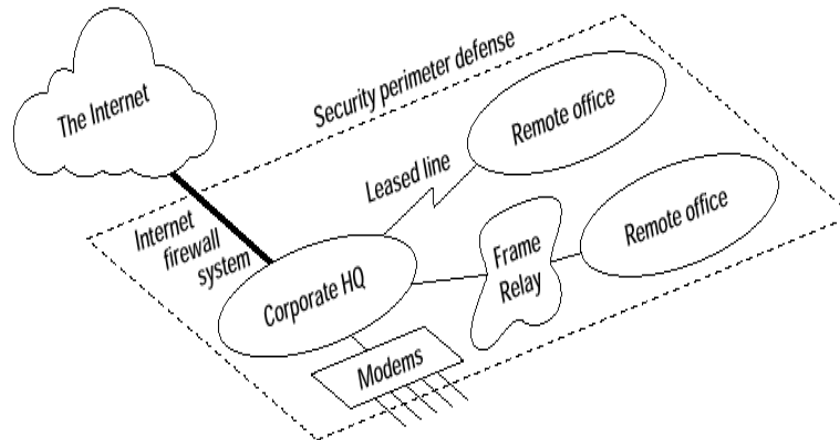


Firewalls



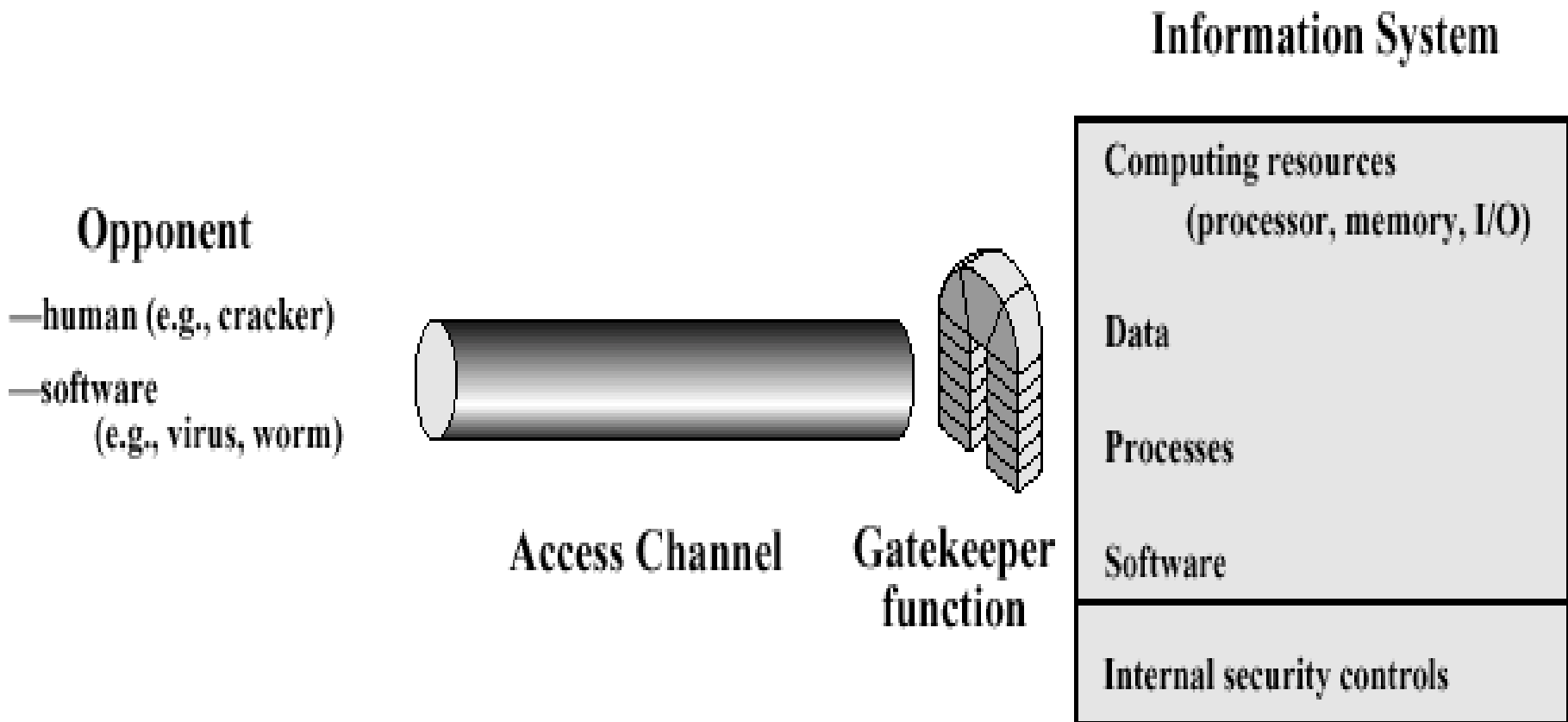
A firewall is a system or group of systems that enforces an access control policy between two networks.

Cars have this part that separates the engine block from the passenger compartment, and it's called a *firewall*. If the car explodes, the firewall protects the passengers.

Lecture Plan

- What is a Firewall?
- Types of Firewalls
- Packet Filtering Firewalls
- Proxy Servers and Application Level Gateways
- More Firewall Configurations
- Firewall performance/connectivity Issues
- Summary

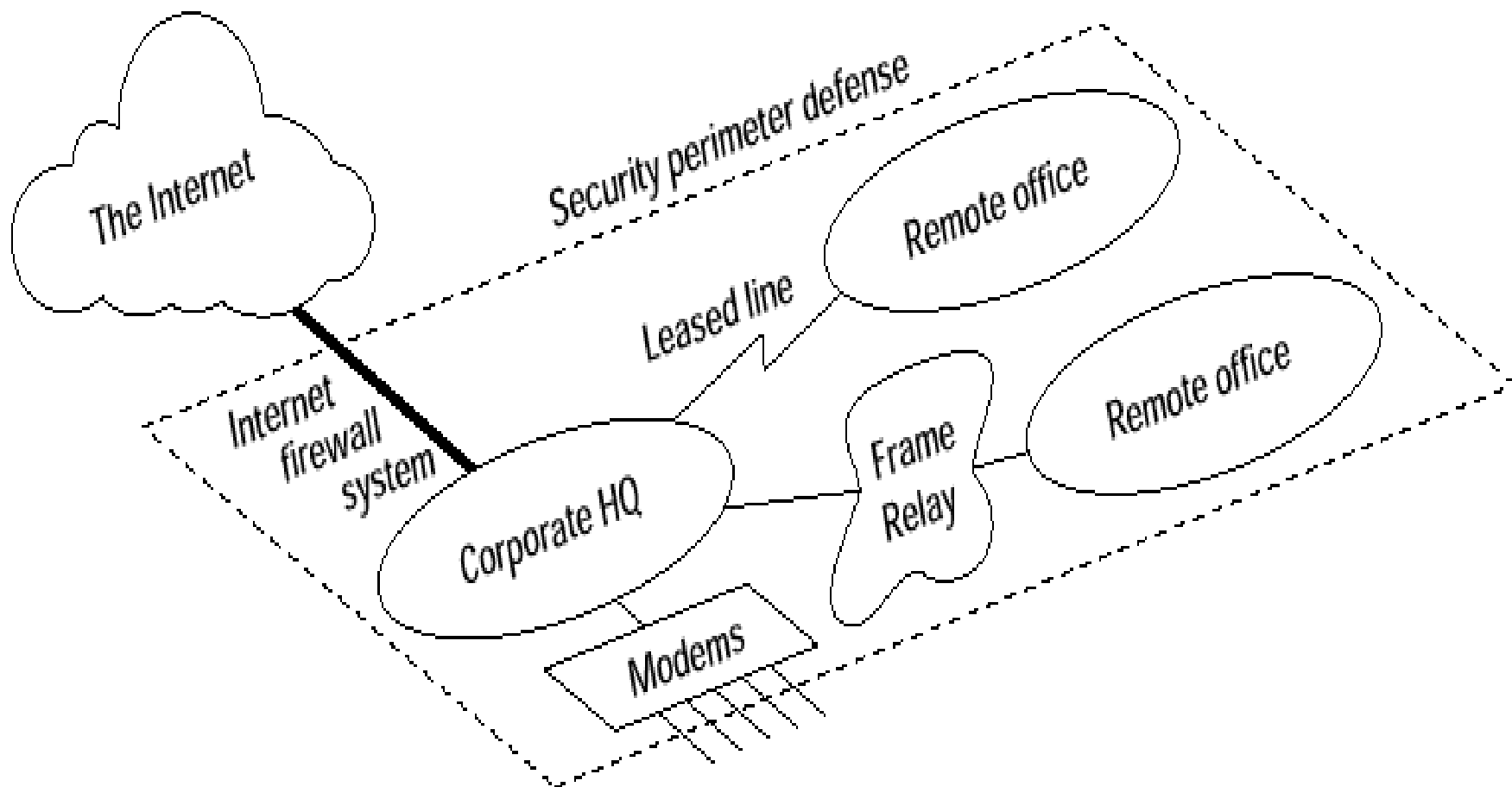
Network Access Security Model



What is a Firewall?

- A firewall is a system designed to prevent unauthorized access to or from a private network.
- Firewalls can be implemented in both hardware and software, or a combination of both.
- Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*.
- All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Firewalls give a Security Perimeter Defense



What Firewalls Do?

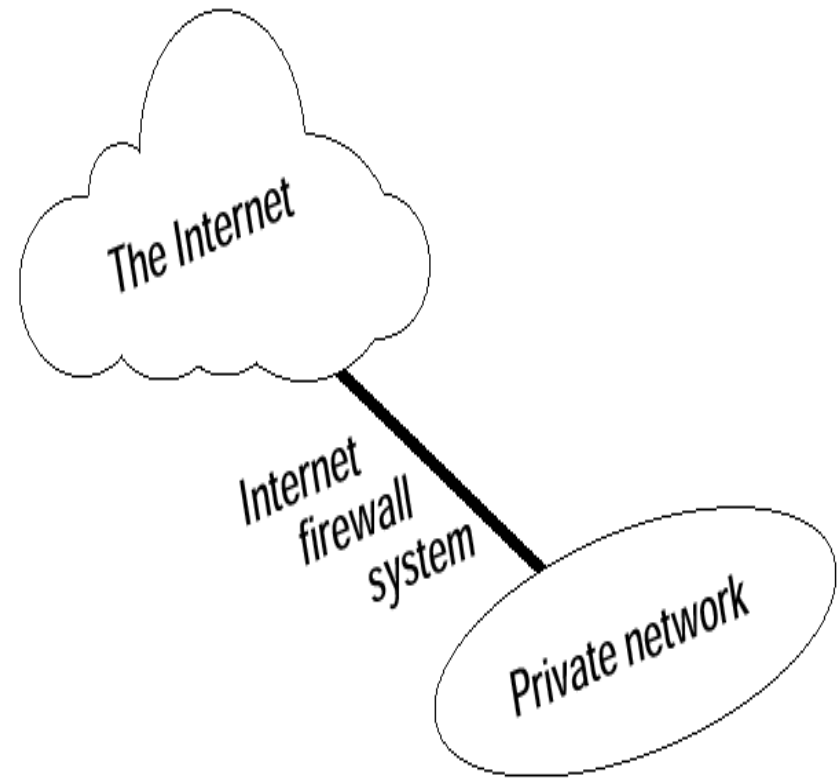
- Probably the most important thing to recognize about a firewall is that it implements an **Access Control Policy**.
- If you don't have a good idea what kind of access you want to permit or deny, or you simply permit someone or some product to configure a firewall based on what they or it think it should do, then they are making policy for your organization as a whole.

What is a network firewall?

- The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms:
 - ⊗ **one which exists to block traffic, and**
 - ⊗ **the other which exists to permit traffic**
- Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic.

Benefits of an Internet Firewall

- Concentrates network security
- Serves as centralized access “choke point”
- Generates security alarms
- Monitors and logs Internet usage
- Good location for Network Address Translator (NAT)
- Good location for WWW and FTP servers



Why Should we Have Firewalls?

- The Internet, like any other society, is plagued with the kind of jerks who enjoy the electronic equivalent of writing on other people's walls with spray paint, tearing their mailboxes off, or just sitting in the street blowing their car horns. Some people try to get real work done over the Internet, and others have sensitive or proprietary data they must protect.
- Usually, a firewall's purpose is to keep the jerks out of your network while still letting you get your job done.

Why Should we Have Firewalls?

- Many traditional-style corporations and data centers have computing security policies and practices that must be adhered to.
- In a case where a company's policies dictate how data must be protected, a firewall is very important, since it is the embodiment of the corporate policy.
- Frequently, the hardest part of hooking to the Internet, if you're a large company, is not justifying the expense or effort, but convincing management that it's safe to do so.
- A firewall provides not only real security - it often plays an important role as a security blanket for management.

Why Should we Have Firewalls?

- Lastly, a firewall can act as your corporate "ambassador" to the Internet.
- Many corporations use their firewall systems as a place to store public information about corporate products and services, files to download, bug-fixes, and so forth.
- Several of these systems have become important parts of the Internet service structure (e.g.: UUnet.uu.net, whitehouse.gov, gatekeeper.dec.com) and have reflected well on their organizational sponsors.

Why Should we Have Firewalls?

- You need to allow users from a protected network, such as your corporate network, to access a public network, such as the Internet, and at the same time, to make available to this public network the services and products of the company.

Classes of Firewalls

- Conceptually, there are two classes of firewalls:
 - ⊗ Network Level Firewall
 - ⊗ Application Level Firewall
- They are not as different as you might think, and latest technologies are blurring the distinction to the point where it's no longer clear if either one is “better” or “worse.”
- As always, you need to be careful to pick the type that meets your needs.

There are several types of firewall techniques:

■ Network Level Firewall

- ❑ Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP_spoofing.
- ❑ Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

■ Application Level Firewall

- ❑ Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
- ❑ Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

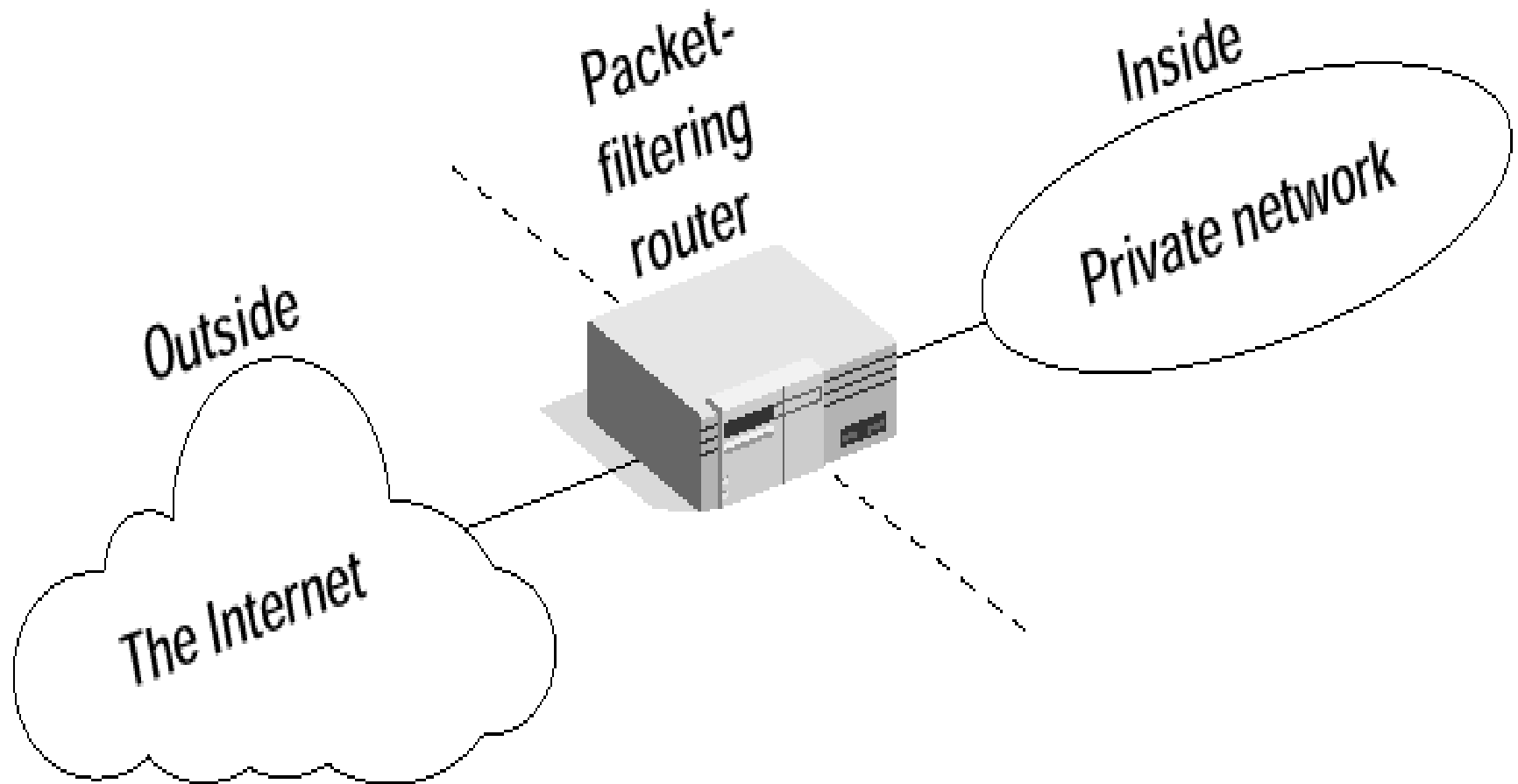
Hybrid Firewalls

- In practice, many firewalls use two or more of these techniques in concert.
- A firewall is considered a first line of defense in protecting private information.
- For greater security, data can be encrypted.

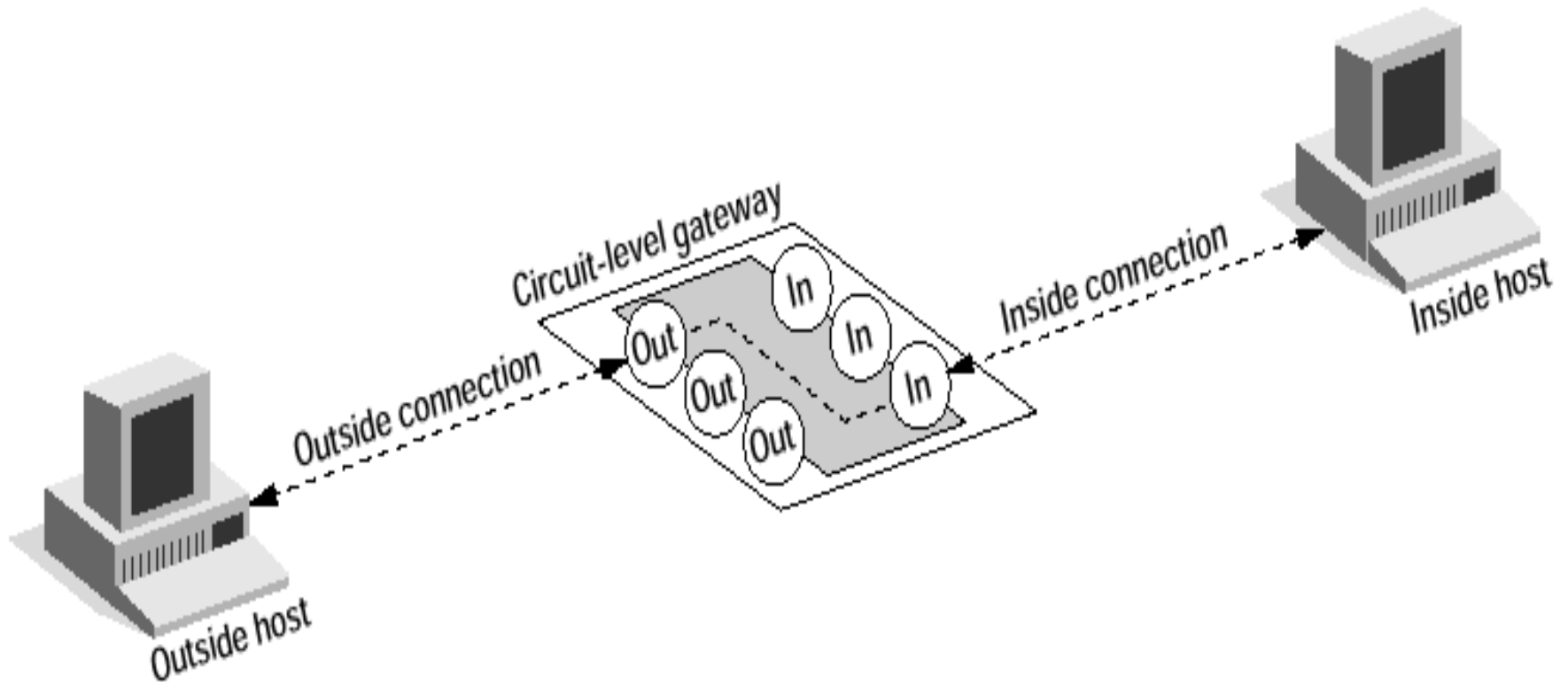
Network Level Firewalls

- **Network level firewalls** generally make their decisions based on the source, destination addresses and ports in individual IP packets. A simple router is the "traditional" network level firewall, since it is not able to make particularly sophisticated decisions about what a packet is actually talking to or where it actually came from. Modern network level firewalls have become increasingly sophisticated, and now maintain internal information about the state of connections passing through them, the contents of some of the data streams, and so on. One thing that's an important distinction about many network level firewalls is that they route traffic directly through them, so to use one you usually need to have a validly assigned IP address block. Network level firewalls tend to be very fast and tend to be very transparent to users.

Packet-Filtering Router Firewall



Circuit-Level Gateway



What is Packet Filtering?

- Packet Filtering means controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP addresses of the source and destination.
- Packet filtering is one technique, among many, for implementing security firewalls.

What Packet Filters can do

...

-
- By using existing information in packet headers, routers can provide system administrators a facility to manage network connections between computers.
 - ⊗ host address
 - ⊗ network number
 - ⊗ interface
 - ⊗ direction
 - ⊗ protocol
 - ⊗ port number
 - are parameters that may be used to implement an access control policy.

Application level firewalls

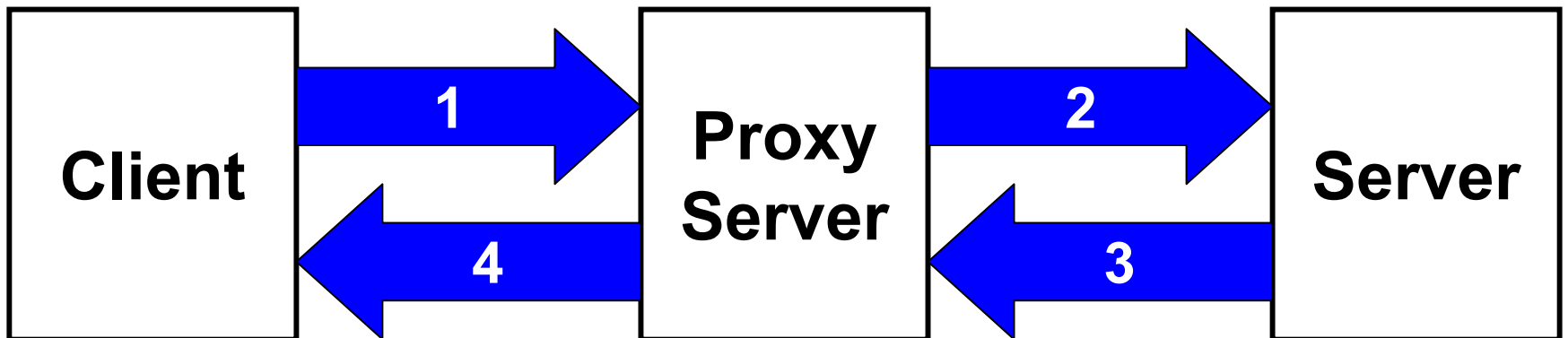
- **Application level firewalls** generally are hosts running proxy servers, which permit no traffic directly between networks, and which perform elaborate logging and auditing of traffic passing through them. Since the proxy applications are software components running on the firewall, it is a good place to do lots of logging and access control. Application level firewalls can be used as network address translators, since traffic goes in one "side" and out the other, after having passed through an application that effectively masks the origin of the initiating connection. Having an application in the way in some cases may impact performance and may make the firewall less transparent. Early application level firewalls such as those built using the TIS firewall toolkit, are not particularly transparent to end users and may require some training. Modern application level firewalls are often fully transparent. Application level firewalls tend to provide more detailed audit reports and tend to enforce more conservative security models than network level firewalls.

What are Proxy Servers?

- A proxy server (sometimes referred to as an application gateway or forwarder) is an application that mediates traffic between a protected network and the Internet. Proxies are often used instead of router-based traffic controls, to prevent traffic from passing directly between networks.
- Many proxies contain extra logging or support for user authentication. Since proxies must "understand" the application protocol being used, they can also implement protocol specific security (e.g., an FTP proxy might be configurable to permit incoming FTP and block outgoing FTP).

Proxy Acts as ...

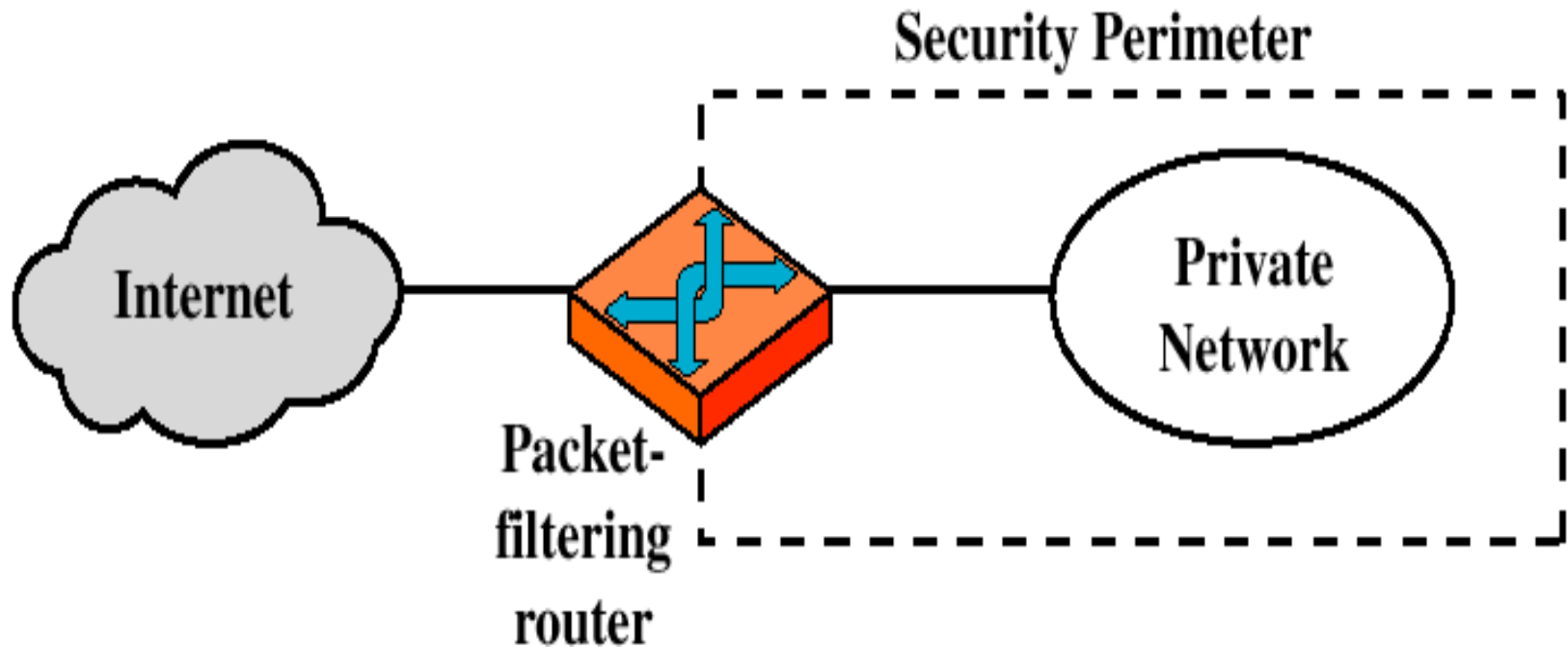
- Proxy acts as a server to the client and as a client to the server
- Proxies in effect break up the connection into two separate connections
- The server talks to the client, the client talks to the proxy server only



Proxy Servers are Application Specific

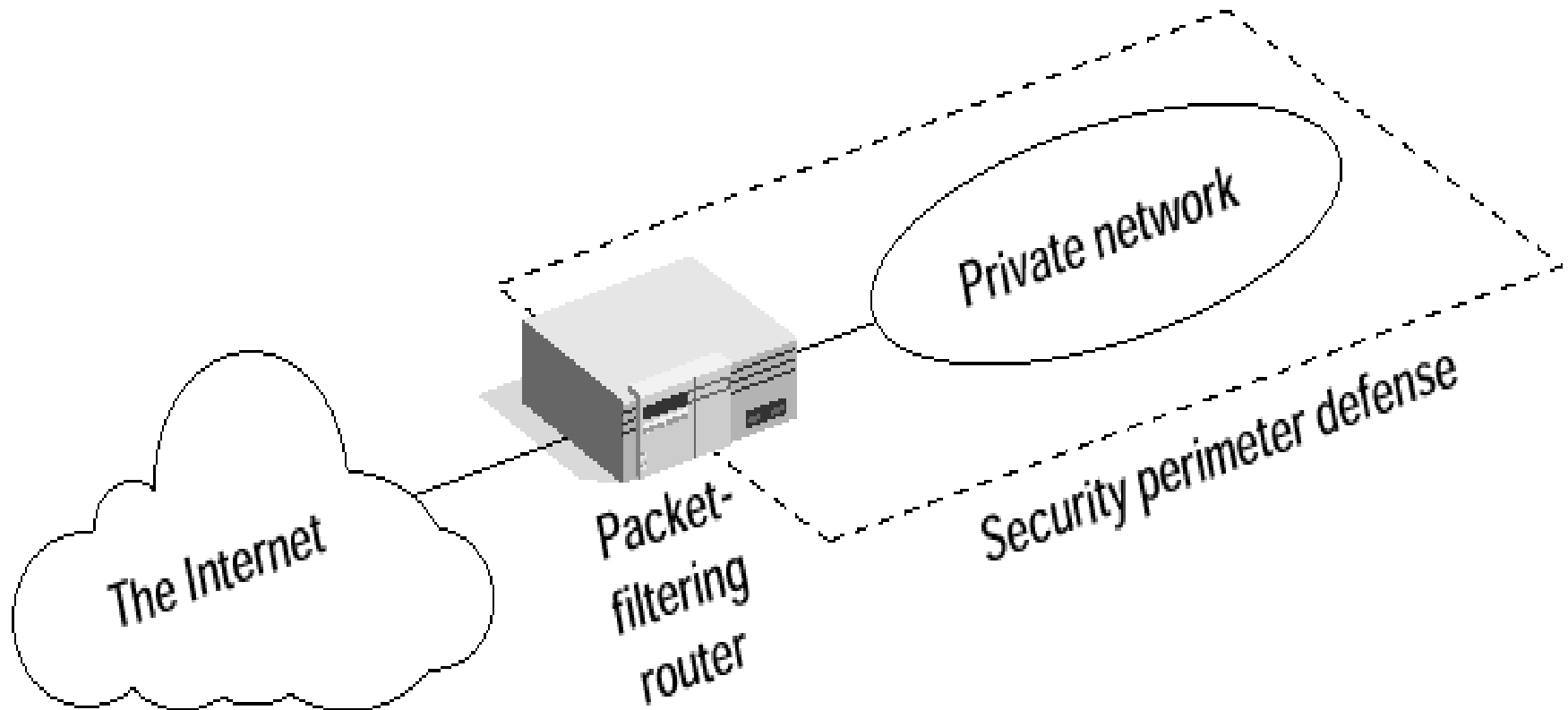
- Proxy servers are application specific. In order to support a new protocol via a proxy, a proxy must be developed for it.
 - ⊗ One popular set of proxy servers is the TIS Internet Firewall Toolkit (“FWTK”) which includes proxies for Telnet, rlogin, FTP, X-Window, http/Web, and NNTP/Usenet news.
 - ⊗ SOCKS is a generic proxy system that can be compiled into a client-side application to make it work through a firewall. Its advantage is that it's easy to use, but it doesn't support the addition of authentication hooks or protocol specific logging. For more information on SOCKS, see <http://www.socks.nec.com/>

Packet-filtering Router

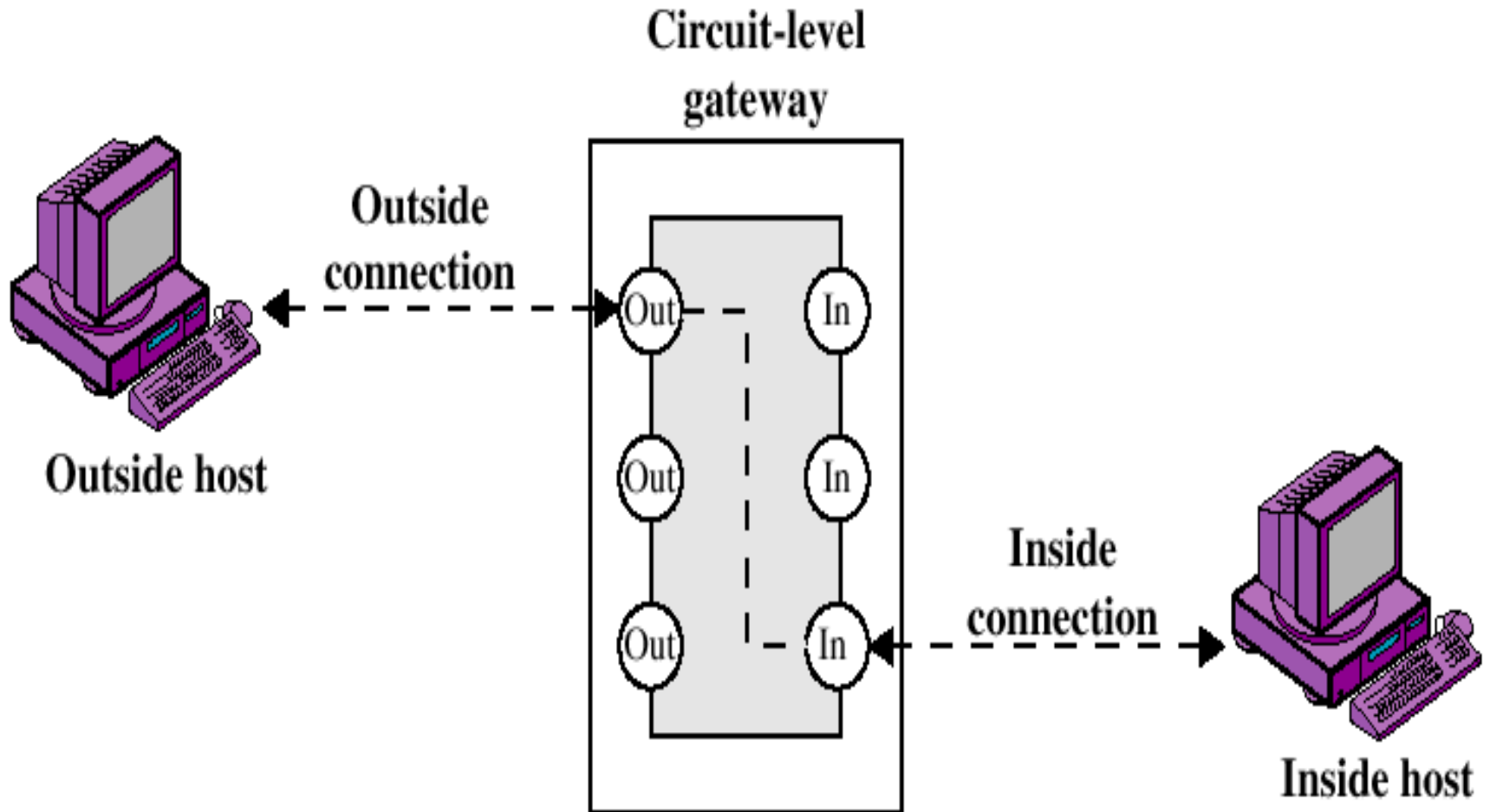


The packet-filtering rules allow a router to permit or deny traffic based on a specific service, since most service listeners reside on well-known TCP/UDP port numbers. For example, a Telnet server listens for remote connections on TCP port 23 and an SMTP server listens for incoming connections on TCP port 25.

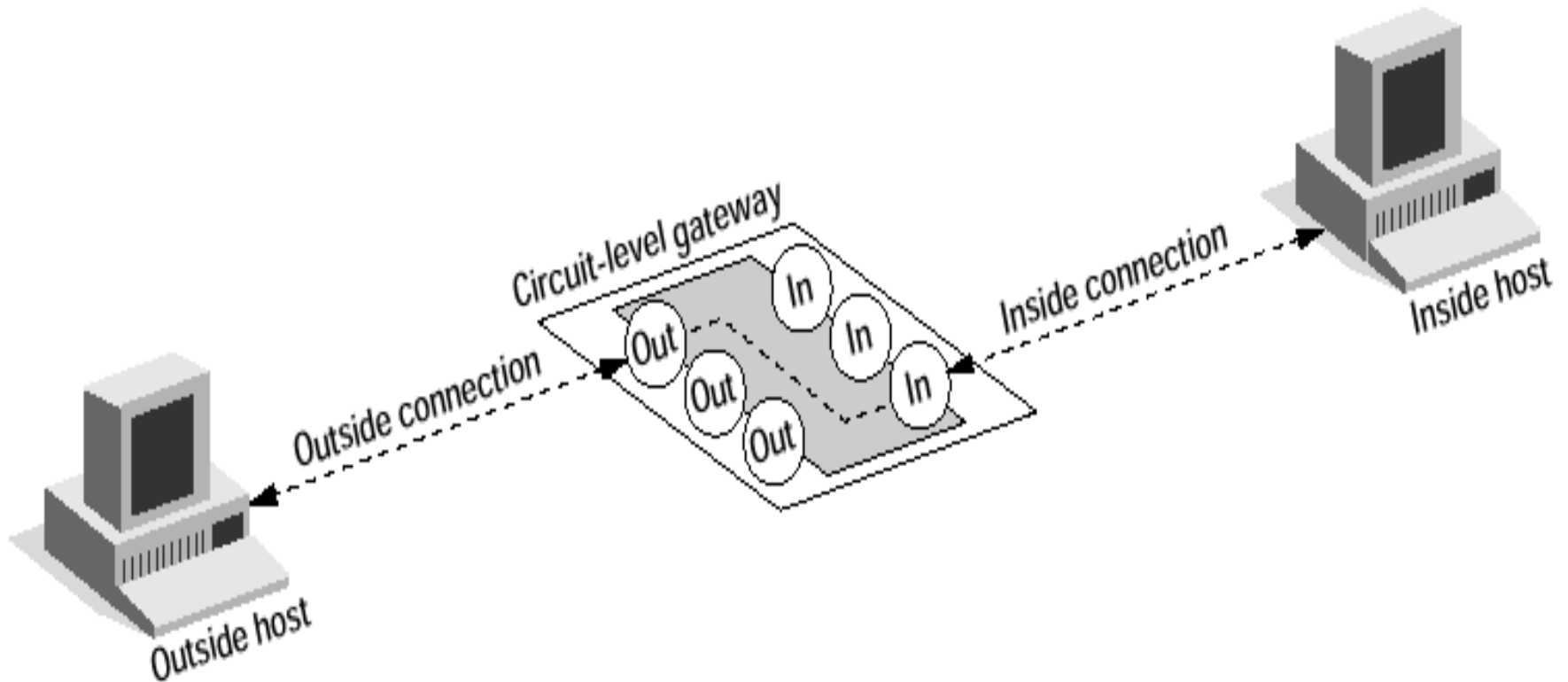
Packet-Filtering Router



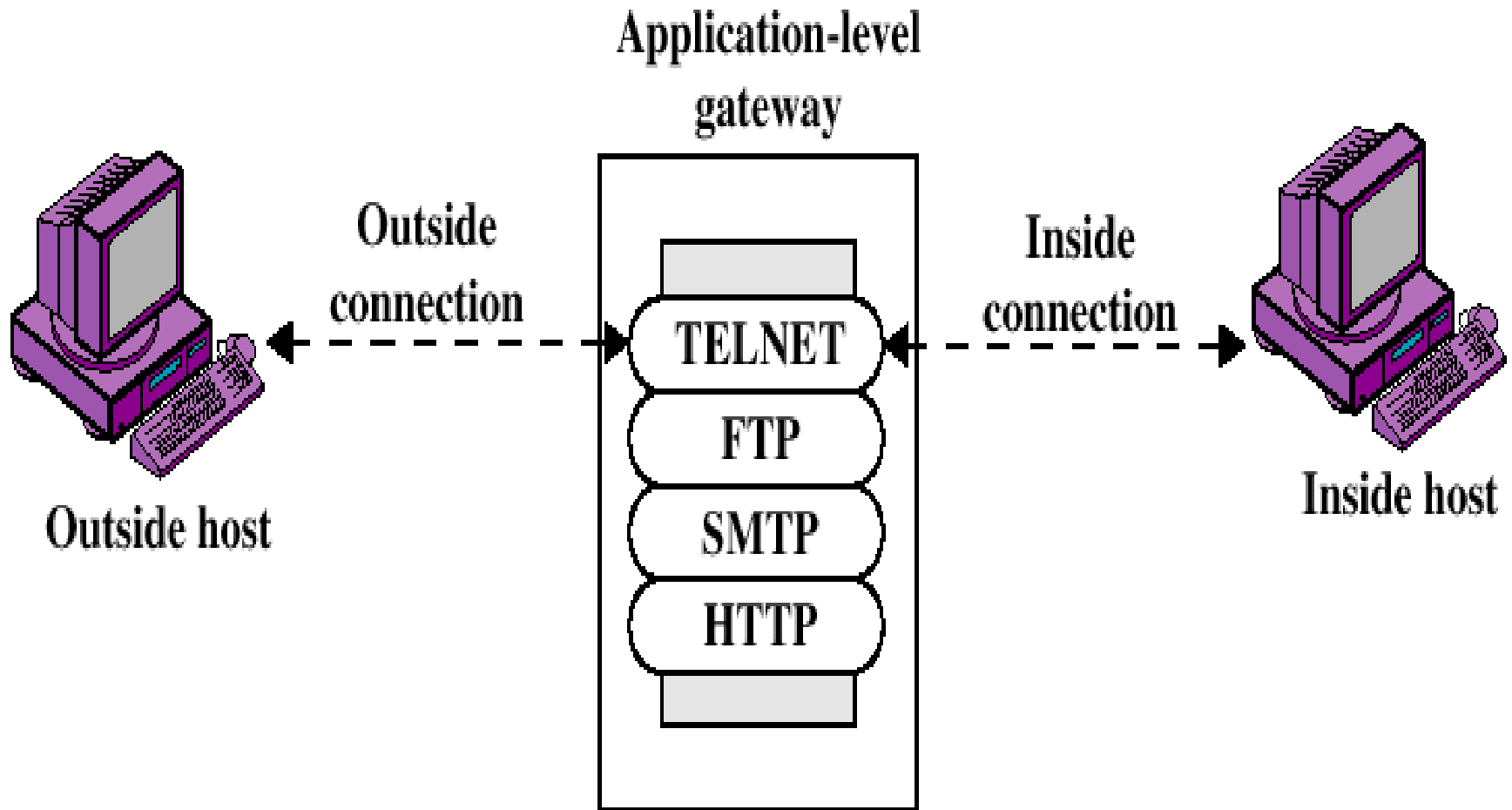
Circuit-level gateway



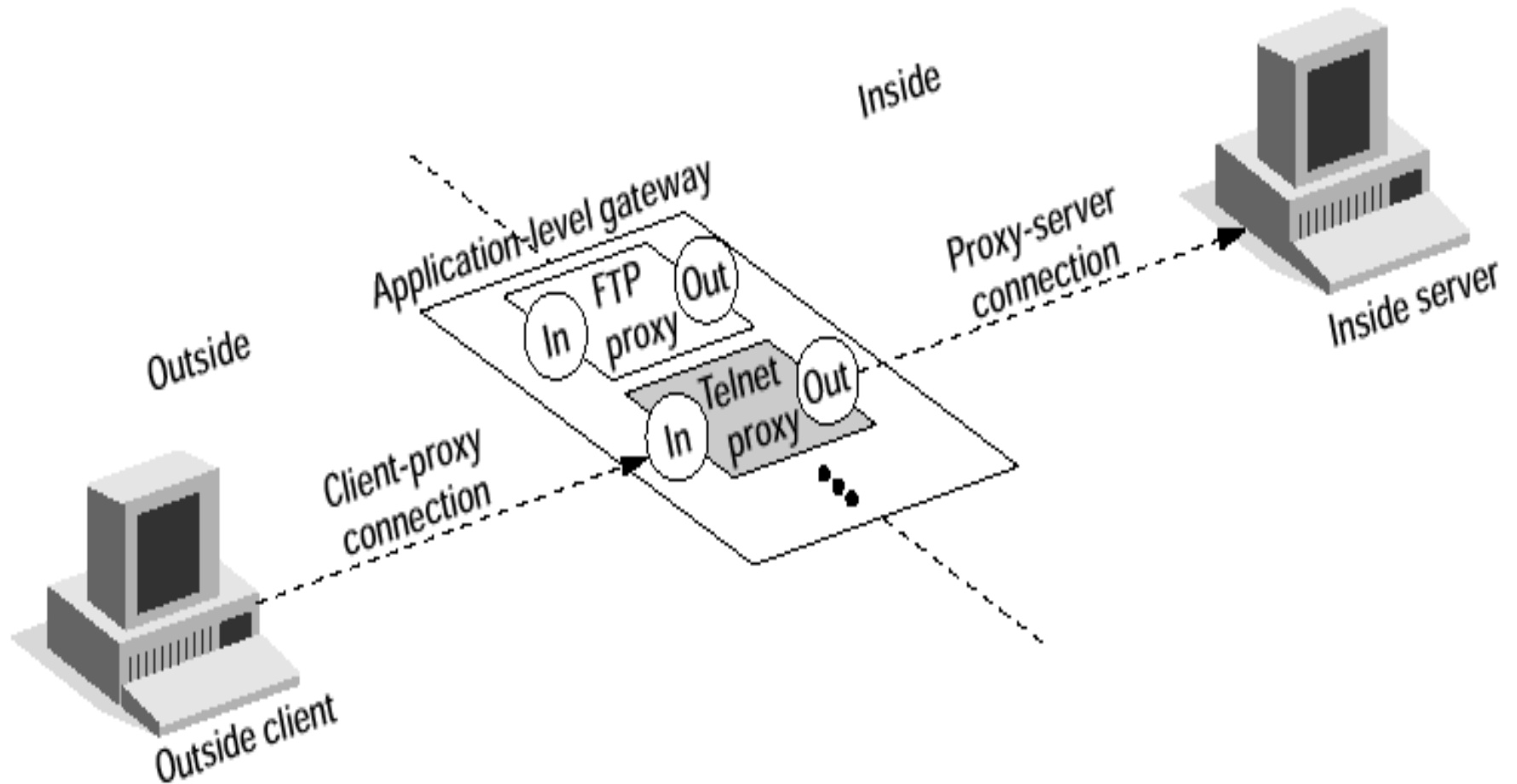
Circuit-Level Gateway



Application-level Gateway

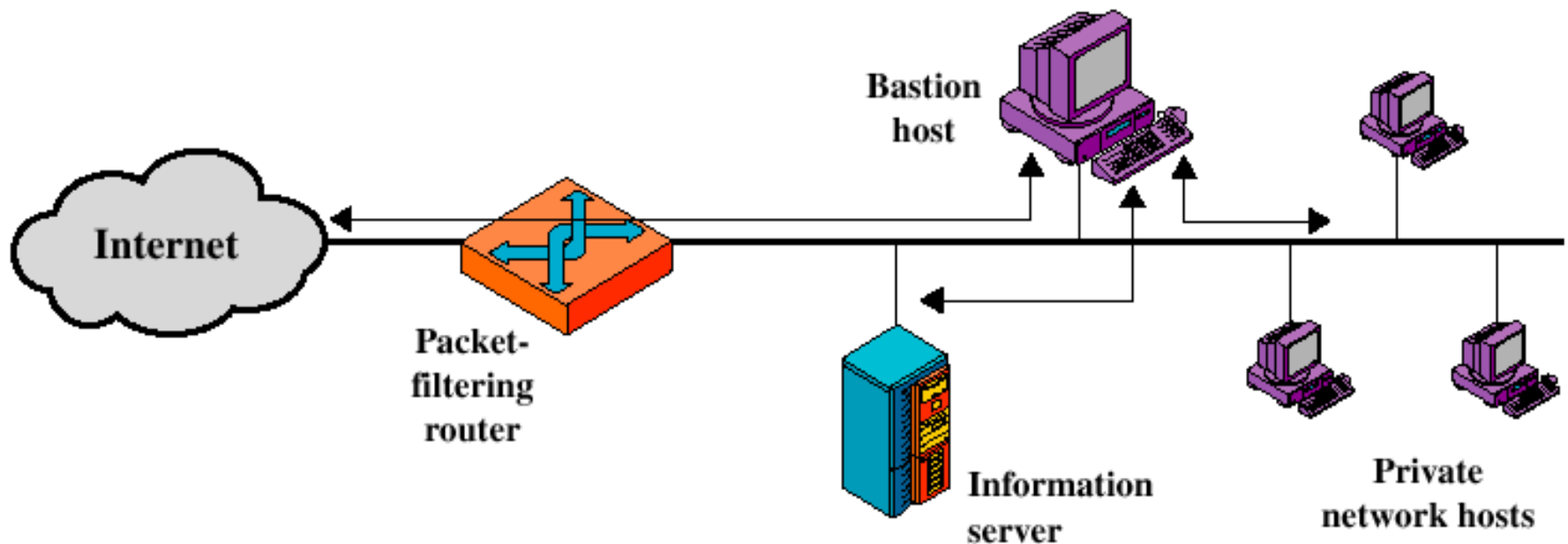


Telnet Proxy

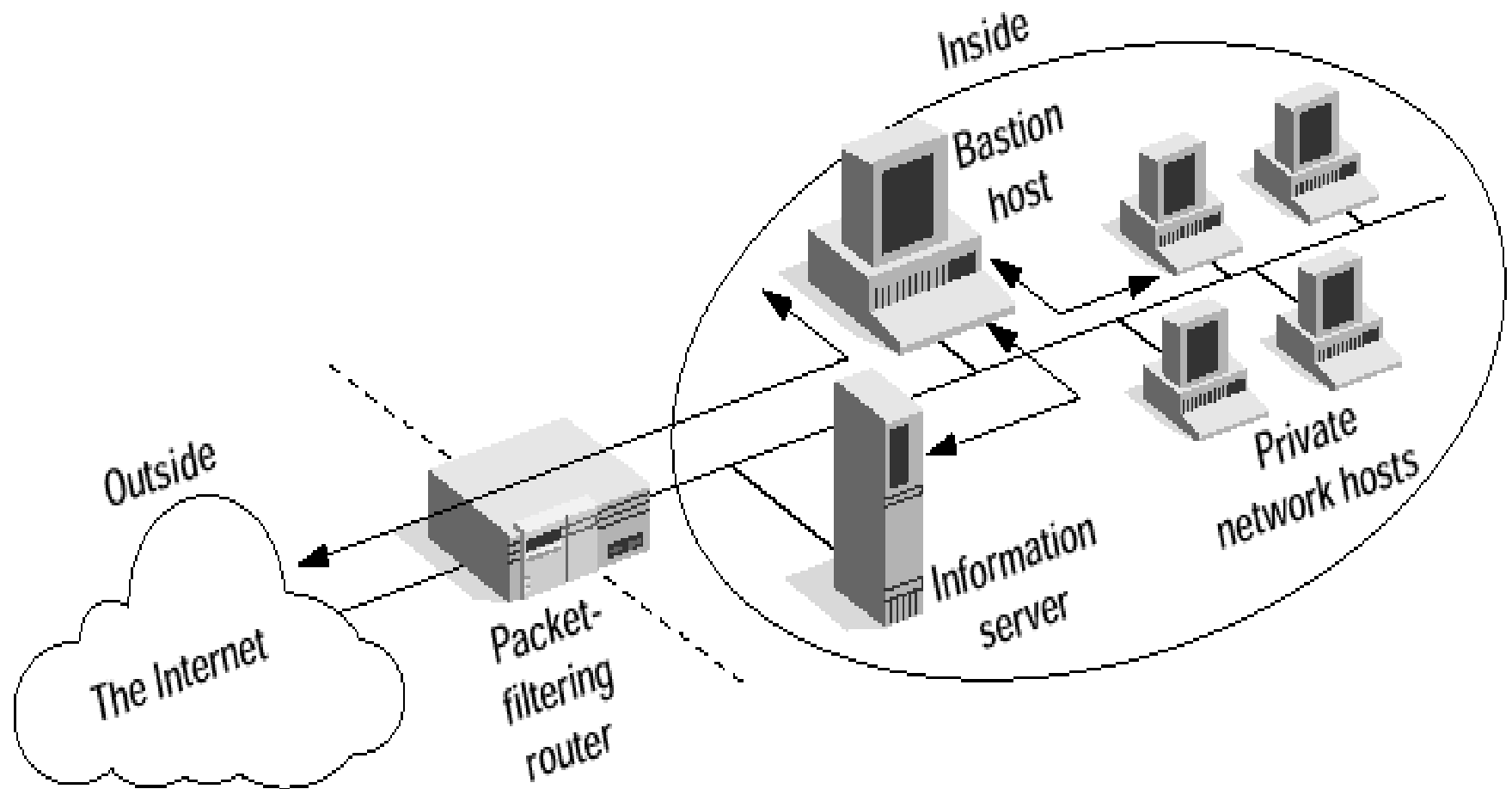


Screened host firewall system (single-homed bastion host)

- Implements both a Network Level Firewall (Packet Filtering Router) and Application Level Firewall (Bastion Host)
- Outside computers can only access the Bastion Host
- Inside computers may or may not use the Bastion Host to access outside network resources

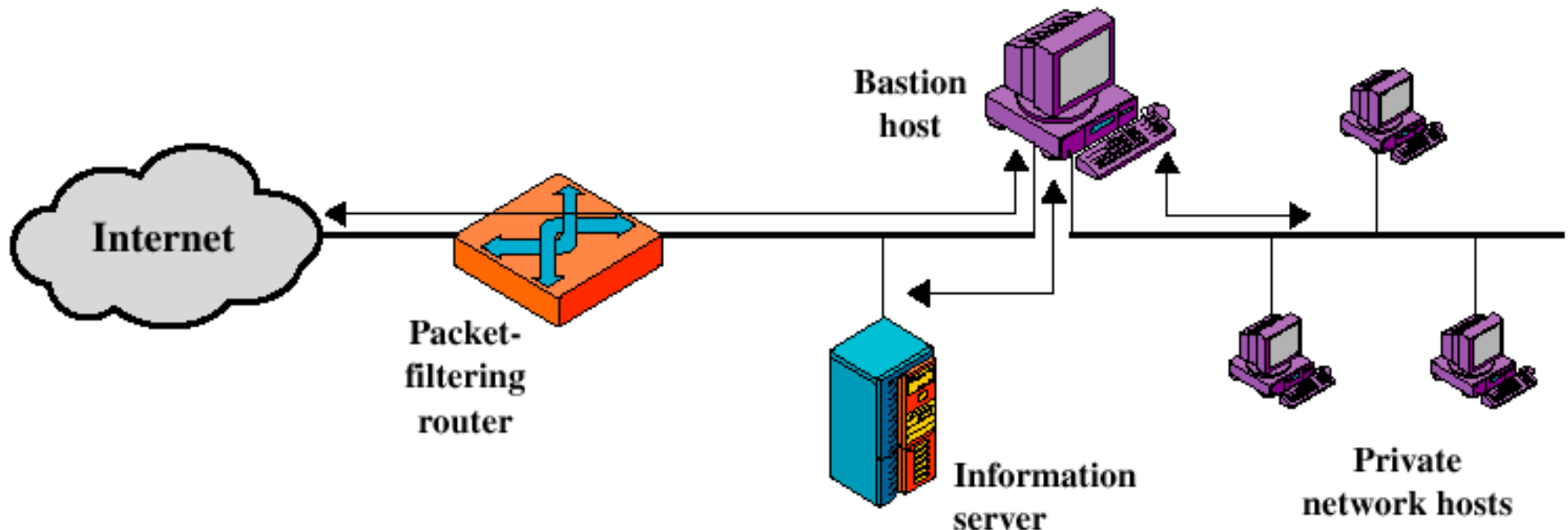


Screened Host Firewall System (Single-Homed Bastion Host)

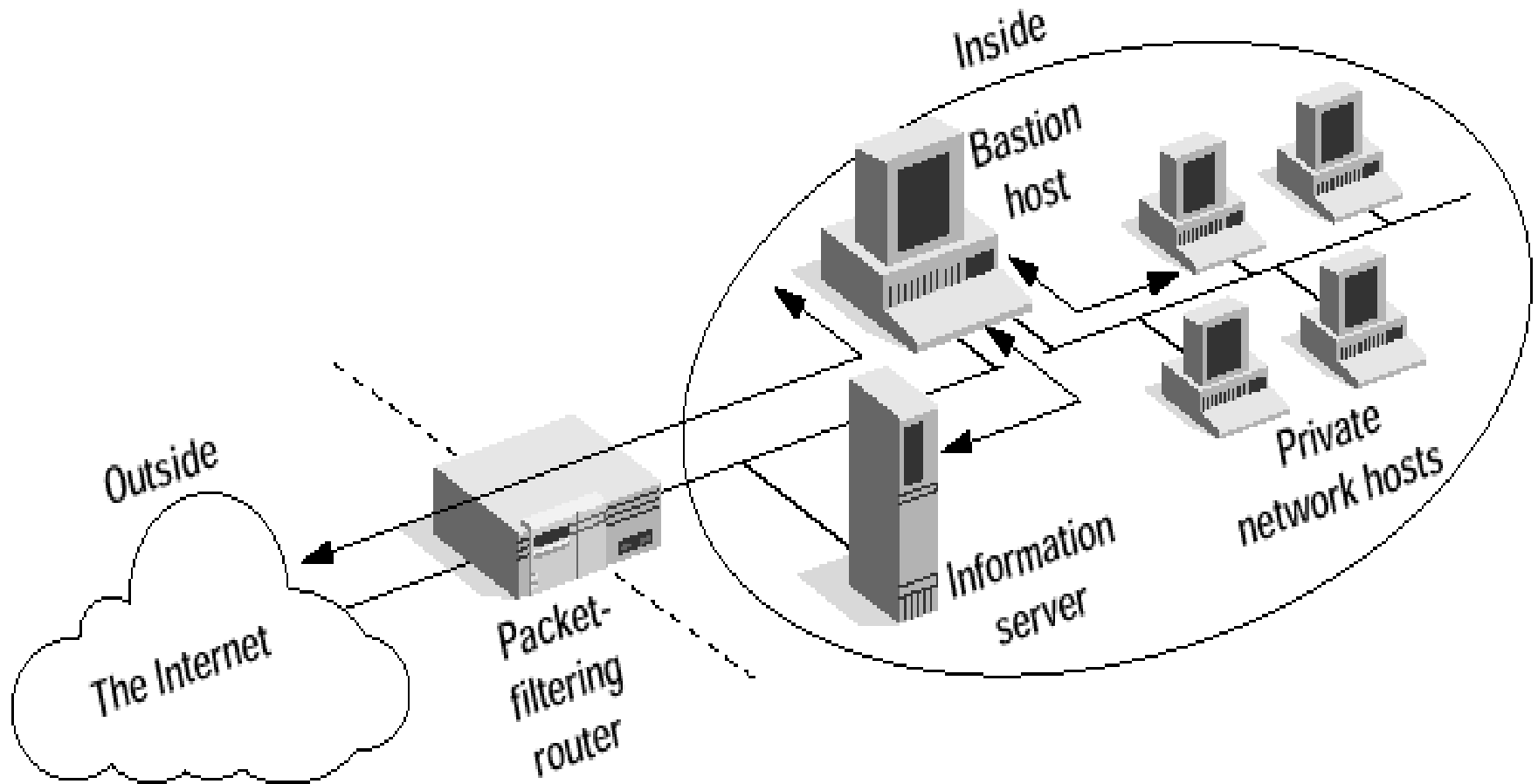


Screened host firewall system (dual-homed bastion host)

- Inside hosts are forced to use the proxy services of the Bastion Host to access Internet
- IP forwarding is disabled on the Bastion Host
- outside computers are allowed to access only the Bastion Host or possibly the Information Server

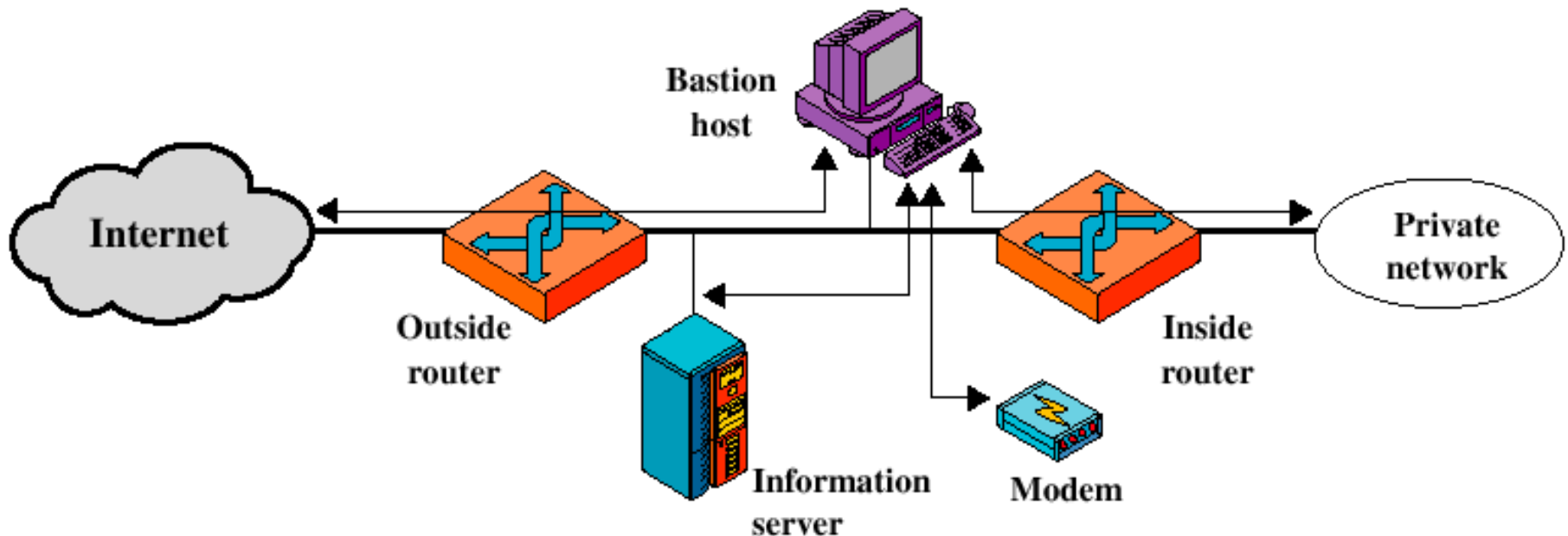


Screened Host Firewall System (Dual-Homed Bastion Host)

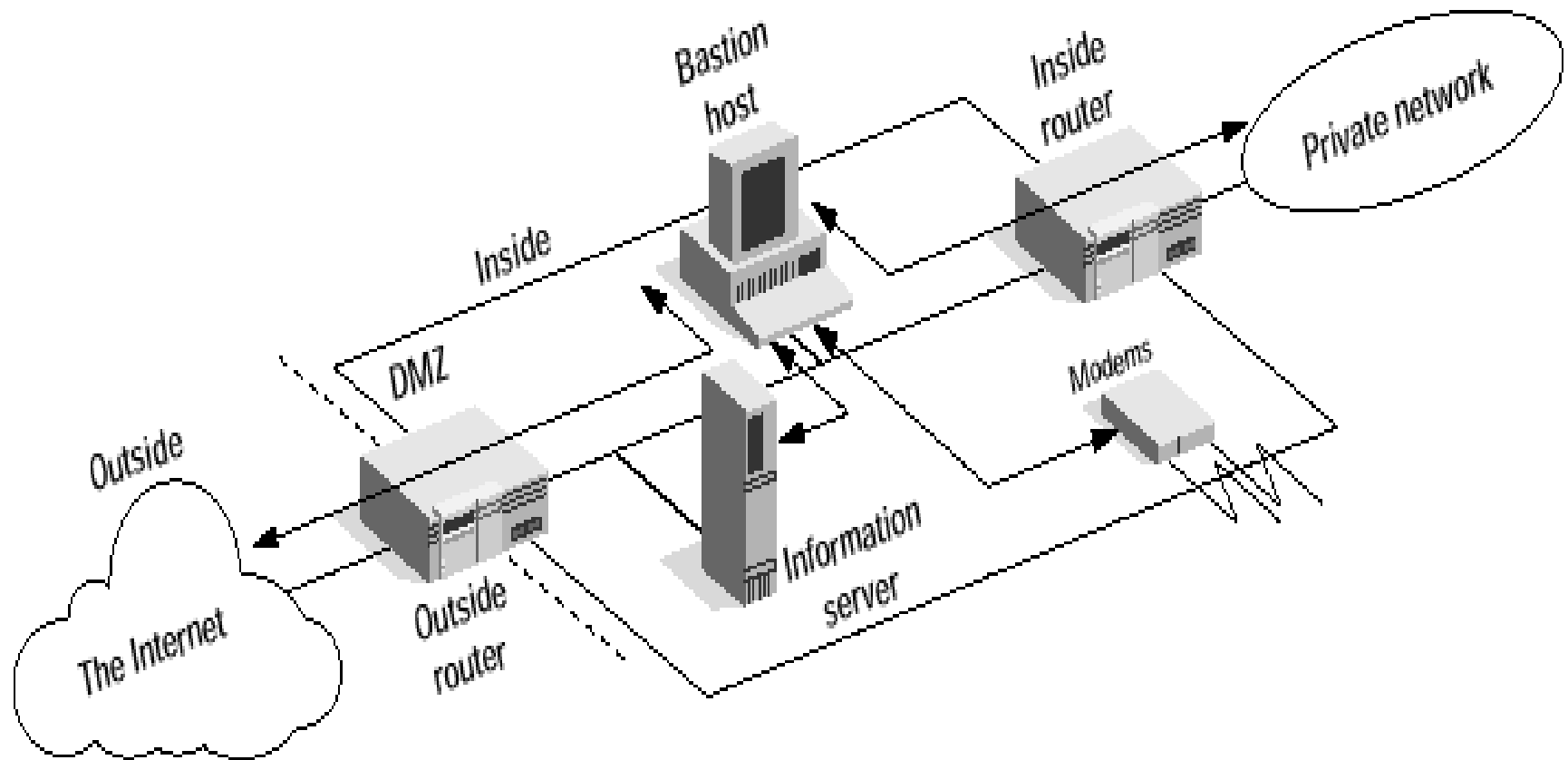


Screened-subnet firewall system

- Creates a DMZ Network
- Two Packet Filtering Routers
- Outside computers can only access the Bastion Host or Information Server
- Inside computers can only access services using the Bastion host



Screened-Subnet Firewall System



The Future

- **The Future** of firewalls lies someplace between network level firewalls and application level firewalls. It is likely that network level firewalls will become increasingly "aware" of the information going through them, and application level firewalls will become increasingly "low level" and transparent. The end result will be a fast packet-screening system that logs and audits data as it passes through. Increasingly, firewalls (network and application layer) incorporate encryption so that they may protect traffic passing between them over the Internet. Firewalls with end-to-end encryption can be used by organizations with multiple points of Internet connectivity to use the Internet as a "private backbone" without worrying about their data or passwords being sniffed.

What Firewalls Can Protect?

- Some firewalls permit only Email traffic through them, thereby protecting the network against any attacks other than attacks against the Email service.
- Other firewalls provide less strict protections, and block services that are known to be problems.

What Firewalls Can Protect?

- Generally, firewalls are configured to protect against unauthenticated interactive logins from the "outside" world. This, more than anything, helps prevent vandals from logging into machines on your network. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside. The firewall can protect you against any type of network-borne attack if you unplug it.

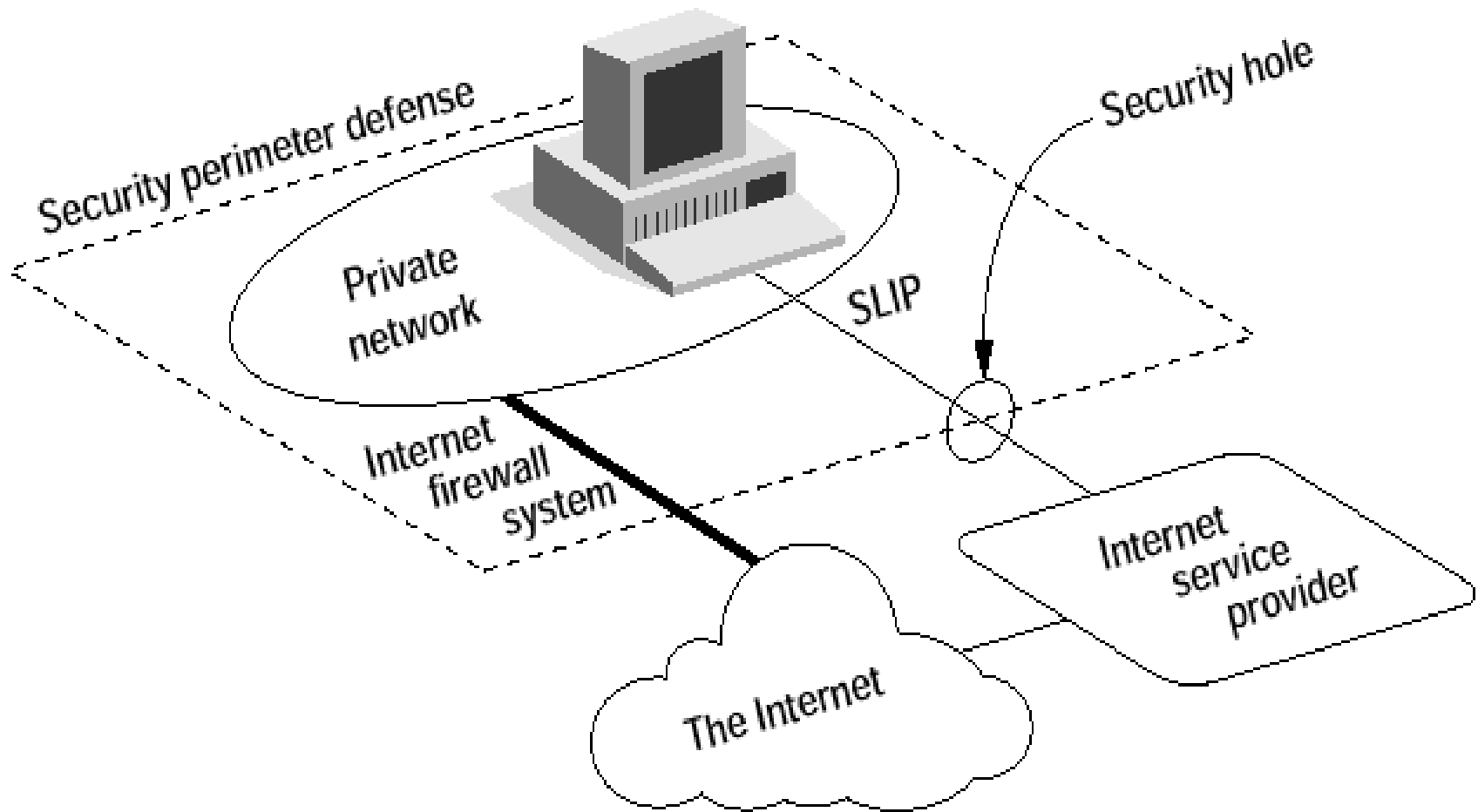
What Firewalls Can Protect?

- Firewalls are also important since they can provide a single "check point" where security and audit can be imposed. Unlike in a situation where a computer system is being attacked by someone dialing in with a modem, the firewall can act as an effective "phone tap" and tracing tool. Firewalls provide an important logging and auditing function; often they provide summaries to the administrator about what kinds and amount of traffic passed through it, how many attempts there were to break into it, etc.

What Firewalls Cannot Protect Against?

- Firewalls can't protect against attacks that don't go through the firewall. e.g. Floppy Disk data theft, Magnetic tape data theft, dialup modem links
- **For a firewall to work, it must be a part of a consistent overall organizational security architecture.**
- Firewall policies must be realistic, and reflect the level of security in the entire network. For example, a site with top secret or classified data doesn't need a firewall at all: they shouldn't be hooking up to the Internet in the first place, or the systems with the really secret data should be isolated from the rest of the corporate network.

A Connection Circumventing an Internet Firewall



What Firewalls Cannot Protect Against?

- Another thing a firewall can't really protect you against is traitors or idiots inside your network. While an industrial spy might export information through your firewall, he's just as likely to export it through a telephone, FAX machine, or floppy disk. Floppy disks are a far more likely means for information to leak from your organization than a firewall! Firewalls also cannot protect you against stupidity. Users who reveal sensitive information over the telephone are good targets for social engineering; an attacker may be able to break into your network by completely bypassing your firewall, if he can find a "helpful" employee inside who can be fooled into giving access to a modem pool.

What Firewalls Cannot Protect Against?

- Firewalls can't protect very well against things like viruses. There are too many ways of encoding binary files for transfer over networks, and too many different architectures and viruses to try to search for them all. In other words, a firewall cannot replace security-consciousness on the part of your users. In general, a firewall cannot protect against a data-driven attack -- attacks in which something is mailed or copied to an internal host where it is then executed. This form of attack has occurred in the past against various versions of `sendmail` and `ghostscript`, a freely-available PostScript viewer.

What Firewalls Cannot Protect Against?

- Organizations that are deeply concerned about viruses should implement organization-wide virus control measures. Rather than trying to screen viruses out at the firewall, make sure that every vulnerable desktop has virus scanning software that is run when the machine is rebooted. Blanketing your network with virus scanning software will protect against viruses that come in via floppy disks, modems, and Internet. Trying to block viruses at the firewall will only protect against viruses from the Internet -- and the vast majority of viruses are caught via floppy disks.
- Nevertheless, an increasing number of firewall vendors are offering "virus detecting" firewalls. They're probably only useful for naive users exchanging Windows-on-Intel executable programs and malicious-macro-capable application documents. Do not count on any protection from attackers with this feature.

What is source routed traffic and why is it a threat?

- Normally, the route a packet takes from its source to its destination is determined by the routers between the source and destination.
- The packet itself only says where it wants to go (the destination address), and nothing about how it expects to get there.
- Source routing means that the packet contains its own routing information.
- This may be abused
- This was necessary in the old days when you could not rely on the Internet Routers

What is source routed traffic and why is it a threat?

- There is an optional way for the sender of a packet (the source) to include information in the packet that tells the route the packet should get to its destination; thus the name "source routing". For a firewall, source routing is noteworthy, since an attacker can generate traffic claiming to be from a system "inside" the firewall. In general, such traffic wouldn't route to the firewall properly, but with the source routing option, all the routers between the attacker's machine and the target will return traffic along the reverse path of the source route. Implementing such an attack is quite easy; so firewall builders should not discount it as unlikely to happen.

What is source routed traffic and why is it a threat?

- In practice, source routing is very little used. In fact, generally the main legitimate use is in debugging network problems or routing traffic over specific links for congestion control for specialized situations.
- When building a firewall, source routing should be blocked at some point. Most commercial routers incorporate the ability to block source routing specifically, and many versions of Unix that might be used to build firewall bastion hosts have the ability to disable or ignore source routed traffic.

What are ICMP redirects and redirect bombs?

- An ICMP Redirect tells the recipient system to over-ride something in its routing table. It is legitimately used by routers to tell hosts that the host is using a non-optimal or defunct route to a particular destination. If you can forge ICMP Redirect packets, and if your target host pays attention to them, you can alter the routing tables on the host and possibly subvert the security of the host by causing traffic to flow via a path the network manager didn't intend.
- ICMP Redirects also may be employed for denial of service attacks, where a host is sent a route that loses its connectivity, or is sent an ICMP Network Unreachable packet telling it that it can no longer access a particular network.
- Many firewall builders screen ICMP traffic from their network, since it limits the ability of outsiders to ping hosts, or modify their routing tables.

Denial of Service Attacks

- Attacks which intend to overload computing resources or which intend to crash software entities and services are known as Denial of Service (DoS) attacks
- Examples:
 - ⊗ TCP SYN Flooding
 - ⊗ TLS Client Hello Messages
 - ⊗ ICMP Echo Requests
- Sophisticated Firewalls can protect against some of these attacks

Firewall Performance

Connectivity Issues

- Firewalls add latency due to the processing at the firewall
- Many services (such as netmeeting, net2phone) might not work through a firewall
- Try using Linux Floppy-based Firewall floppy-fw

Summary

- Firewalls provide the first line of defense against external attacks
- Firewall implementation requires an understanding of the connectivity needs
- Firewalls are basically of two different types:
 - ⊗ Network Level
 - ⊗ Application Level