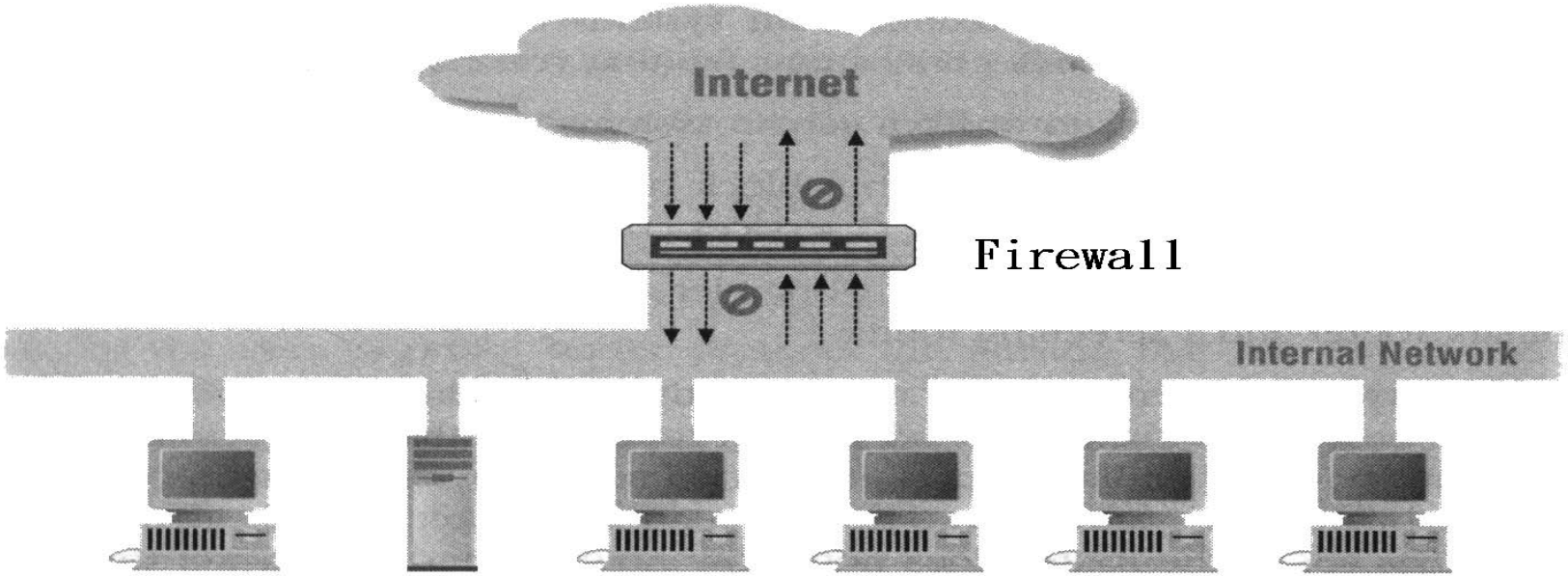
What is an Internal Firewall?

- Keep a fire from spreading from one part of the building to another (intranet).



What Can a Firewall Do?

- A firewall is a focus for security decision
- A firewall can enforce security policy
- A firewall can log Internet activity efficiently
- A firewall limits your exposure

What a Firewall Can't Do?

- A firewall can't protect you against malicious insiders
- A firewall can't protect you against backdoor connections (e.g., modem servers)
- A firewall can't protect against new threats
- A firewall can't protect against viruses

Terminologies

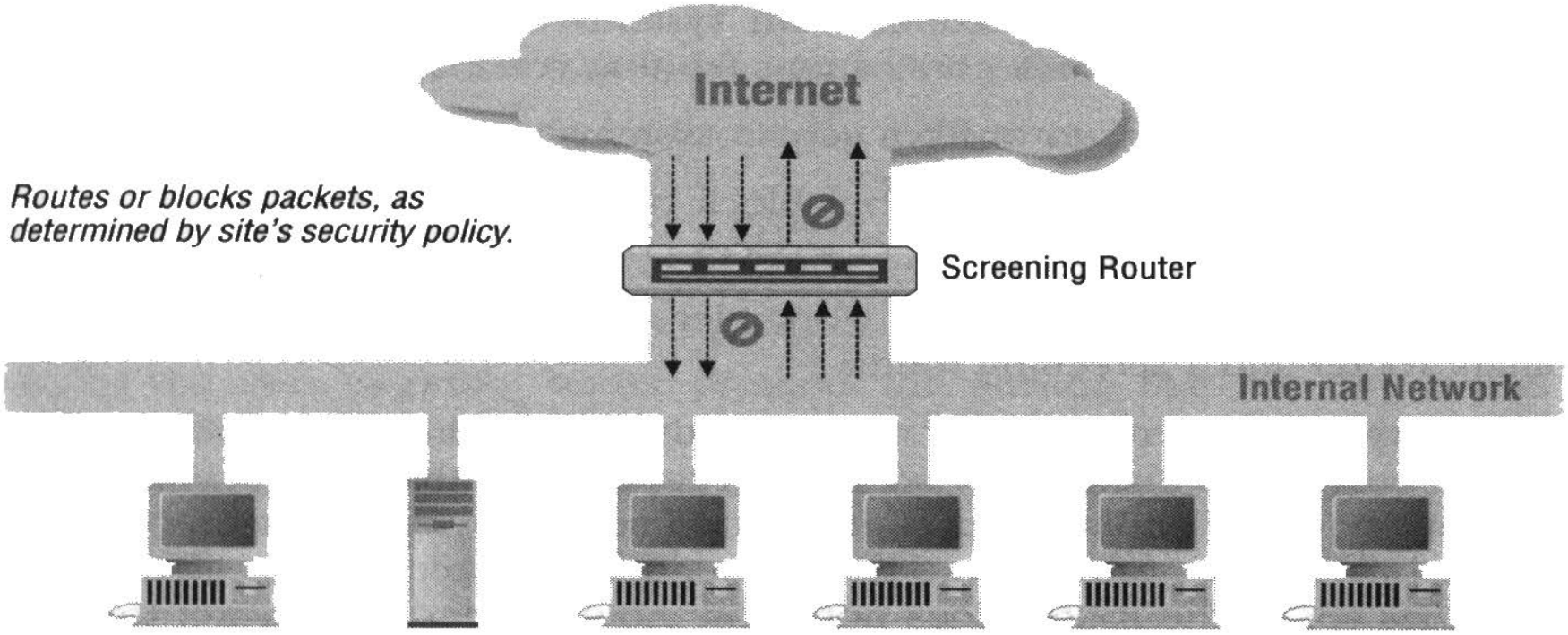
- Firewall:
- Bastion host (main contact point)
- Packet filtering (or screening)
- Perimeter network (De-Militarized Zone; DMZ)
- Proxy server (application level relay)

Major approaches to build firewalls:

- Packet filtering
- Proxy services

Packet Filtering

- Use screening router

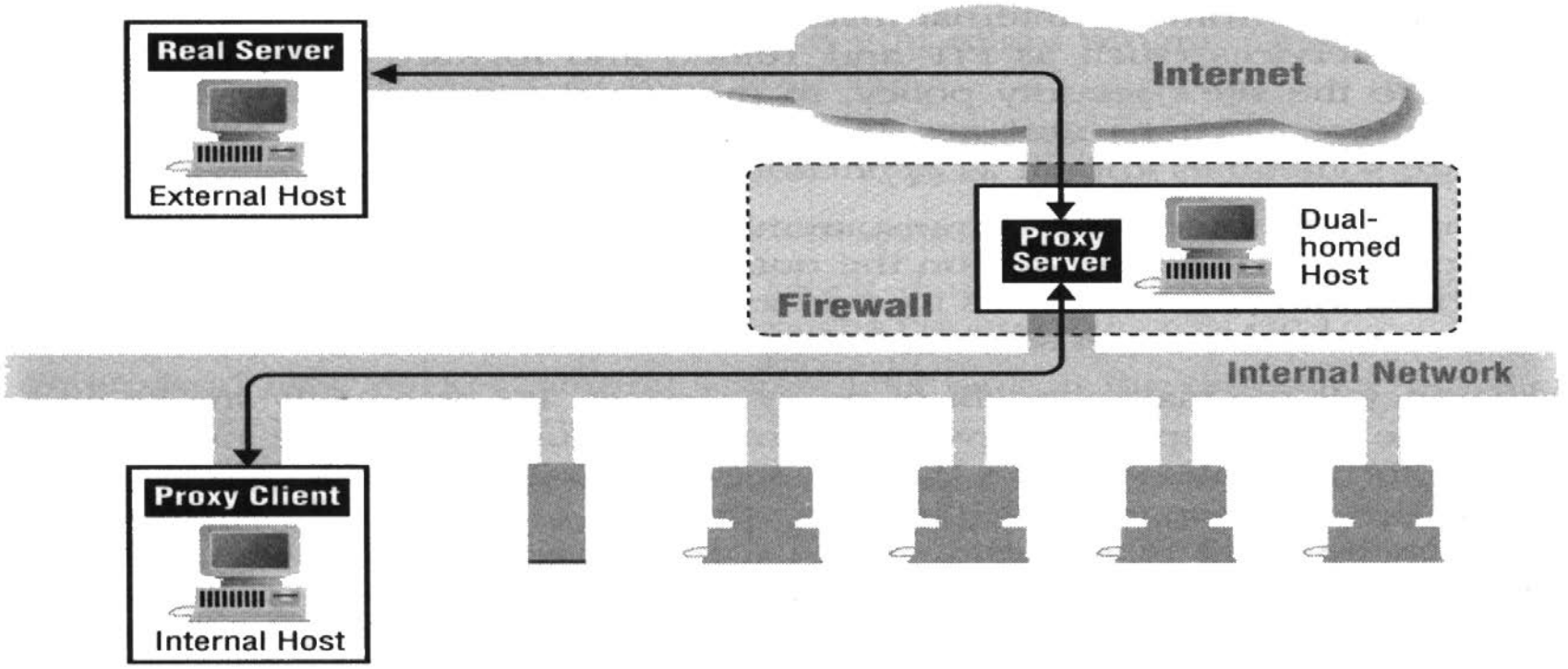


Screening

- Investigate:
  - IP source (address, port)
  - IP destination (address, port)
  - Protocol (TCP, UDP, etc.)
  - ICMP messages types
- Examples:
  - Block all incoming connections except for SMTP
  - Block all connections to or from certain systems you distrust
  - Allow email and FTP services, but not others.

Proxy Services

- Proxy client: a special client talks to proxy server.



Proxy Server

- An application-level gateway
- SOCKS: a proxy construction toolkit.
  - convert current client/server applications into proxy versions.
  - most standard services equipped with proxying or support SOCKS.
- Trusted Information Systems Internet Firewall Toolkit (TIS FWTK): include proxy servers for protocols like telnet, ftp, http, ...etc.

Hybrid Solution

- Packet filtering
  - more effective for telnet and smtp (purely filtering)
- Proxy services
  - more effective for WWW or FTP (can do caching)

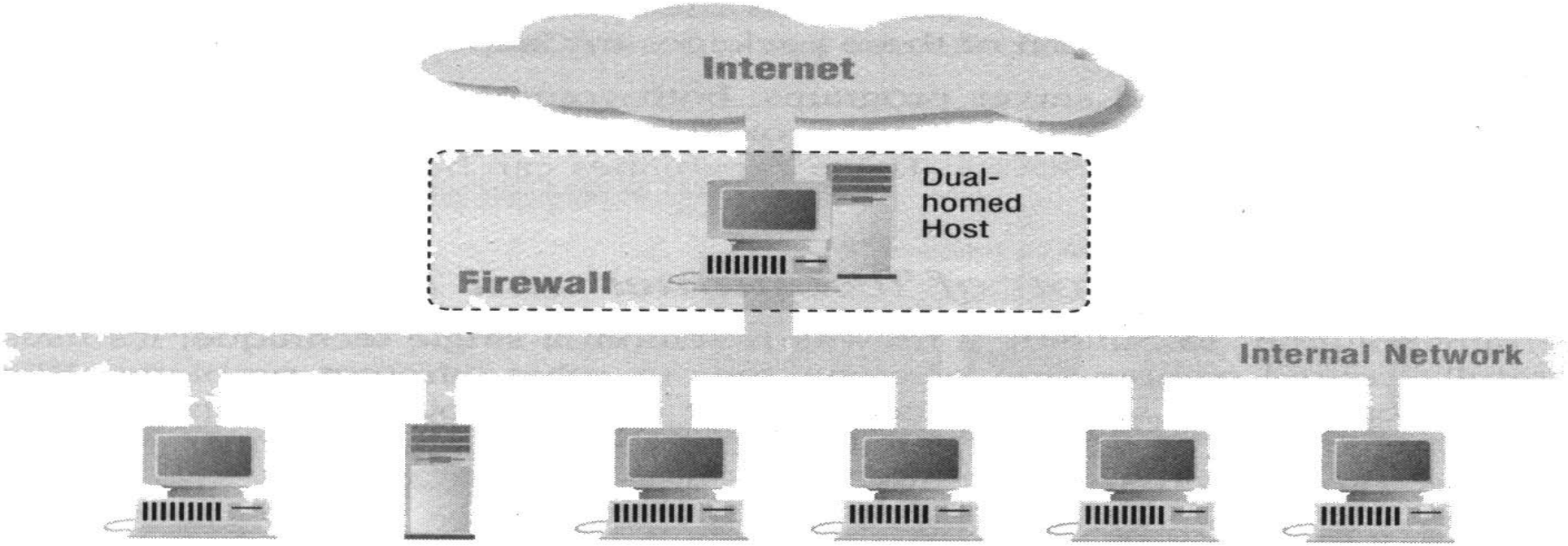
==> usually, a combination of both.

Firewall Architecture

- Dual-Homed Host Architecture
- Screened Host Architecture
- Screened Subnet Architecture

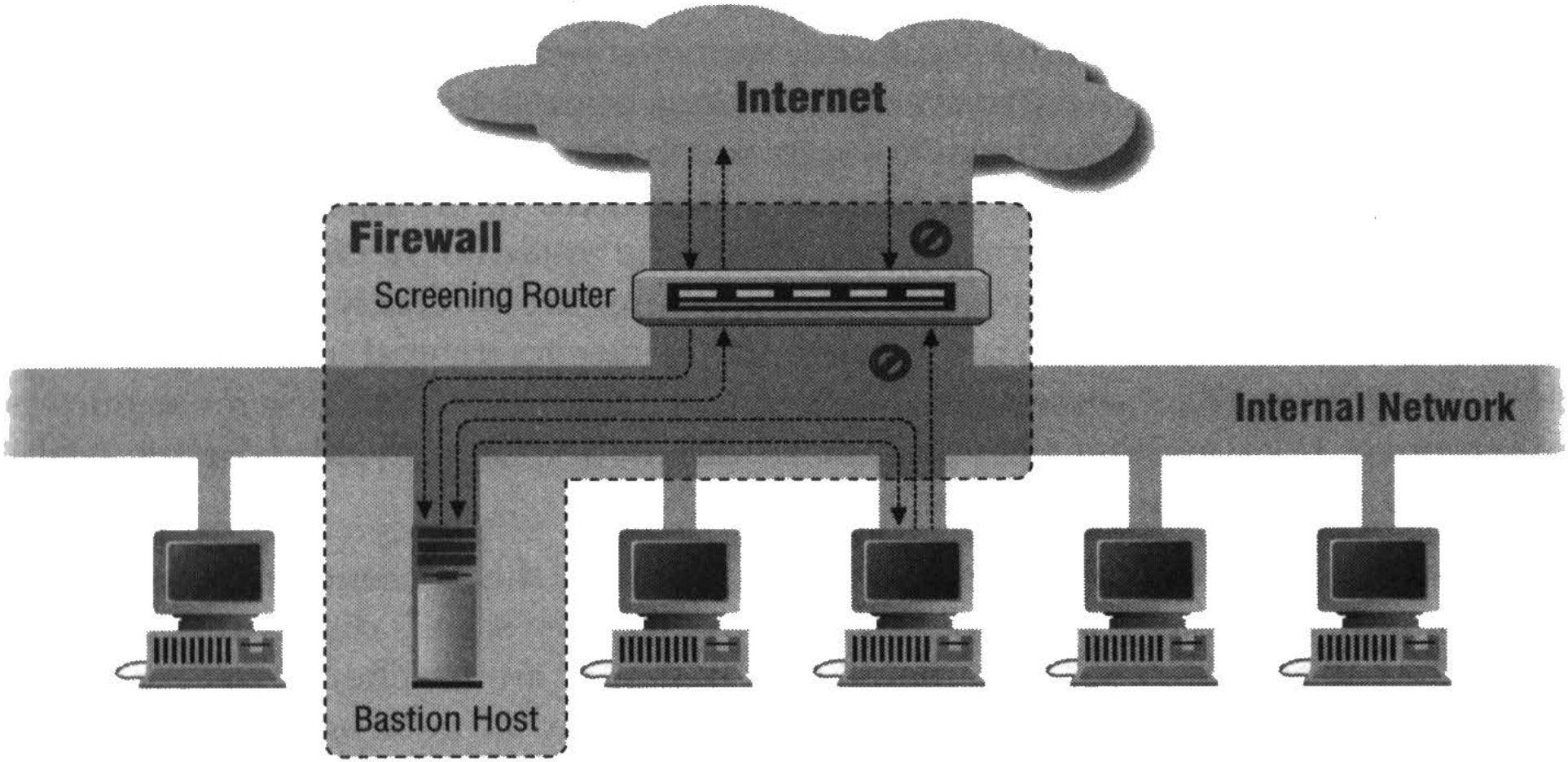
Dual-Homed Host Architecture

- Disable the routing function (block all IP packets)
- Only provide proxy services
- Problem: not for all applications



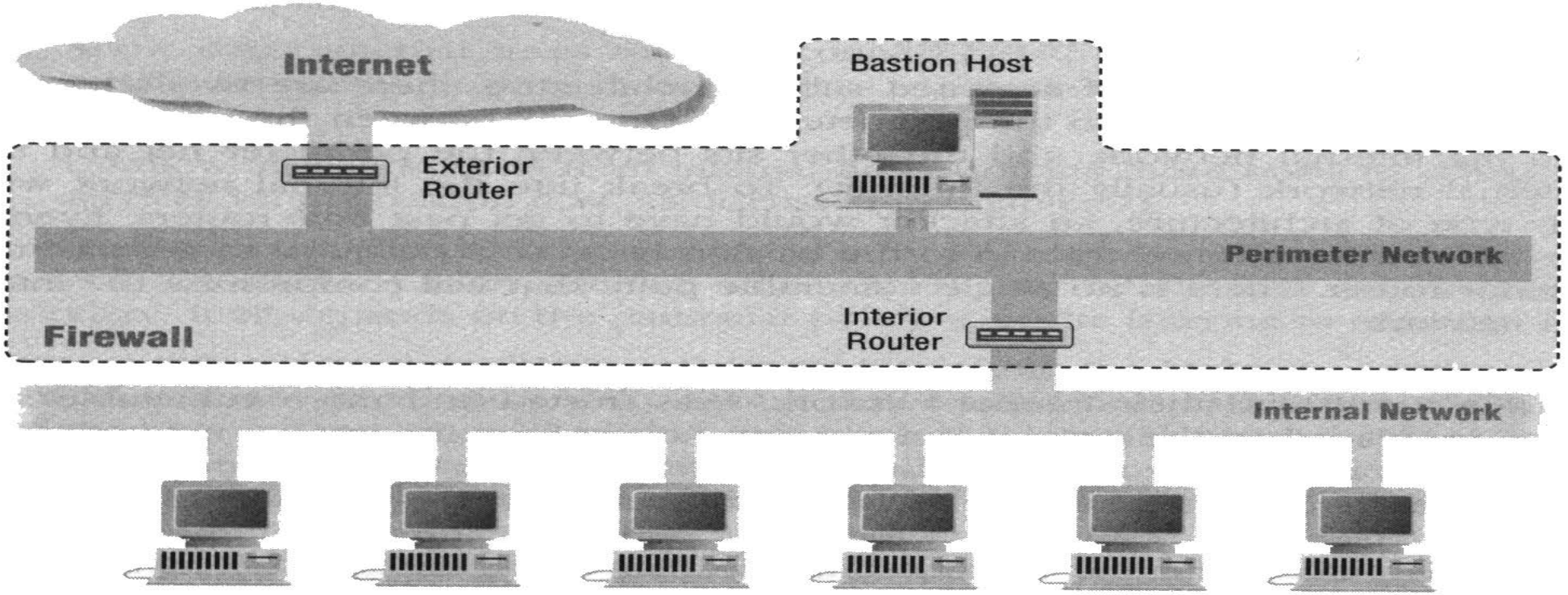
Screened Host Architecture

- packet filtering in the router
  - allow certain services (from internal to outside)
  - disallow all connections from outside
- always through the bastion host (application level)
- Problem:
  - if attackers break in the bastion host, others expose to be attacked. E.g., in the bastion host, the intruder can watch all passwords or key information inside the network.


Internet
Firewall
Screening Router
Internal Network
Bastion Host

Screened Subnet Architecture

- Add a perimeter network ==> need to past two routers to break in.



Components

- Perimeter:
  - less trusted and more vulnerable services put in the perimeter network.
  - intruded bastion host can only watch traffic. (So, assume that the traffic is not confidential.)
- Bastion host:
  - Inbound services
    - SMTP servers, FTP servers, DNS servers, ...
  - Outbound services
    - let internal host pass two routers to external hosts.
    - use bastion host as proxy servers.

Components (cont.)

- Interior router (or called choke router)
  - Does most packet filtering
  - Outbound
    - Allow selected services, telnet, ftp, etc.
  - Inbound
    - Usually, allow services (e.g. SMTP) from bastion to internal.
- Exterior router (or called access router)
  - Does little packet filtering
    - But, fine to filter those filtered by interior router.
    - Usually provider by Internet provider (not so secure)
  - Key mission: don’t allow forge IP address (e.g. bastion)

Variations on Firewall Architectures

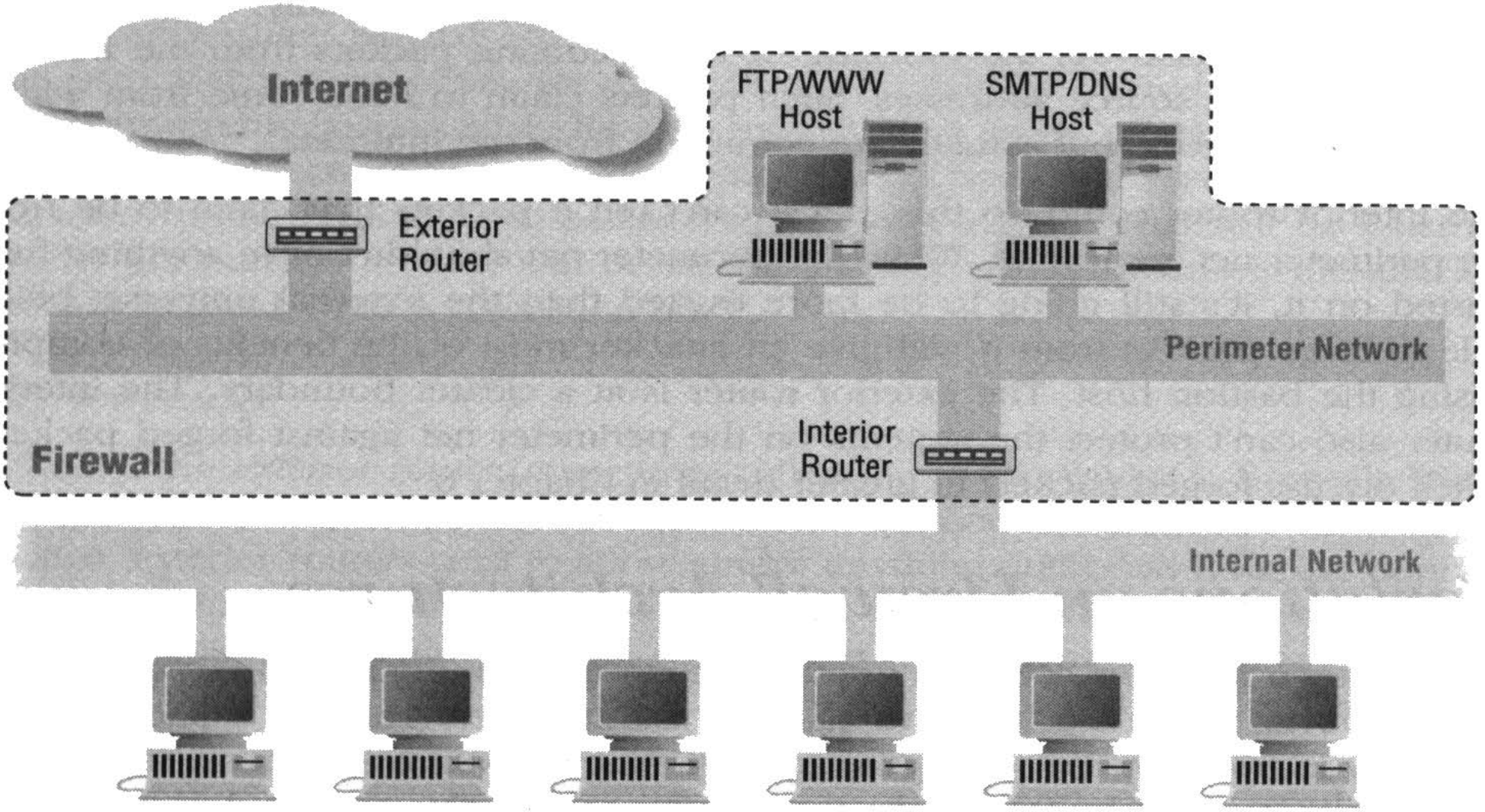
- Multiple bastion hosts
- Merging interior and exterior routers
- Merging bastion host and exterior router
- Multiple Exterior Routers
- Multiple Perimeter Networks
- Dual-Homed Hosts and Screened Subnets

But, it is dangerous to be:

- Multiple Interior Routers
- Merging bastion host and interior router

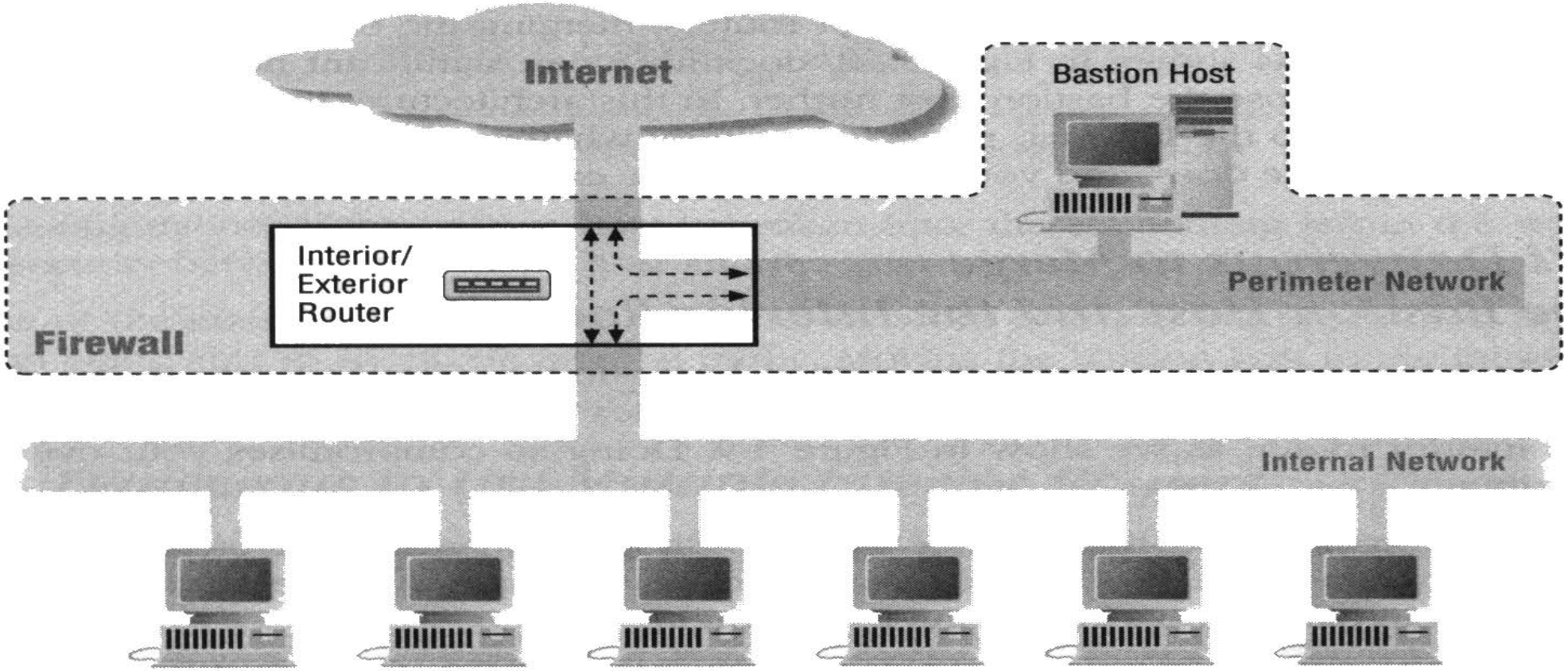
Multiple bastion Hosts

- Reasons:
  - Performance
    - E.g., Usenet News are resource-intensive and easily separated from others.
  - Redundancy:
    - Fault tolerance: Some failed. Other can replace it.
      => but only some services (DNS) allow to do this.
  - Separate data
    - E.g., one http server for internal users and one http server for external users.
      (Make data more secure or manageable.)


Internet
FTP/WWW
Host
SMTP/DNS
Host
Exterior
Router
Perimeter Network
Interior
Router
Firewall
Internal Network

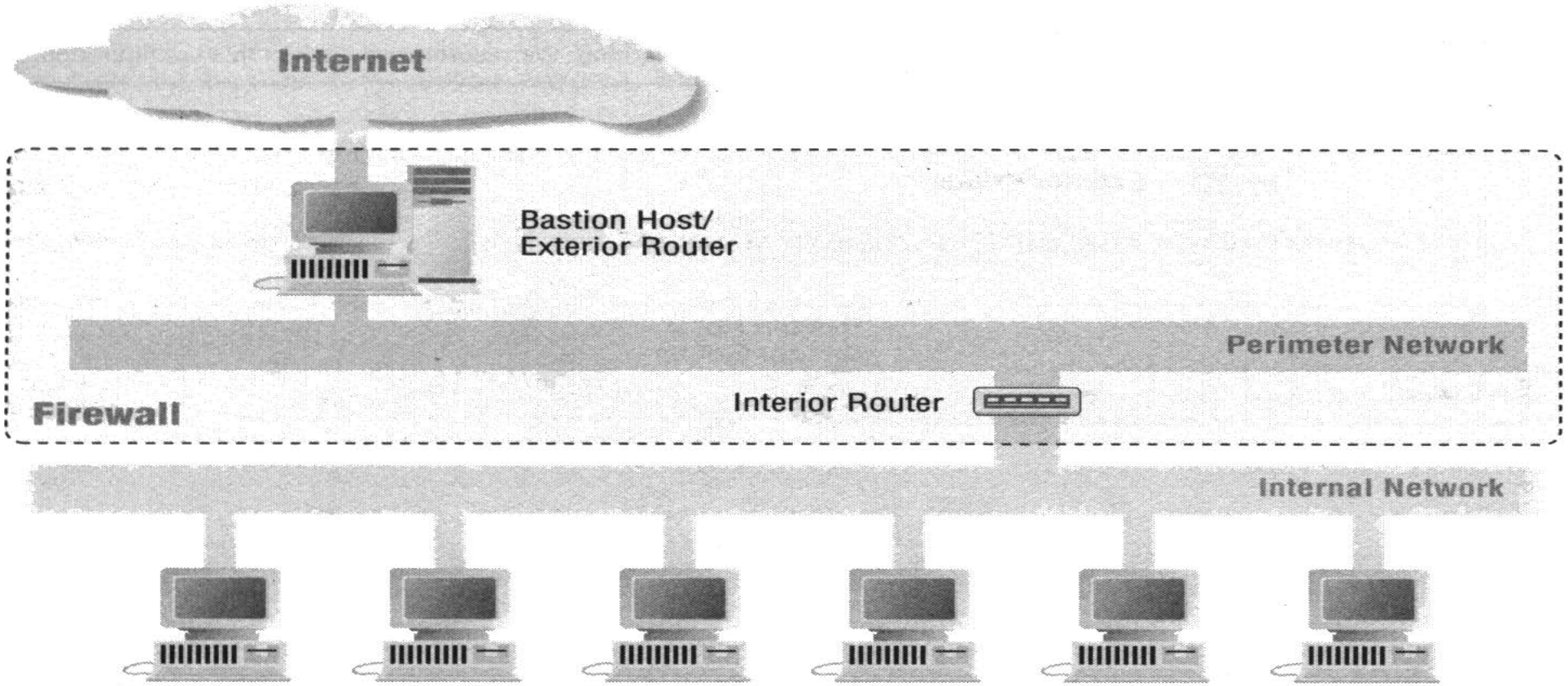
Merging Interior and Exterior Routers

- The only problem: only need to penetrate the router.



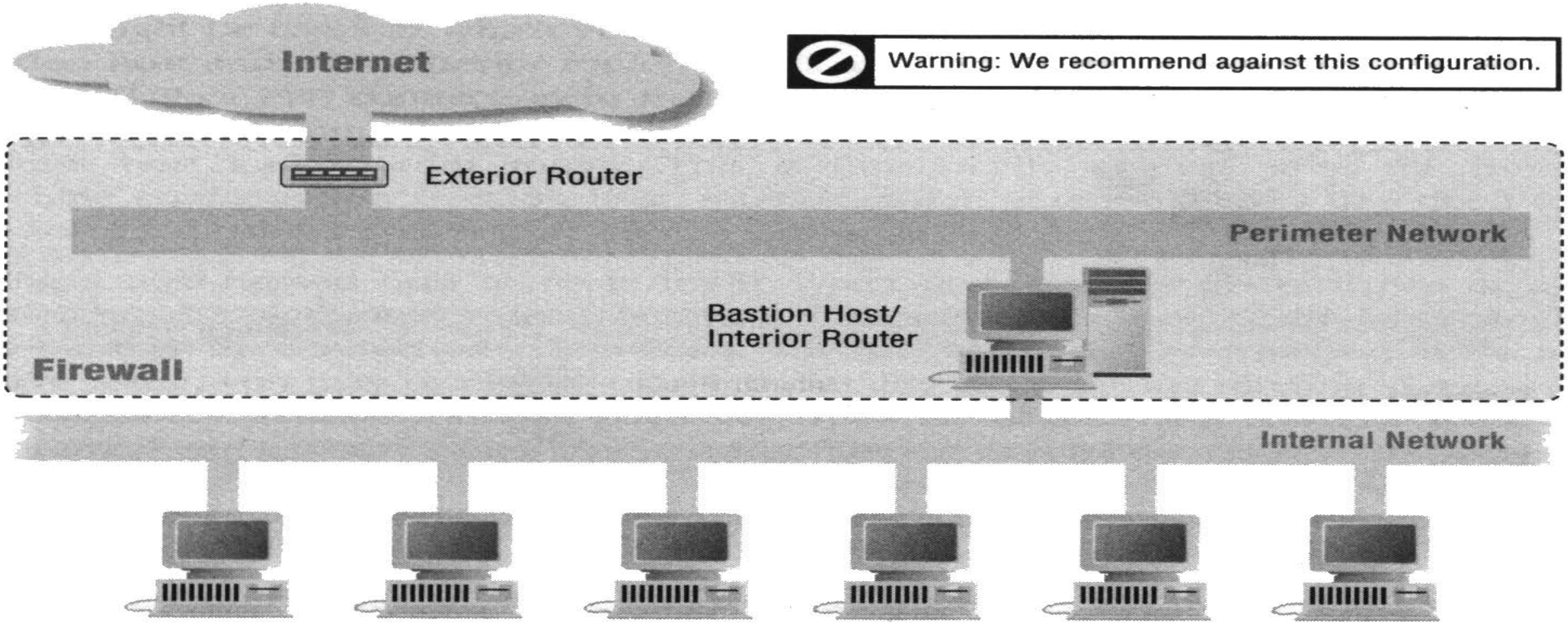
Merging bastion and Exterior Router

- Usually for PPP or SLIP



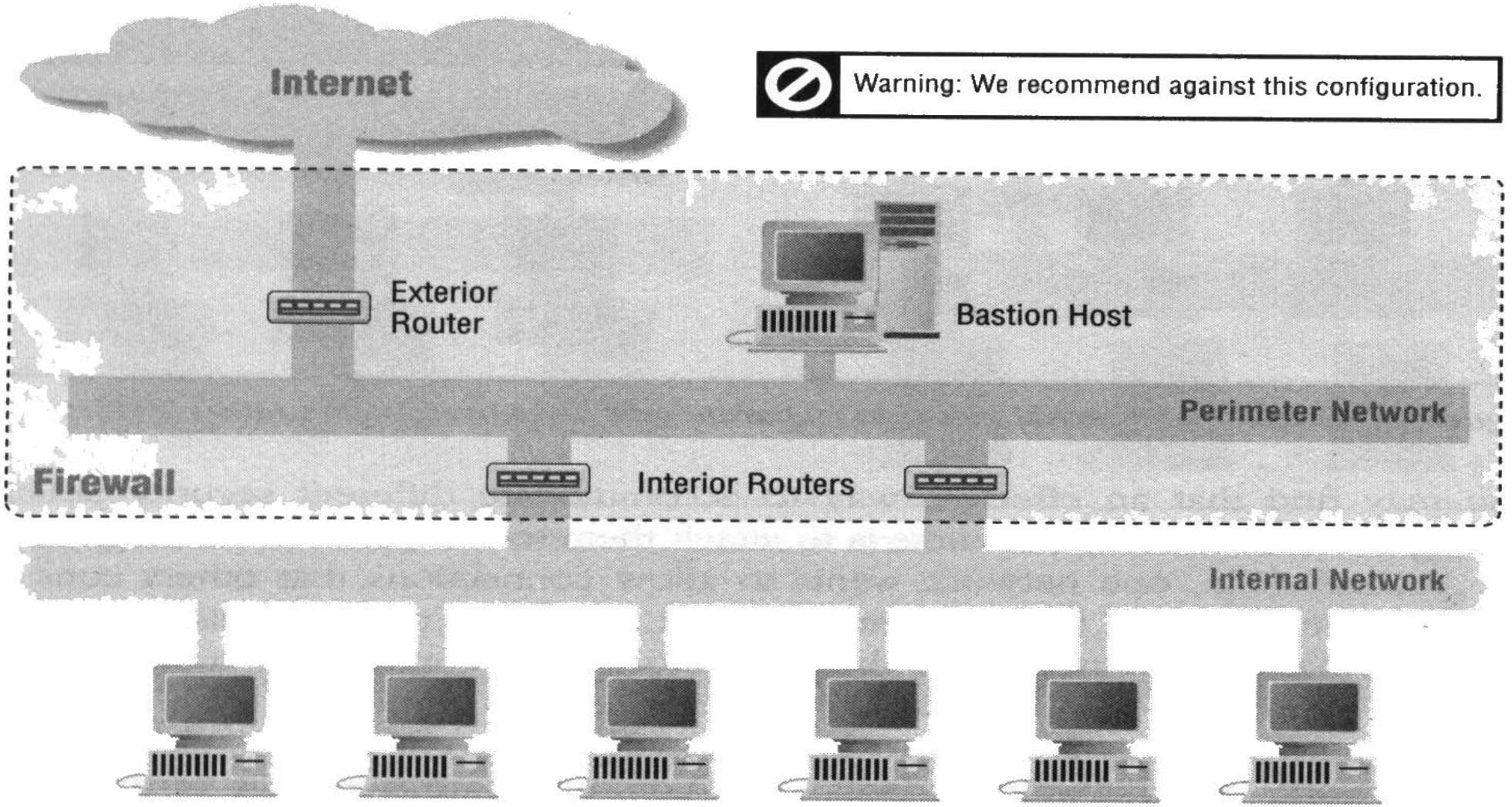
Merging bastion and Interior Router

- Intruded bastion host can see EVERYTHING.
- DANGEROUS!!!



Multiple Interior Routers

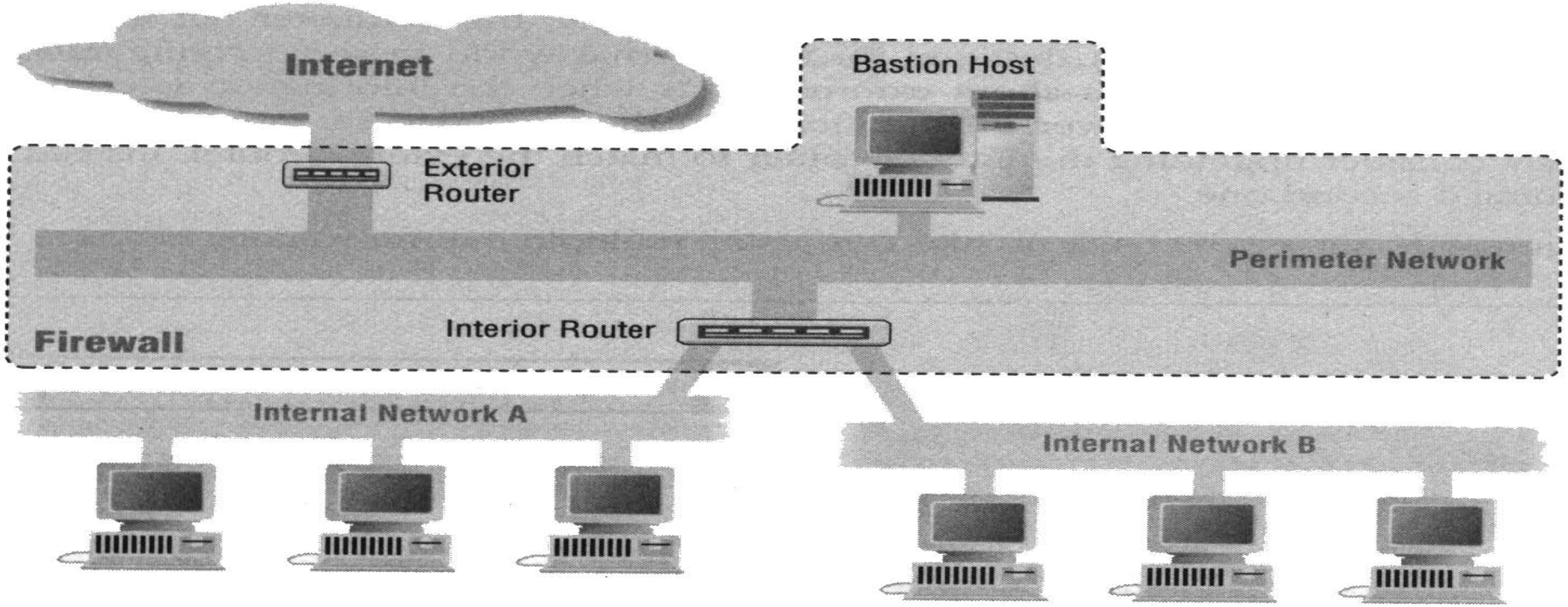
- Bad Ideas!! Why?
  - The perimeter network may become a route for one internal network to another, then expose internal data.
  - More interior routers will increase break-in chances.
  - Difficult to keep multiple interior routers correctly configured.
- What if the interior router is really a performance bottleneck? (Actually, rare.) Cases:
  - More traffic on Interior than Exterior (must reconfig)
  - Exterior is faster than Interior


Internet
Warning: We recommend against this configuration.
Exterior Router
Bastion Host
Perimeter Network
Firewall
Interior Routers
Internal Network

Multiple Interior Routers (Alternative)

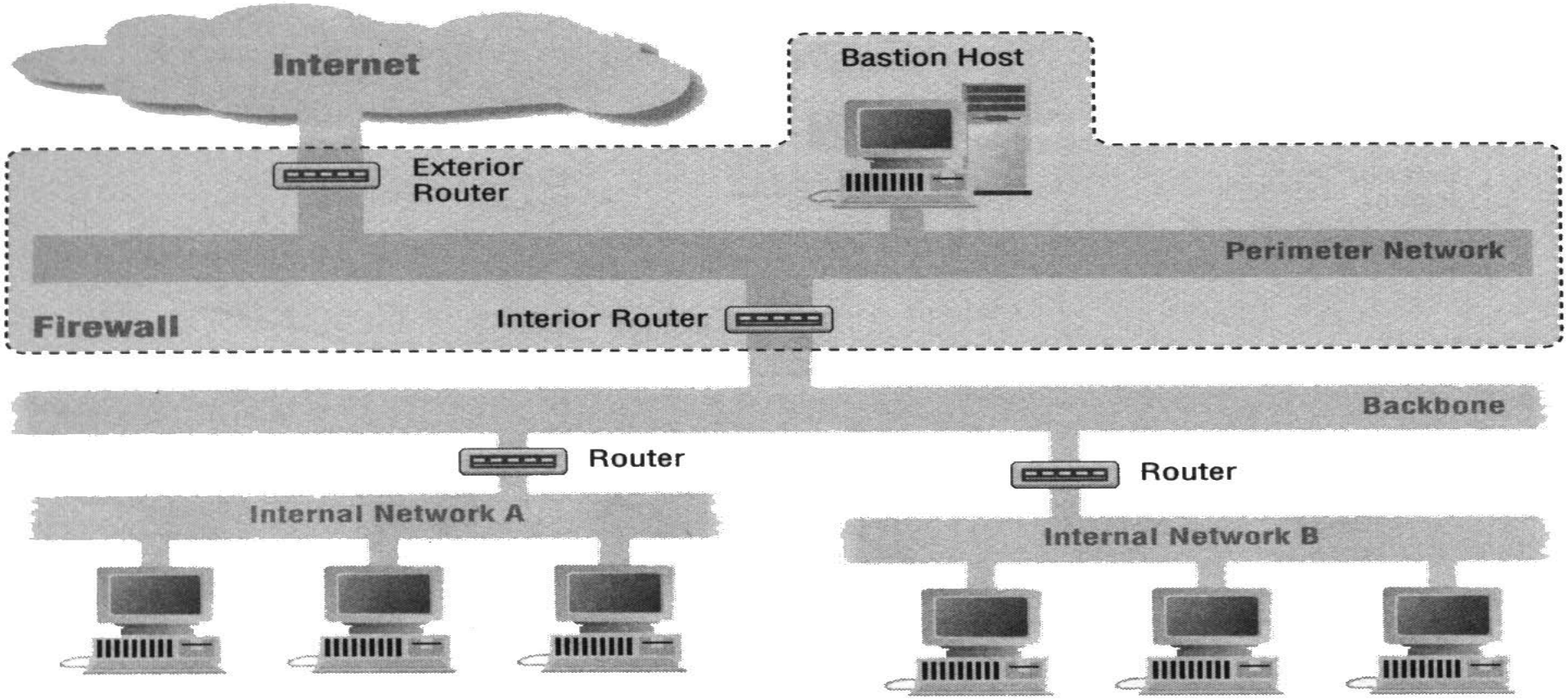
- Another reason: organizational separation

Multiple internal networks:



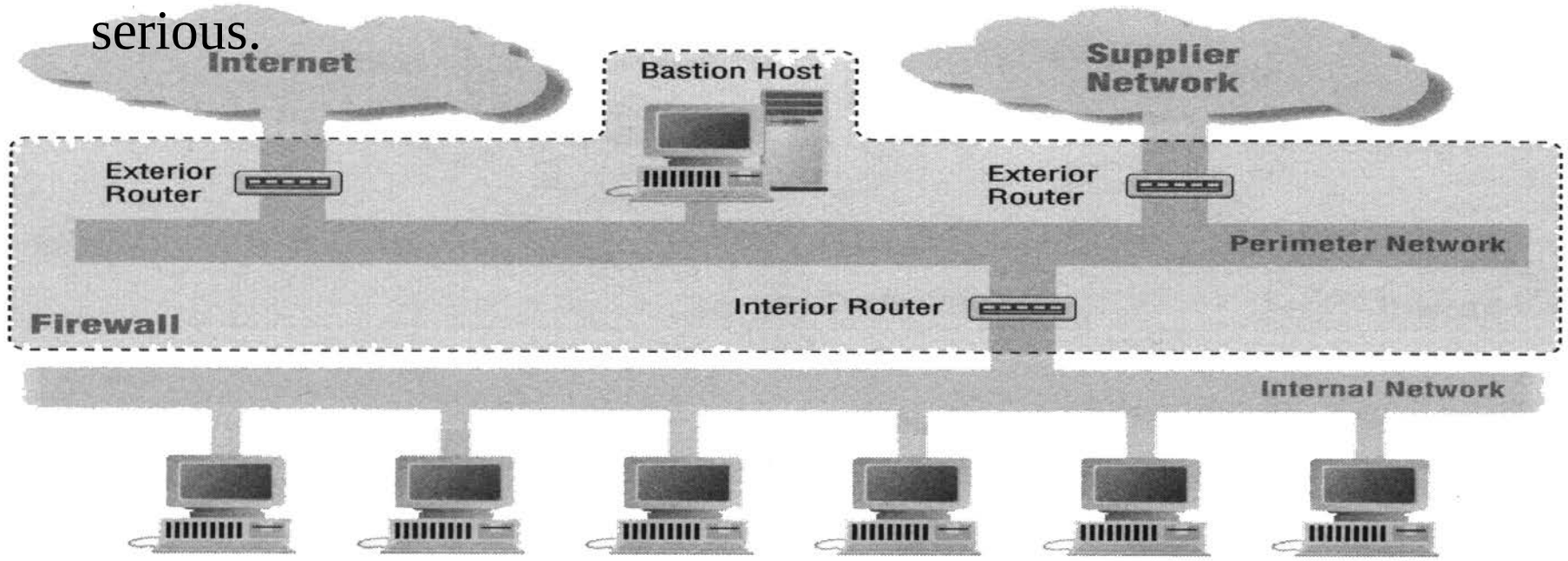
Multiple Internal Networks

- Backbone architecture:



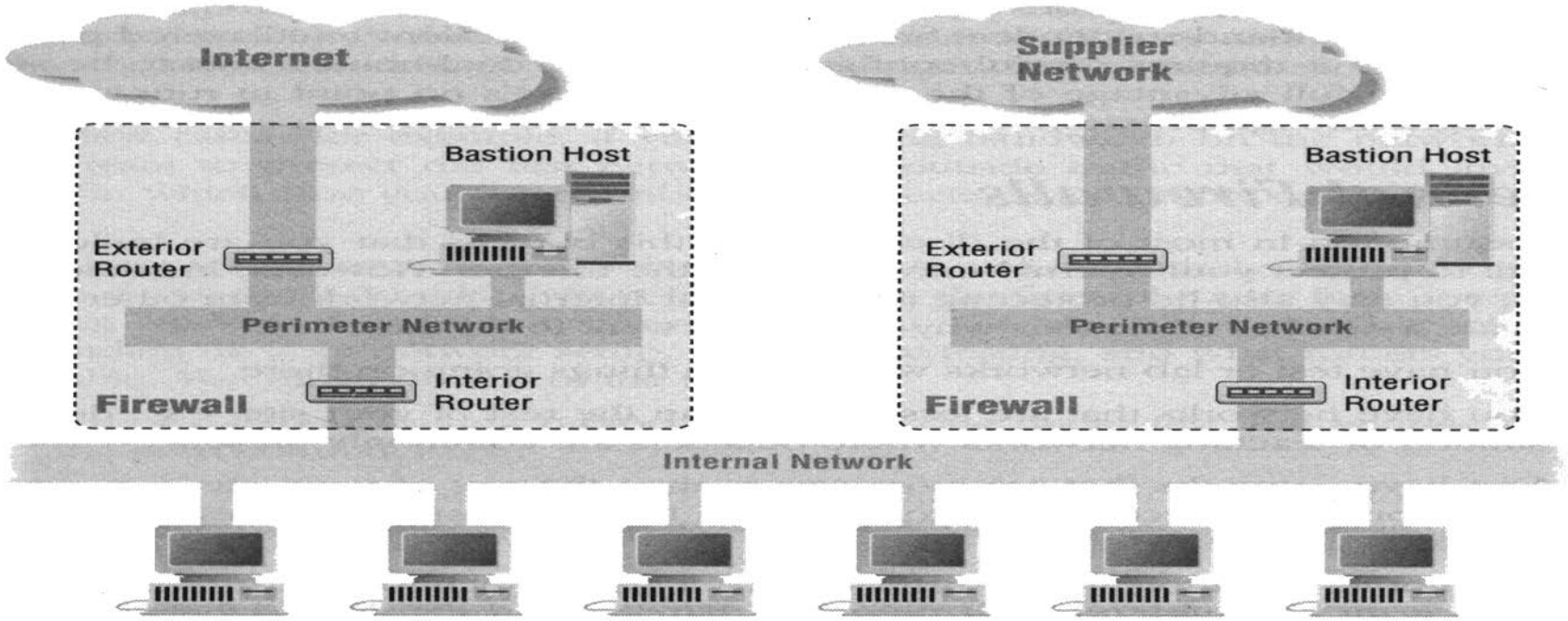
Multiple Exterior Routers

- Examples
  - Multiple connections to Internet (different ISPs)
  - A connection to Internet and another for other sites
- Security: A little easier to break in perimeter, but it is not serious.



Multiple Perimeter Networks

- No serious security problem.
- Used when the company is really big.
- Non-sense for providing two lines



Internal Firewalls

- Reasons:
  - A test or lab network (might send weird messages)
  - Less secure networks (e.g., for teaching)
  - Network requiring more security (e.g., secret project, financial or grade data)
- Types
  - Laboratory Networks
  - Insecure Networks
  - Extra-Secure Networks
  - Joint-Venture Firewalls

Lab Networks

- Why? May have horrible experience there.
- Configuration:
  - No exterior router and bastion hosts
  - Only need a packet filtering router
    - inbound (to the lab network) connections: Almost all ok.
    - outbound connections: only known safe ones.
  - If do testing routers,
    - disconnect the whole test networks.
    - Use a different routing protocol
    - Do not accept any routing updates
    - Specify which hosts the router will accept updates

Insecure Networks

- Examples:
  - dormitory network (most dangerous)
    - just viewed as exterior networks
  - training network (less dangerous)
  - demo network (less dangerous)
    - just use packet filtering router or a dual-homed host to prevent confidential traffic from flowing across those networks.
    - ask trusted users not to expose passwords or important information through there.
    - Usually, use a dual-homed host to send a warning message for crossing messages.

Extra Secure Network

- Encrypting traffic
- Separate networks
  - No bastion host
  - A perimeter network is needed only for the most secret
- Cases:
  - Universities: try to put on different secure networks.
  - Government or companies: since most share the same network, use encrypted messages.

Joint-Venture Firewalls (Extranet)

- Examples:
  - common data for Apple and IBM collaboration.
- Problems:
  - collaborators may steal information or break in.
  - Even if not competitors, they may find a way to their competitors.
- Factors (to decide how to do):
  - What you want to link for?
  - If just email or files, why not UUCP, etc?
  - Need a full work?

What the Future Holds

- Extranet will get more important
- IPv6 will cause profound changes in firewalls
- ATM will have less security problems.