FIREWALL

What is a firewall?

- Two goals:
  - To provide the people in your organization with access to the WWW without allowing the entire world to peak in;
  - To erect a barrier between an untrusted piece of software, your organization's public Web server, and the sensitive information that resides on your private network.
- Basic idea:
  - Impose a specifically configured gateway machine between the outside world and the site's inner network.
  - All traffic must first go to the gateway, where software decide whether to allow or reject.

What is a firewall

- A firewall is a system of hardware and software components designed to restrict access between or among networks, most often between the Internet and a private Internet.
- The firewall is part of an overall security policy that creates a perimeter defense designed to protect the information resources of the organization.

Firewalls DO

- Implement security policies at a single point
- Monitor security-related events (audit, log)
- Provide strong authentication
- Allow virtual private networks
- Have a specially hardened/secured operating system

Firewalls DON'T

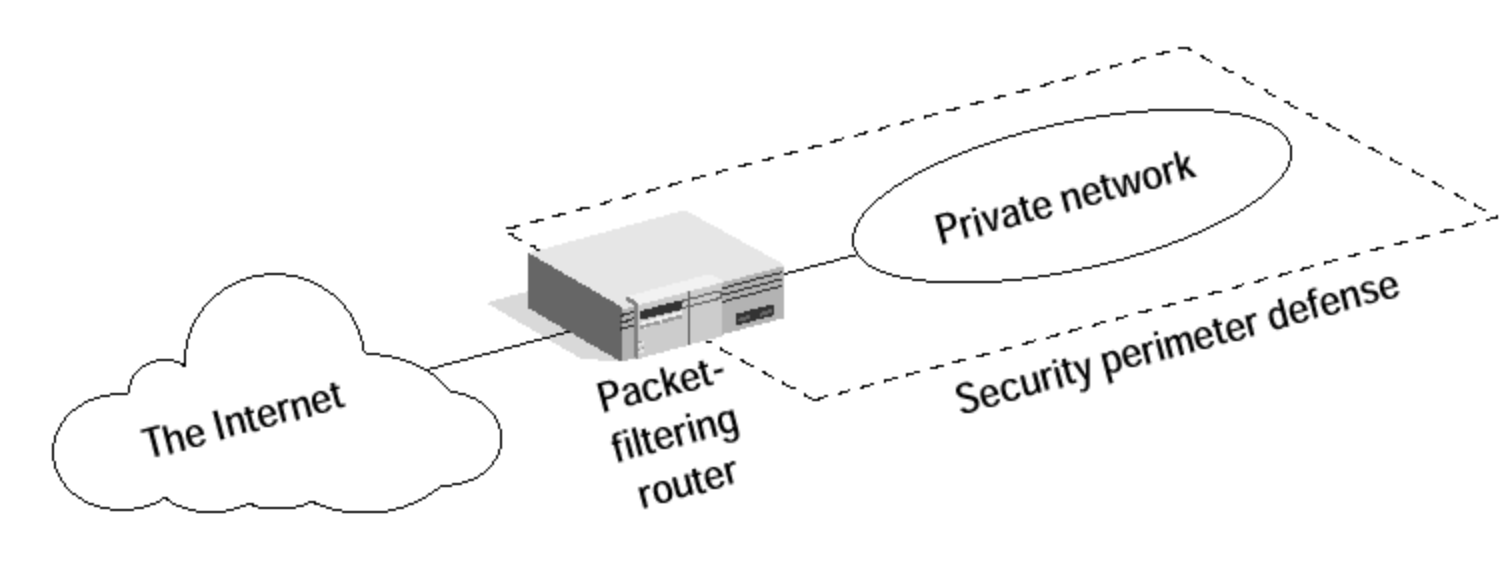
- Protect against attacks that bypass the firewall
  - Dial-out from internal host to an ISP
- Protect against internal threats
  - disgruntled employee
  - Insider cooperates with and external attacker
- Protect against the transfer of virus-infected programs or files

Types of Firewalls

- Packet-Filtering Router
- Application-Level Gateway
- Circuit-Level Gateway
- Hybrid Firewalls

Packet Filtering Routers

- Forward or discard IP packet according a set of rules
- Filtering rules are based on fields in the IP and transport header



What information is used for filtering decision?

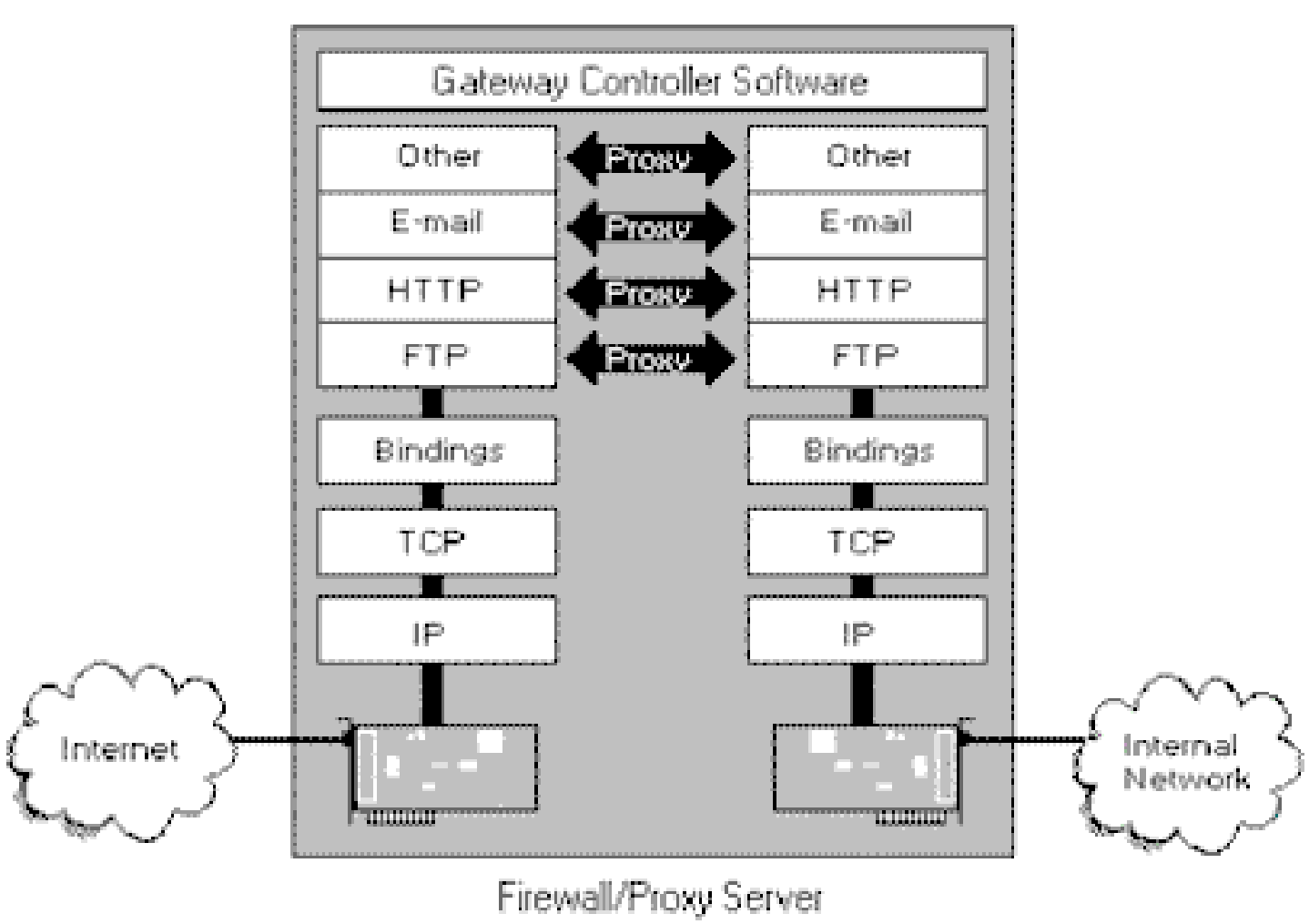
- Source IP address (IP header)
- Destination IP address (IP header)
- Protocol Type
- Source port (TCP or UDP header)
- Destination port (TCP or UDP header)
- ACK. bit

Web Access Through a Packet Filter Firewall

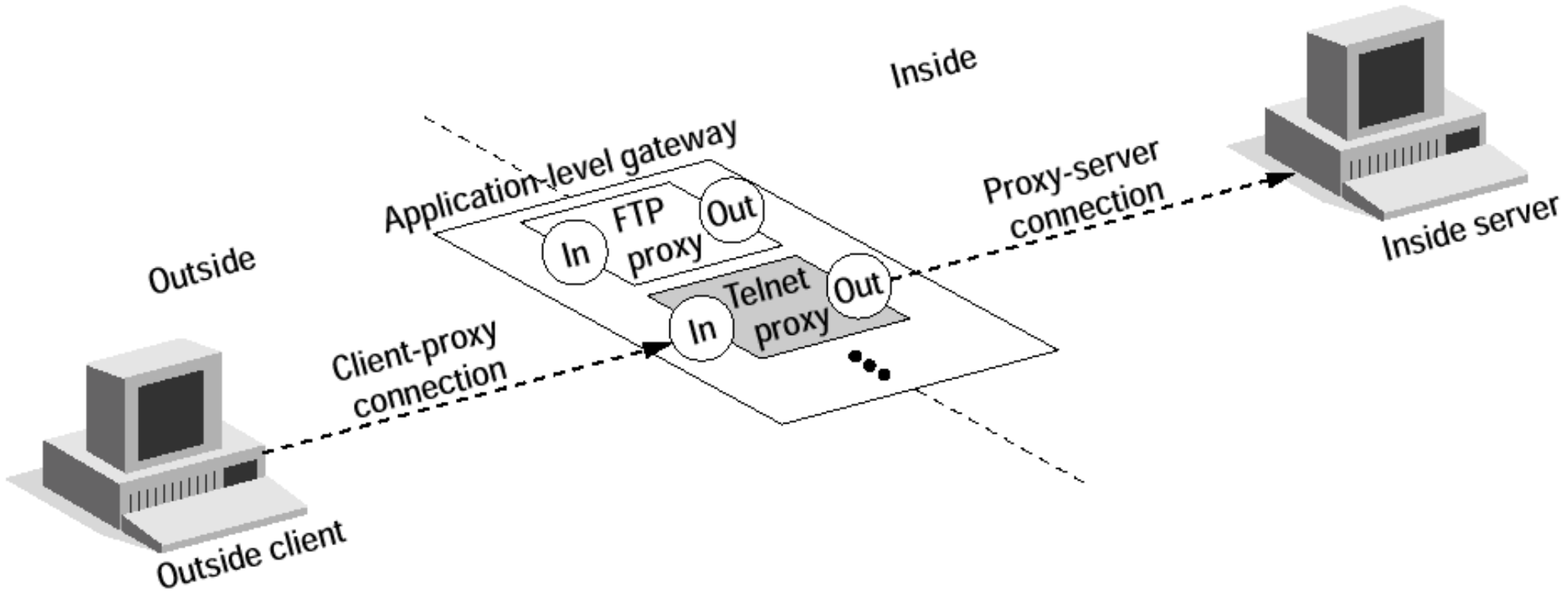
TABLE 14.1 Web Access Through a Packet Filter Firewall

Action	Src	Port	Dest	Port	Flags	Comment
block	*	*	*	*	*	Block all by default
allow	*{Internal net}*	*	*	80	*	Outgoing Web
allow	*	80	*	*	ACK	Incoming Web
allow	*{Internal net}*	*	*	21	*	Outgoing FTP control channel
allow	*	21	*	*	ACK	Incoming FTP control channel
allow	*{Internal net}*	*	*	≥1024	*	Outgoing FTP data
allow	*	≥1024	*	*	ACK	Incoming FTP data
allow	*{Internal net}*	*	*	443	*	Outgoing SSL
allow	*	443	*	*	ACK	Incoming SSL
allow	*{Internal net}*	*	*	70	*	Outgoing Gopher
allow	*	70	*	*	ACK	Incoming Gopher

Application Level Gateways (Proxy Server)



A Telnet Proxy



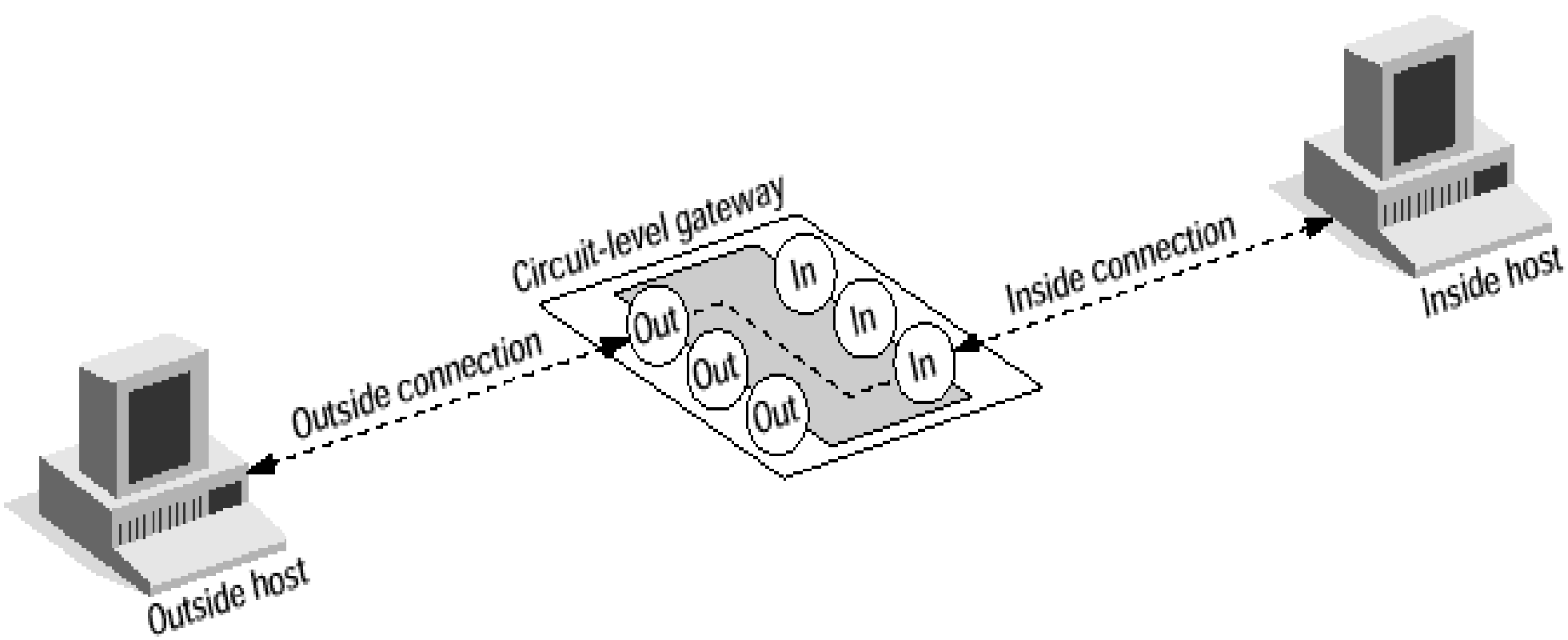
A sample telnet session

```
Outside-Client > telnet bastion_host
Username: John Smith
Challenge Number "237936"
Challenge Response: 723456
Trying 200.43.67.17 ...

HostOS UNIX (bastion_host)

bh-telnet-proxy> help
Valid commands are:

connect hostname
help/?
quit/exit

bh-telnet-proxy> connect inside_server

HostOS UNIX (inside_server)

login: John Smith
Password: ######
Last login: Wednesday April 15 11:17:15
```

Application Level Gateways (Proxy Server)

- Advantages:
  - complete control over each service (FTP/HTTP…)
  - complete control over which services are permitted
  - Strong user authentication (Smart Cards etc.)
  - Easy to log and audit at the application level
  - Filtering rules are easy to configure and test
- Disadvantages:
  - A separate proxy must be installed for each application-level service
  - Not transparent to users

Circuit Level Gateways



Circuit Level Gateways (2)

- Often used for outgoing connections where the system administrator trusts the internal users
- The chief advantage is that a firewall can be configured as a hybrid gateway supporting application-level/proxy services for inbound connections and circuit-level functions for outbound connections

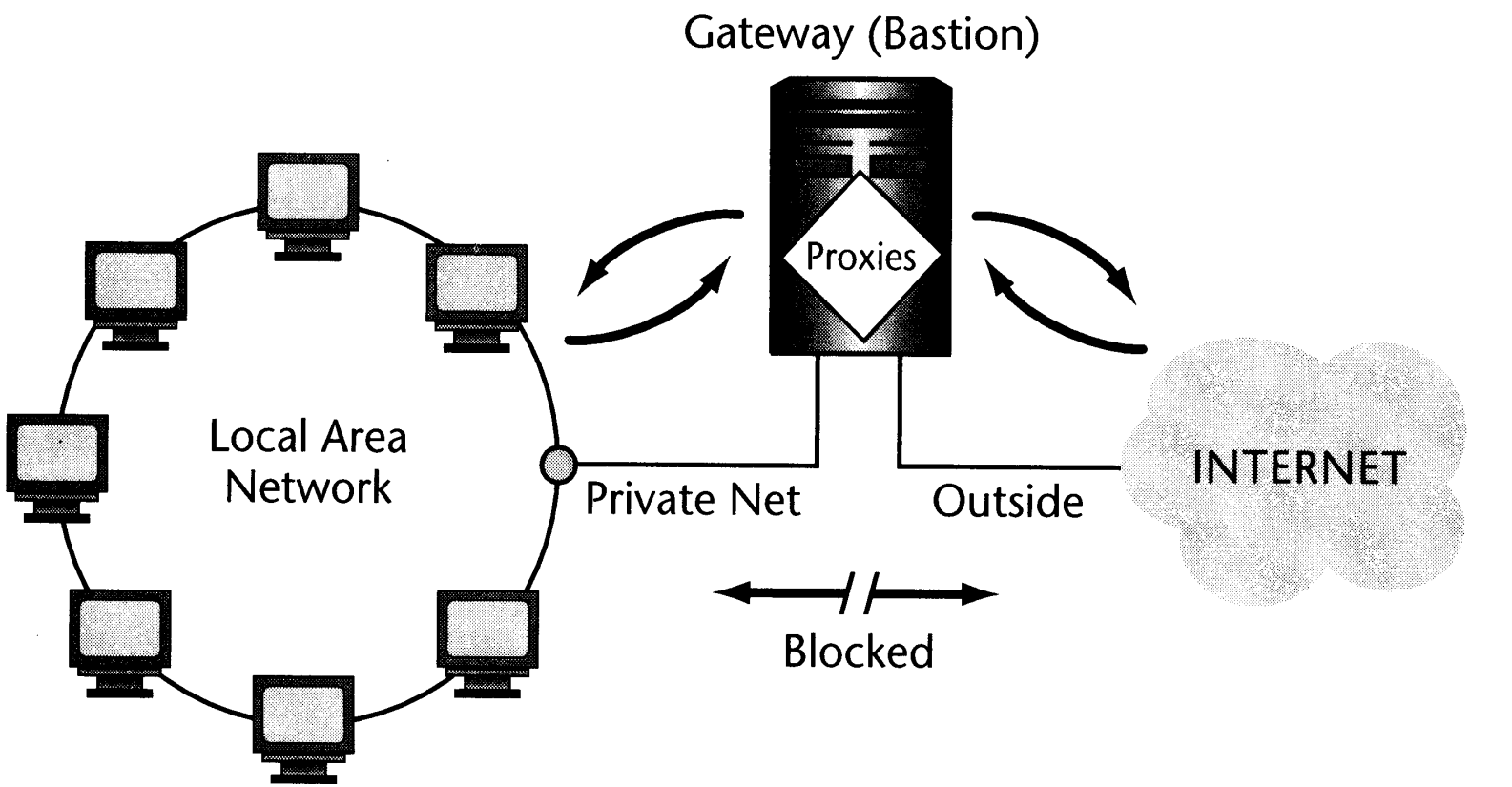
Hybrid Firewalls

- In practice, many of today's commercial firewalls use a combination of these techniques.
- Examples:
  - A product that originated as a packet-filtering firewall may since have been enhanced with smart filtering at the application level.
  - Application proxies in established areas such as FTP may augment an inspection-based filtering scheme.

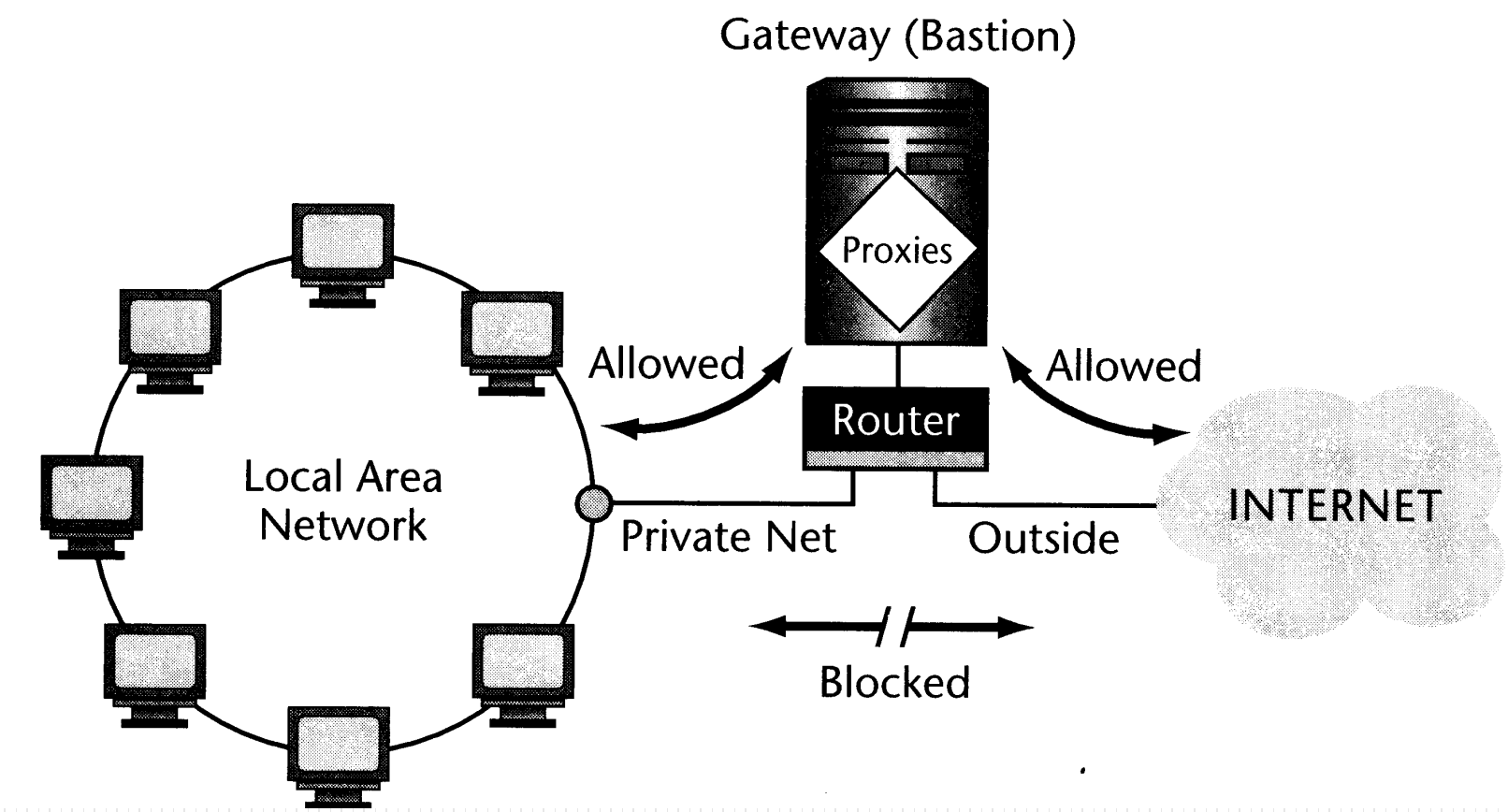
Firewall Configurations

- Bastion host
  - a system identified by firewall administrator as a critical strong point in the network's security
  - typically serves as a platform for an application-level or circuit-level gateway
  - extra secure O/S, tougher to break into
- Dual homed gateway
  - Two network interface cards: one to the outer network and the other to the inner
  - A proxy selectively forwards packets
- Screened host firewall system
  - Uses a network router to forward all traffic from the outer and inner networks to the gateway machine
- Screened-subnet firewall system

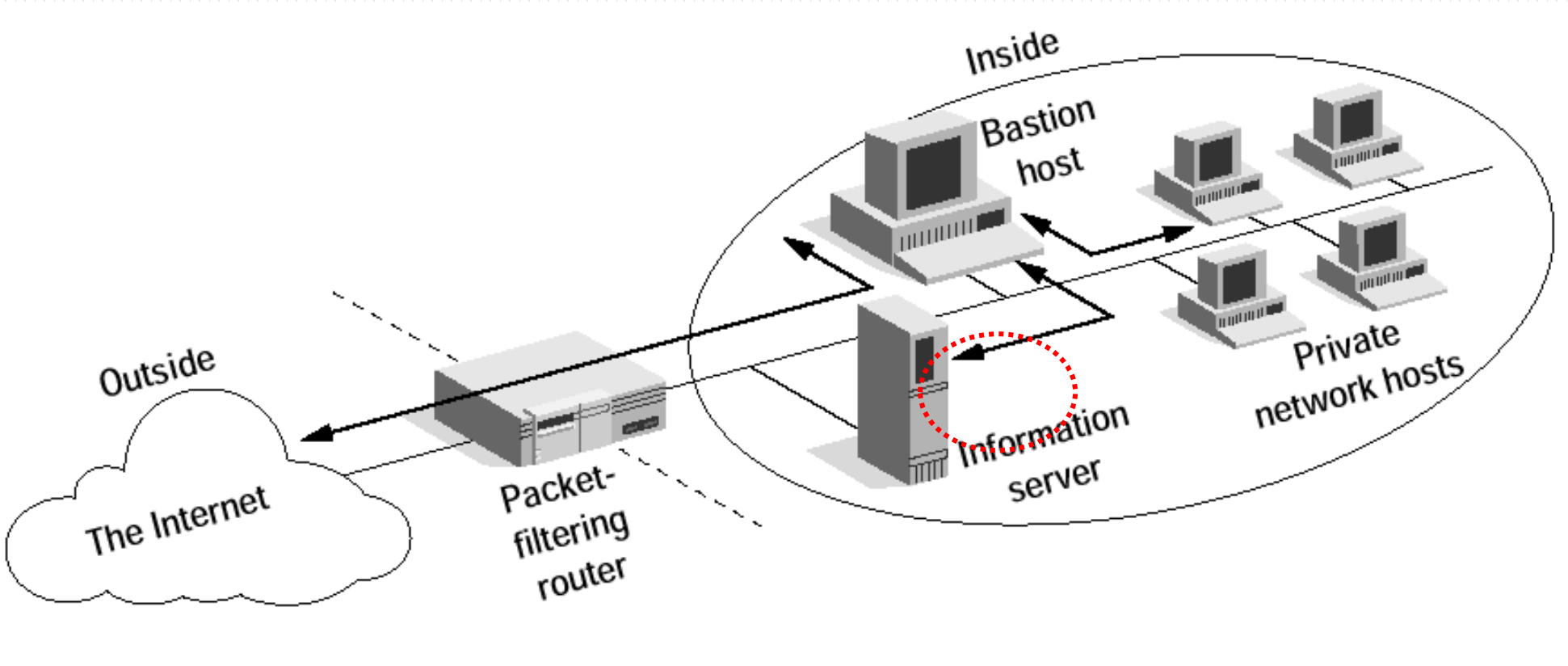
Dual-homed gateway



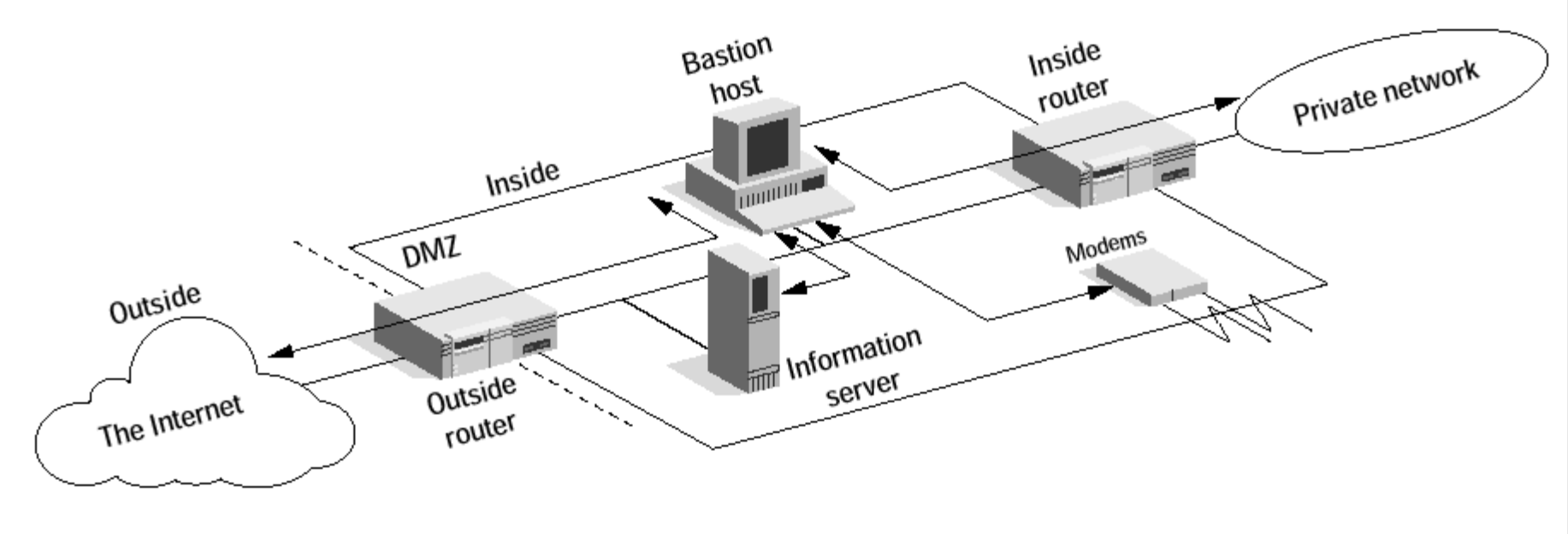
Screened-host gateway



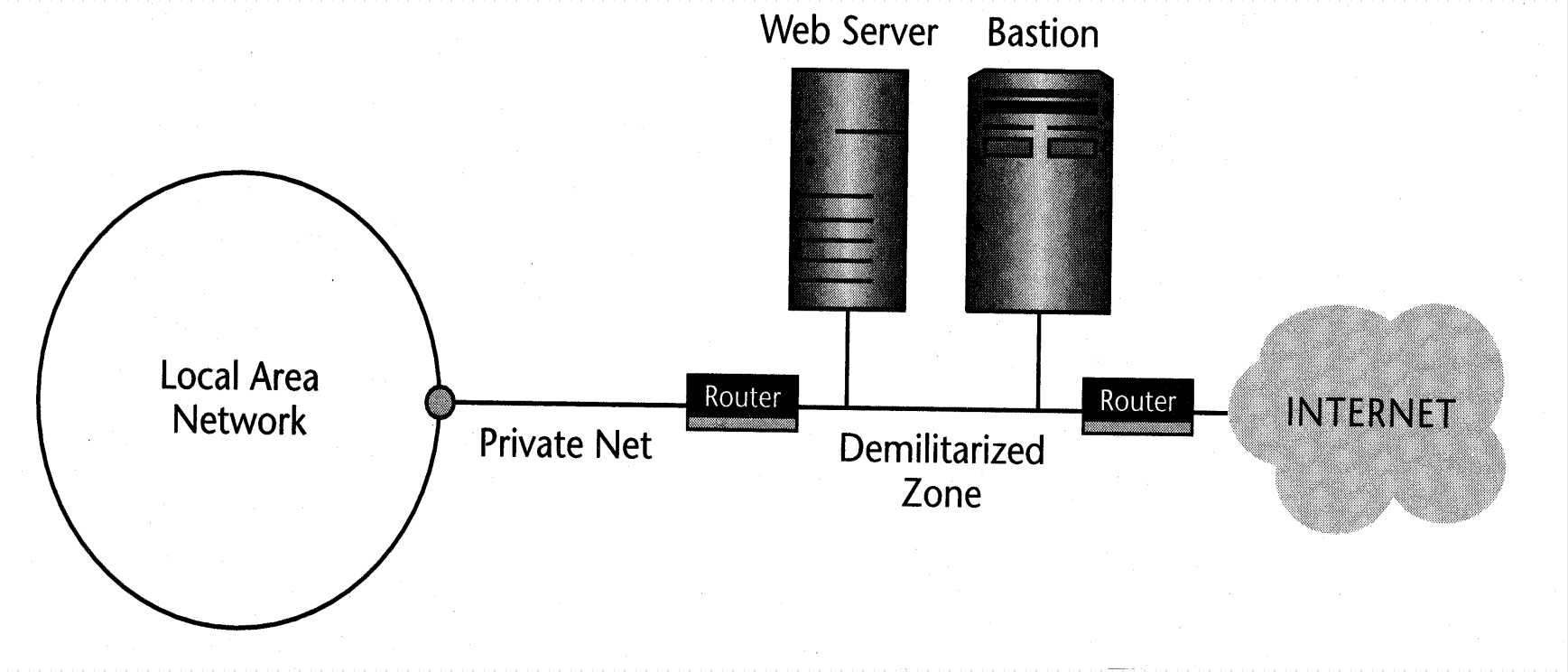
Screened Host Firewall



Screened Subnet Firewall



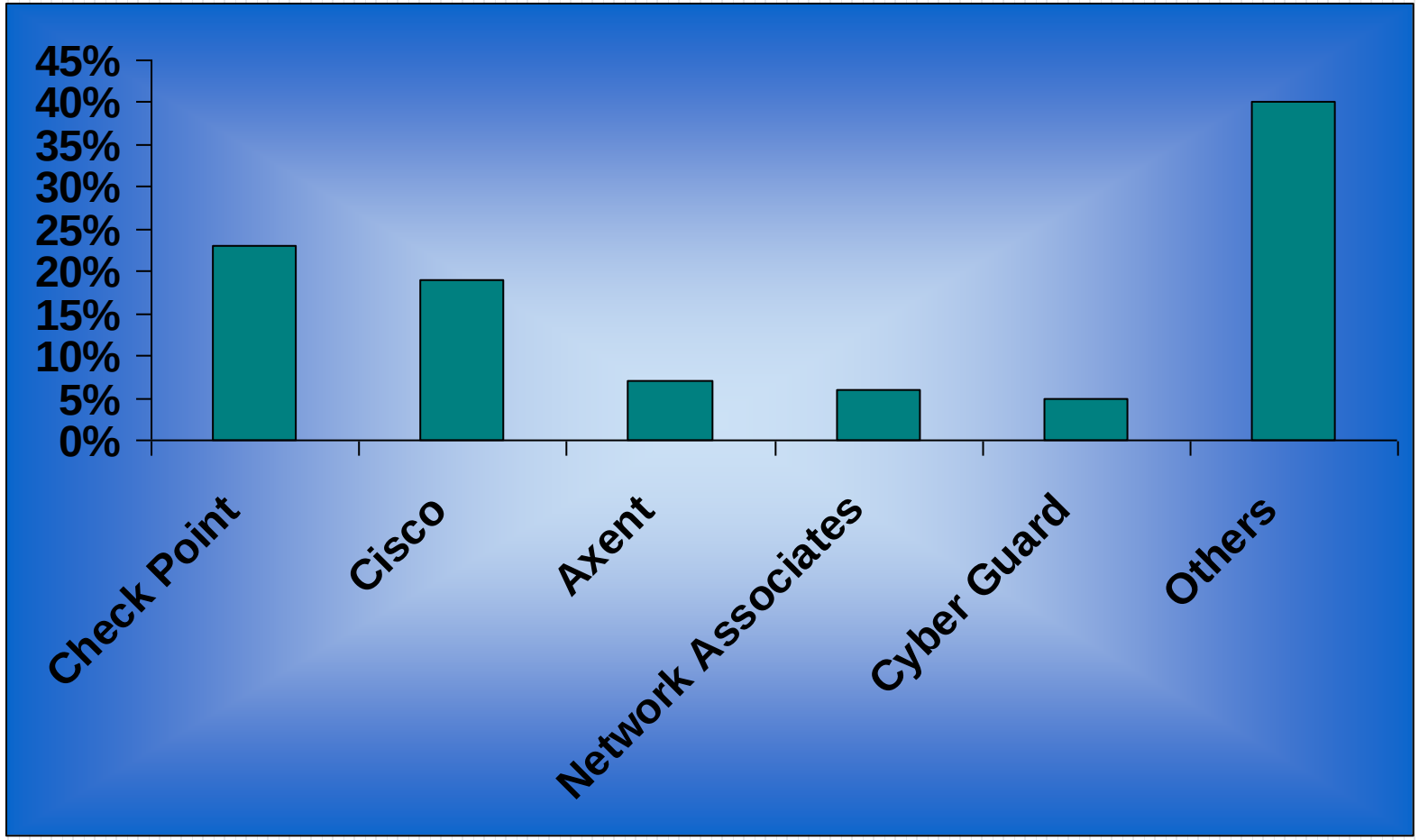
Screened subnet gateway



Selecting a firewall system

- Operating system
- Protocols handled
- Filter types
- Logging
- Administration
- Simplicity
- Tunneling

Commercial Firewall Systems



Widely used commercial firewalls

- AltaVista
- BorderWare (Secure Computing Corporation)
- CyberGurad Firewall (CyberGuard Corporation)
- Eagle (Raptor Systems)
- Firewall-1 (Checkpoint Software Technologies)
- Gauntlet (Trusted Information Systems)
- ON Guard (ON Technology Corporation)

Thanks