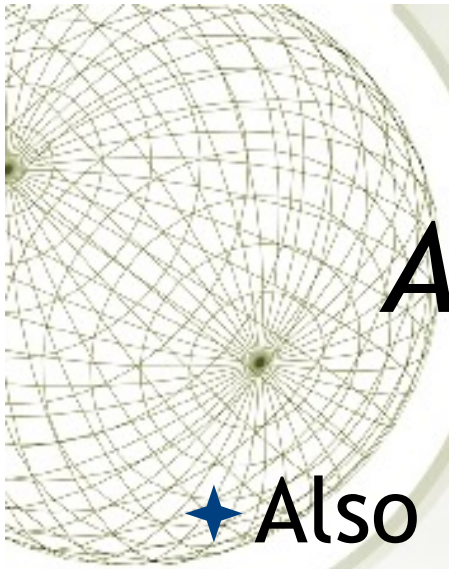
- Packet arrives from outside: SA=37.96.87.123, SP=80, DA=222.22.1.7, DP=12699, SYN=0, ACK=1

action	source address	dest address	proto	source port	dest port	flag bit	check conn.
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	x
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	x
deny	all	all	all	all	all	all	

- Check filter table ➜ check stateful table
- Connection is listed in connection table ➜ let packet through

Application-level Gateway





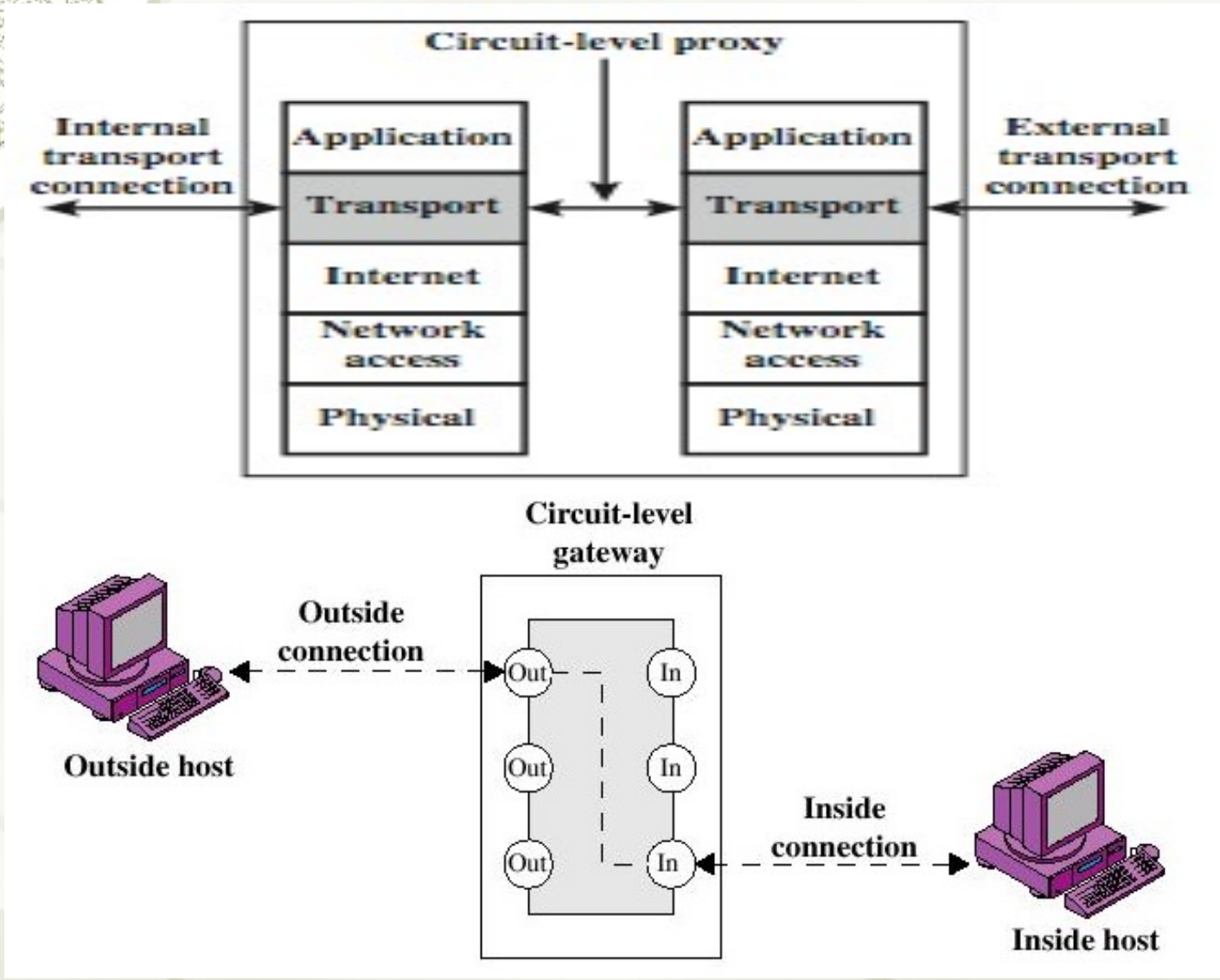
Application-level Gateway

- Also called proxy server
- Acts as a relay of application-level traffic

Application-level Gateway

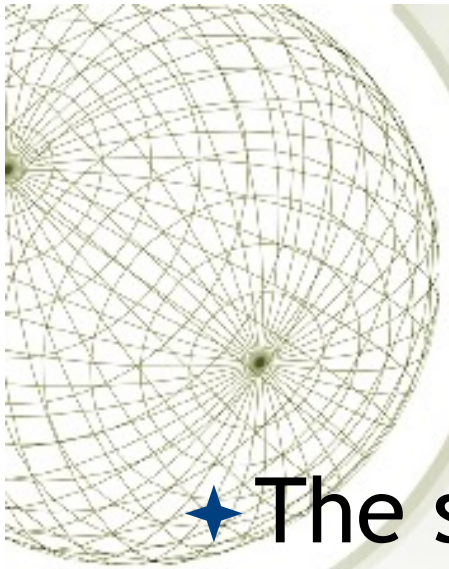
- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)
  - What about not supported protocols?

Circuit-level Gateway



Circuit-level Gateway

- Stand-alone system or
- Specialized function performed by an Application-level Gateway
- Sets up two TCP connections
- The gateway typically relays TCP segments from one connection to the other without examining the contents

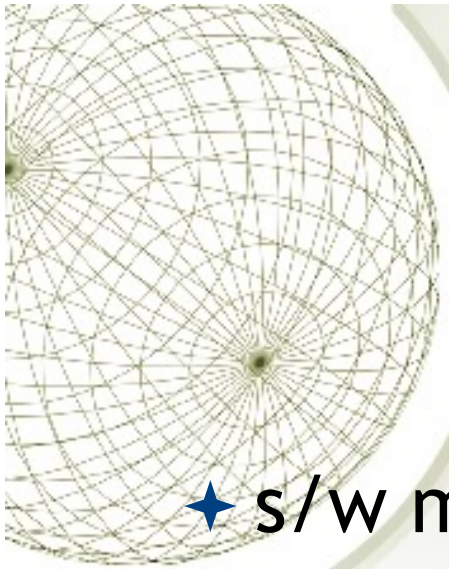


Circuit-level Gateway

- The security function consists of determining which connections will be allowed
- Typically use is a situation in which the system administrator trusts the internal users
- An example is the SOCKS package

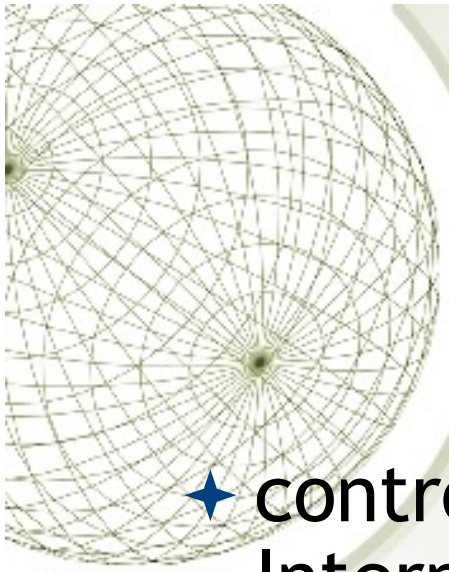
Bastion Host

- A system identified by the firewall administrator as a critical strong point in the network's security
- The bastion host serves as a platform for an application-level or circuit-level gateway



Host-Based Firewalls

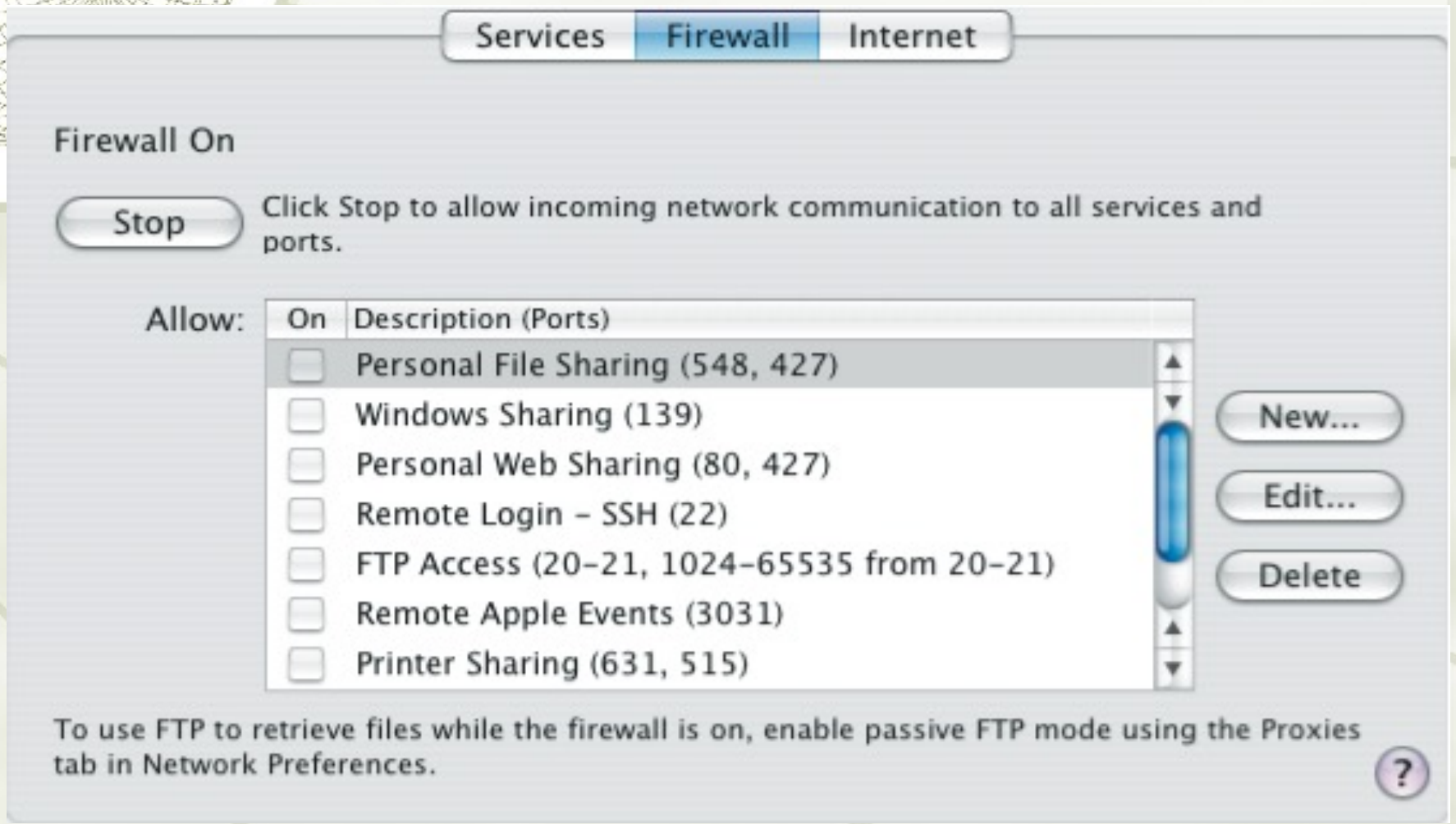
- s/w module used to secure individual host
  - available in many operating systems
  - or can be provided as an add-on package
- used both on servers and separate clients
- advantages:
  - can tailor filtering rules to host environment
  - protection is provided independent of topology
  - provides an additional layer of protection



Personal Firewalls

- controls traffic between PC/workstation and Internet or enterprise network
- a software module on personal computer
- or in home/office DSL/cable/ISP router
- Typically less complex than other firewall types
- primary role to deny unauthorized remote access to the computer
- and monitor outgoing activity for malware

Personal Firewalls

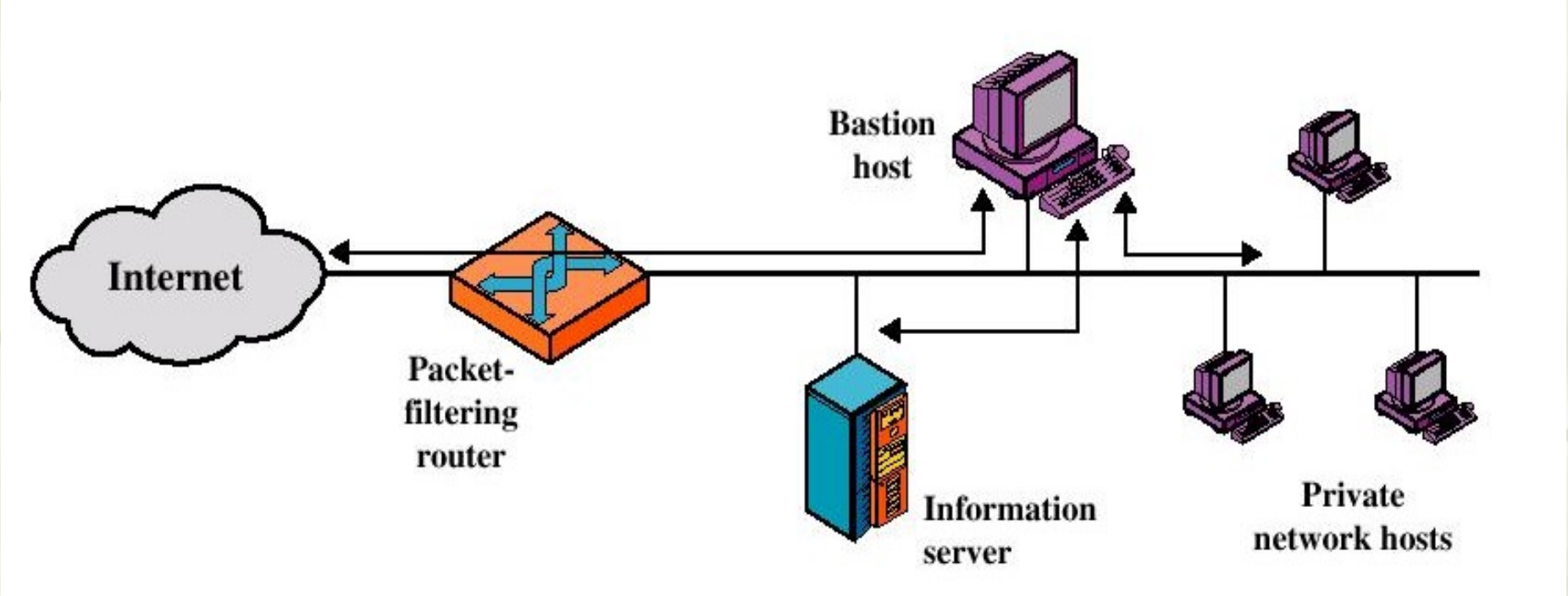


Firewall Configurations

- In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible
- Three common configurations

Firewall Configurations

- Screened host firewall system (single-homed bastion host)

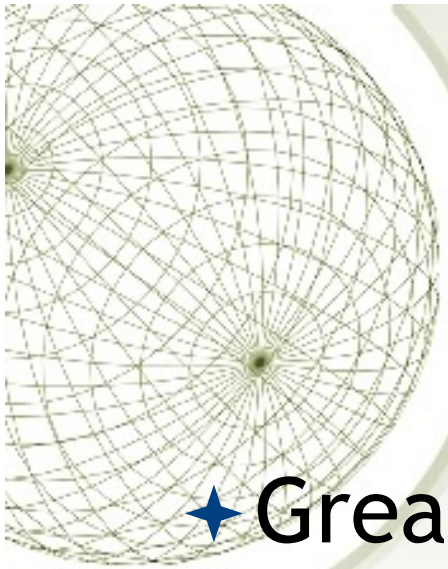


Firewall Configurations

- Screened host firewall, single-homed bastion configuration
- Firewall consists of two systems:
  - A packet-filtering router
  - A bastion host

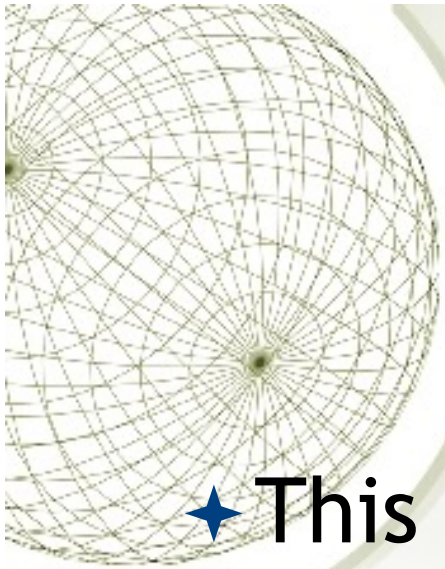
Firewall Configurations

- Configuration for the packet-filtering router:
  - Only packets from and to the bastion host are allowed to pass through the router
- The bastion host performs authentication and proxy functions



Firewall Configurations

- Greater security than single configurations because of two reasons:
  - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
  - An intruder must generally penetrate two separate systems

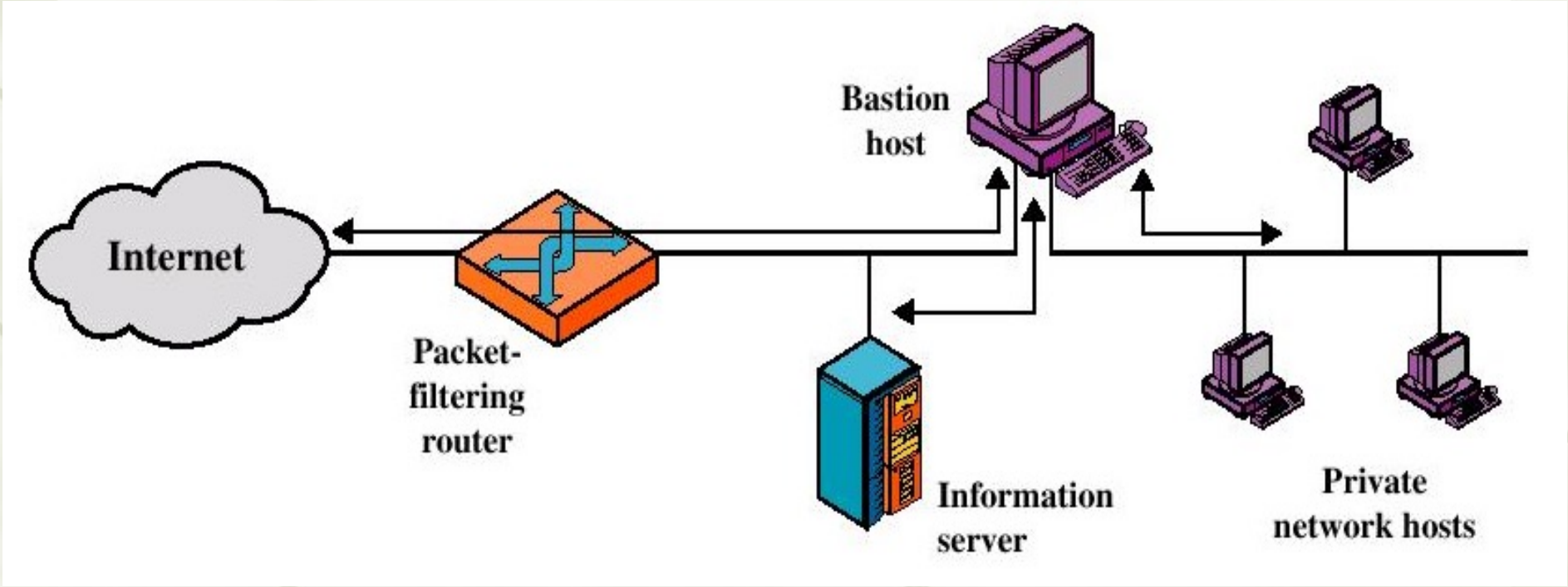


Firewall Configurations

- This configuration also affords flexibility in providing direct Internet access (public information server, e.g. Web server)

Firewall Configurations

- Screened host firewall system (dual-homed bastion host)

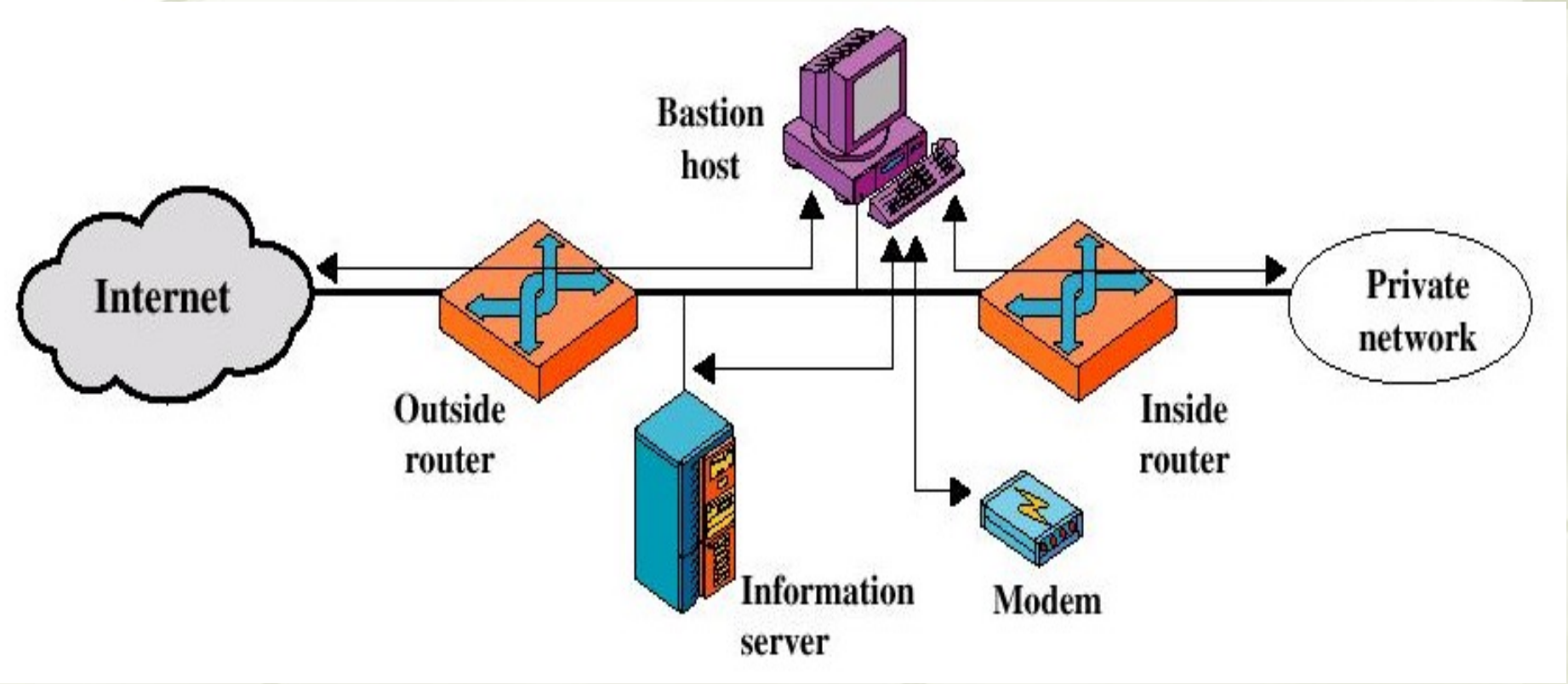


Firewall Configurations

- Screened host firewall, dual-homed bastion configuration
  - The packet-filtering router is not completely compromised
  - Traffic between the Internet and other hosts on the private network has to flow through the bastion host

Firewall Configurations

- Screened-subnet firewall system



Firewall Configurations

- Screened subnet firewall configuration
  - Most secure configuration of the three
  - Two packet-filtering routers are used
  - Creation of an isolated sub-network

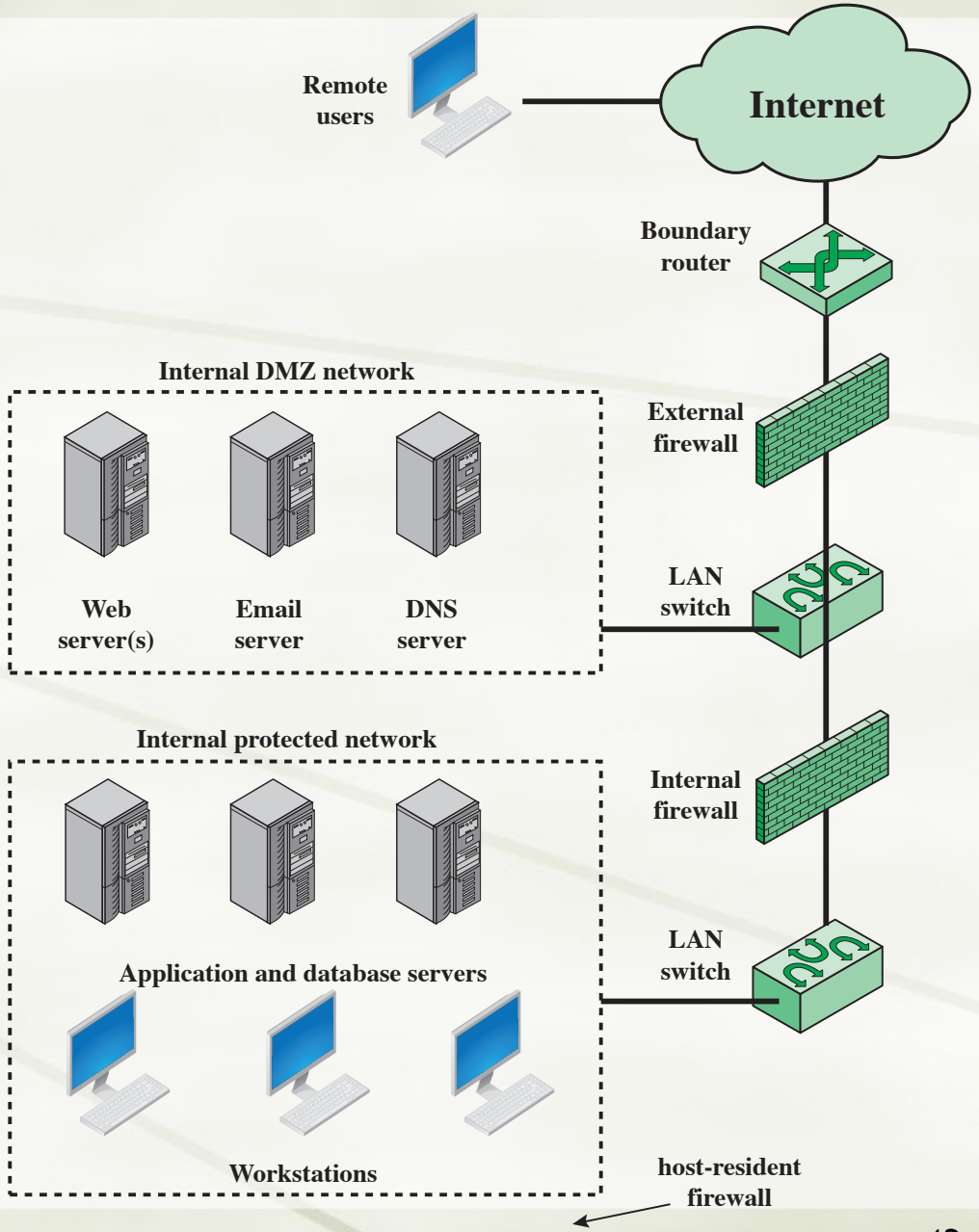
Firewall Configurations

- Advantages:
  - Three levels of defence to thwart intruders
  - The outside router advertises only the existence of the screened subnet to the Internet (internal network is invisible to the Internet)

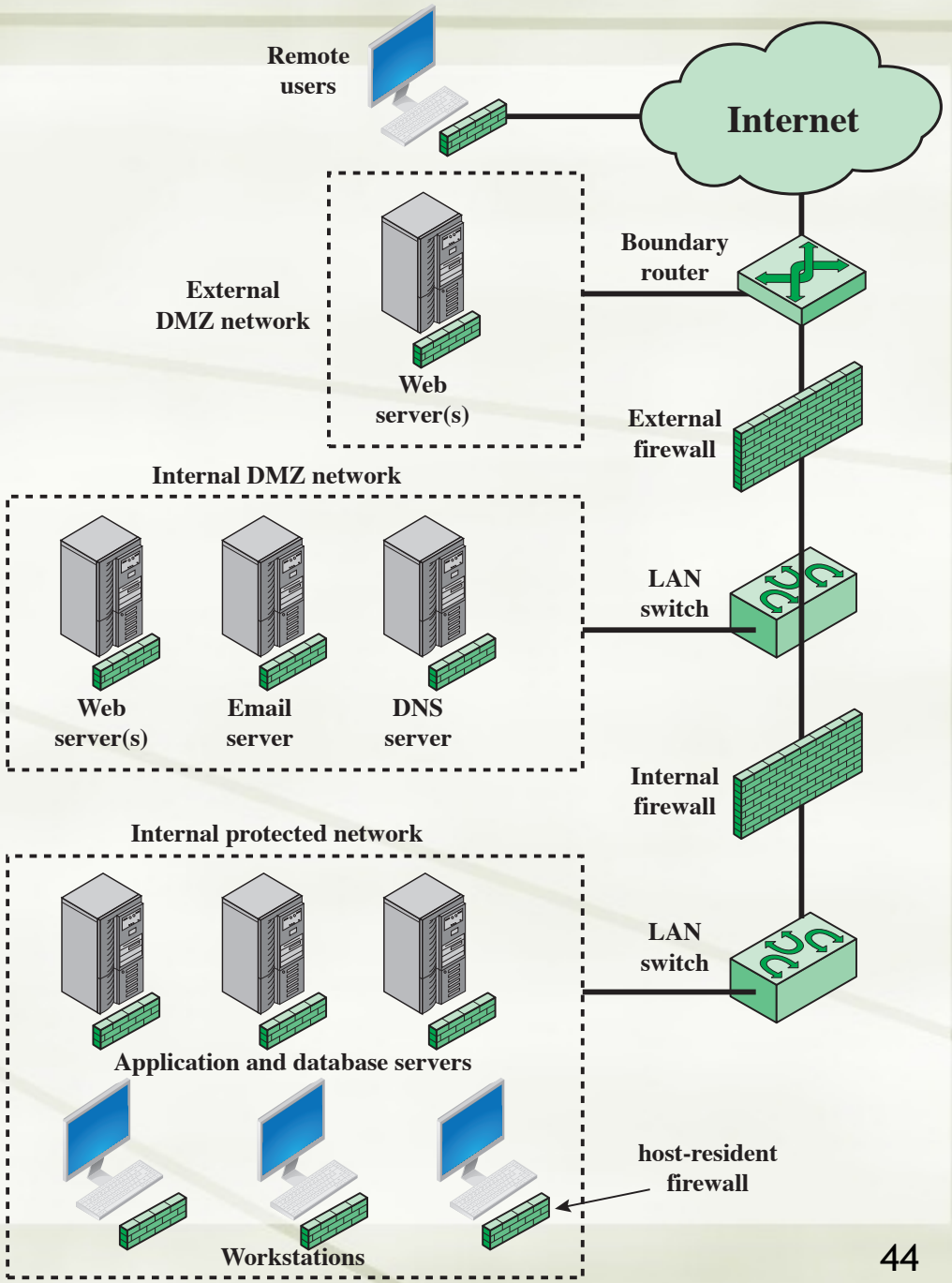
Firewall Configurations

- Advantages:
  - The inside router advertises only the existence of the screened subnet to the internal network (the systems on the inside network cannot construct direct routes to the Internet)

DMZ Networks



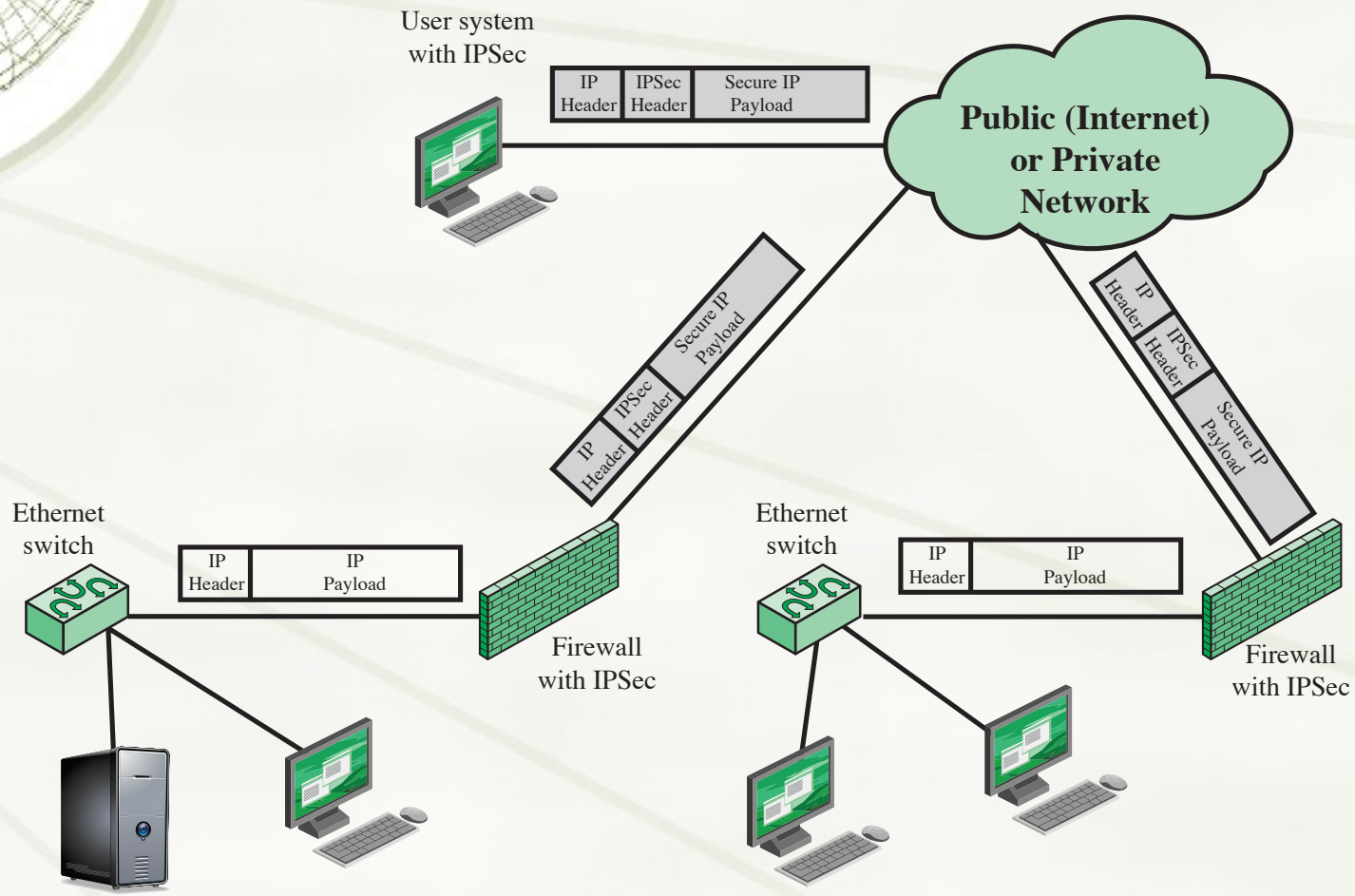
Distributed Firewalls



Combining Firewalls with other functions

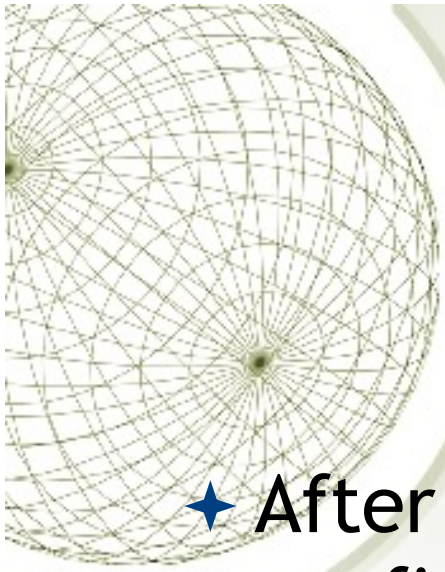
- A firewall may be co-implemented with other functionality such as:
  - VPN
  - IDS/IPS
  - NAT
  - Router
  - Authentication Server
  - Wireless Access Point

Virtual Private Networks



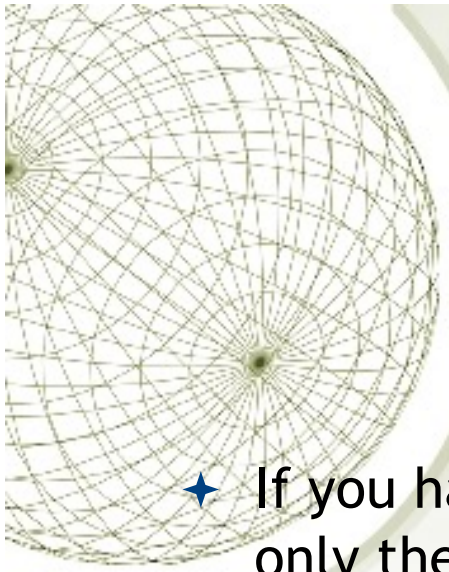
Summary of Firewall Locations and Topologies

- **Host-resident firewall**
  - This category includes personal firewall software and firewall software on servers
  - Can be used alone or as part of an in-depth firewall deployment
- **Screening router**
  - A single router between internal and external networks with stateless or full packet filtering
  - This arrangement is typical for small office/home office (SOHO) applications
- **Single bastion inline**
  - A single firewall device between an internal and external router
  - This is the typical firewall appliance configuration for small-to-medium sized organizations
- **Single bastion T**
  - Similar to single bastion inline but has a third network interface on bastion to a DMZ where externally visible servers are placed
- **Double bastion inline**
  - DMZ is sandwiched between bastion firewalls
- **Double bastion T**
  - DMZ is on a separate network interface on the bastion firewall
- **Distributed firewall configuration**
  - Used by some large businesses and government organizations



Firewall Testing

- After having designed, implemented, and configured your firewall, it is extremely important to test your firewall thoroughly before putting it in use. Eg:
  - Your firewall should not allow any packet from outside the network to go into your internal network if the source address is the same as any host in your internal network.



Firewall Testing

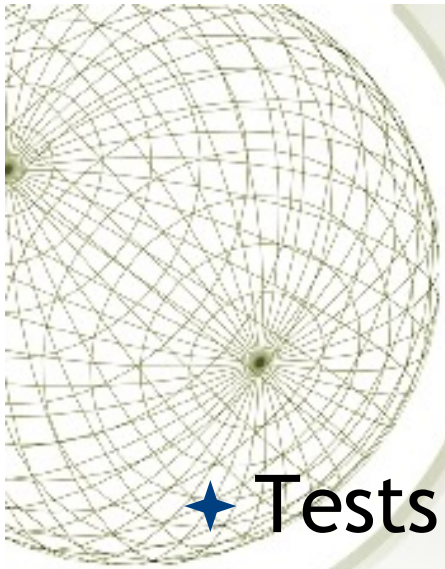
- If you have a proxy firewall, running Squid eg., make sure that only the needed ports are open.
  - Daemons such as Telnetd, FTPd, HTTPd and others should be shut down when they are not needed.
- You may sometimes require the ability to remotely administer your firewall. However, you should consider disabling all remote logins to your internal system.
- It is best to allow only interactive logins at your firewall hosts.
- If you must log in the firewall host from other machines, use only a relatively secure login application, such as SSH with one time passwords.

Firewall Testing

- Regularly testing your firewall system and verifying that it operates properly. In general, a firewall professional has at least to test the following:
  - Host hardware (processor, disk, memory, network interfaces, etc.)
  - Operating system software (booting, console access programs, start-up scripts, etc.)
  - Network interconnection equipment (cables, switches, hubs, routers, APs, etc.)
  - Firewalls
    - To check all possible flaws in the software is difficult and this requires expert knowledge, but you still can use software such as a packet injector and listening sniffer (together with other tools: port canners, system vulnerability checking tools and some hacking tools) to test your firewalls
    - Check if configuration files, log files, audit files are modified by unauthorised people or processes

Firewall Testing

- Exhaustive tests of all the possibilities are expensive and practically not possible
- However we can use boundary tests. Eg.
  - identify boundaries in your packet filtering firewall rules
  - then test the regions immediately adjacent to each boundary



Firewall Testing

- Tests also should be conducted thoroughly:
  - Test the routing configuration, packet filtering rules (including service-specific testing), and logging and alert options separately and together
  - Test the firewall system as a whole (such as hardware/software failure recovery, sufficient log file space, proper archival procedure of logs, performance monitoring)
  - Exercise both normal conditions and abnormal conditions

Firewall Testing Tools

- There is no way that you can manually test a firewall as complete as needed, you need to employ firewall testing tools:
  - Network traffic generators (Eg: SPAK (Send PAcKets), ipsend, etc.)
  - Network monitors (Eg: tcpdump and Network Monitor)
  - Port scanners (Eg: strobe, nmap, etc)
  - Vulnerability detection tools (Eg: COPS, Tiger, ISS, Nessus, SAINT, MacAnalysis, etc.)
  - Intrusion detection systems Snort, Cisco IDS, etc.