Firewall Design

reference

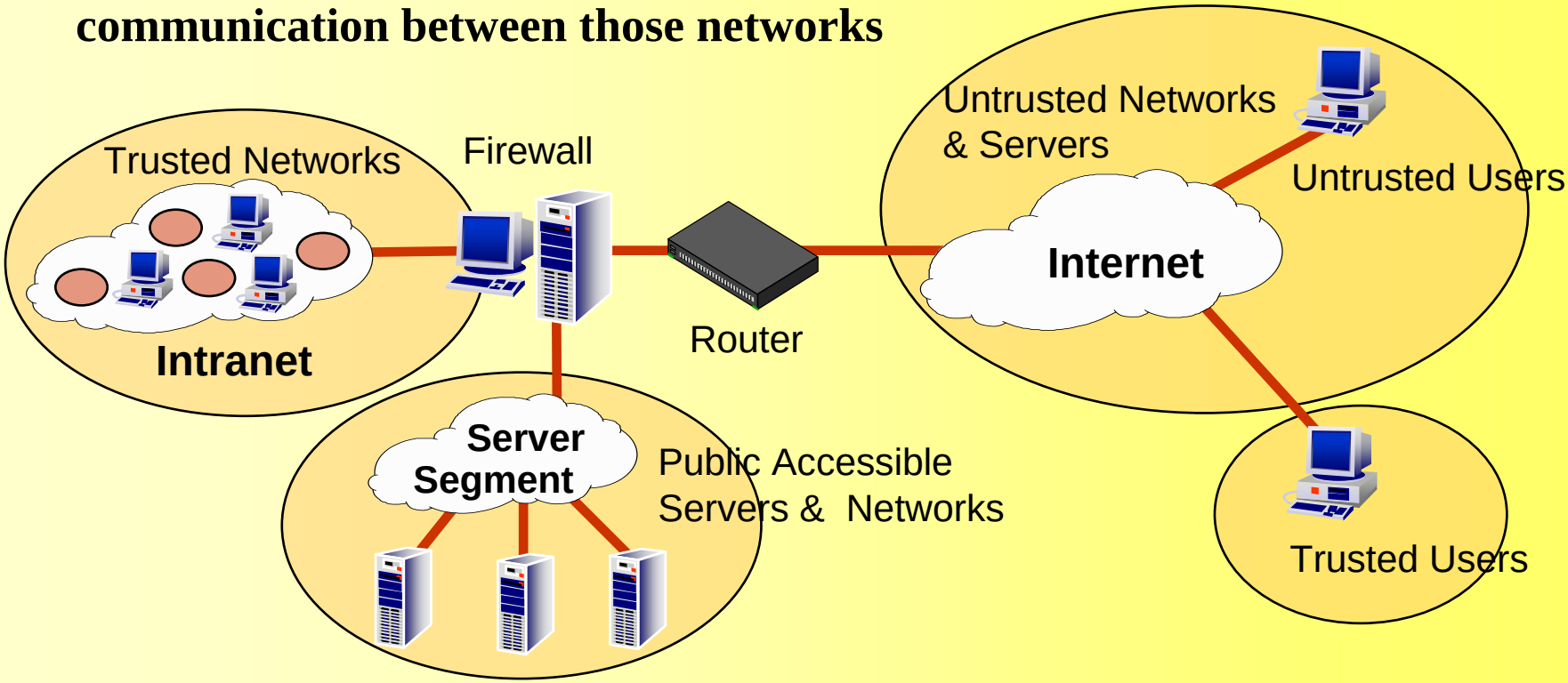
- D. Brent Chapman & Elizabeth D. Zwicky, **Building Internet Firewalls**, 1st Edition September 1995.
- Chris Hare, Karanjit Siyan, **Internet Firewalls and Network Security**, New Ricers Publishing, Indeanapolis, Indiana, 1995.
  - 刘成勇，刘明刚，王明举等译，网络安全技术系列丛书，**Internet防火墙与网络安全**，机械工业出版社，西蒙与舒斯特国际出版公司，1998年5月第1版。

Contents

1. Introduction

What Is A Firewall?

- **Device that connects networks (internal and/or external with varying levels of trust)**
- **Used to implement and enforce a *Security Policy* regarding communication between those networks**



Firewall can do

- A firewall is a focus for security decisions
  - All traffic in and out must pass through this single , narrow choke point which connects your network to Internet.
- A firewall can enforce a security policy.
- A firewall can log Internet activity efficiently.
- A firewall limits your exposure
  - Firewall can be used to keep one section of your site’s network separate from another section.

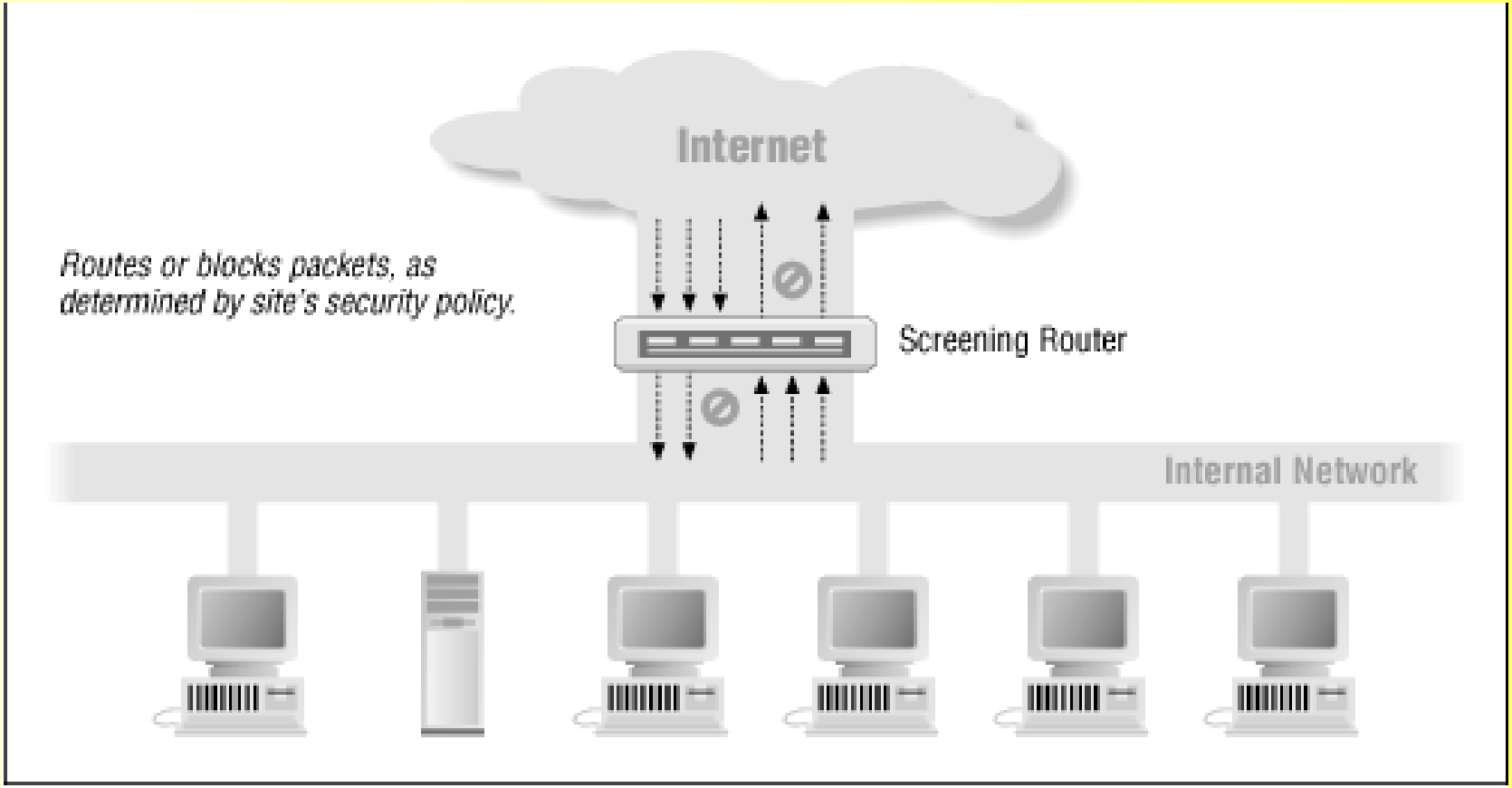
Firewall can’t do

- A firewall can’t protect you against malicious insiders;
- A firewall can’t protect you against connections that don’t go through it
- A firewall can’t protect against completely new threats
- A firewall can’t fully protect against viruses
- A firewall can’t set itself up correctly

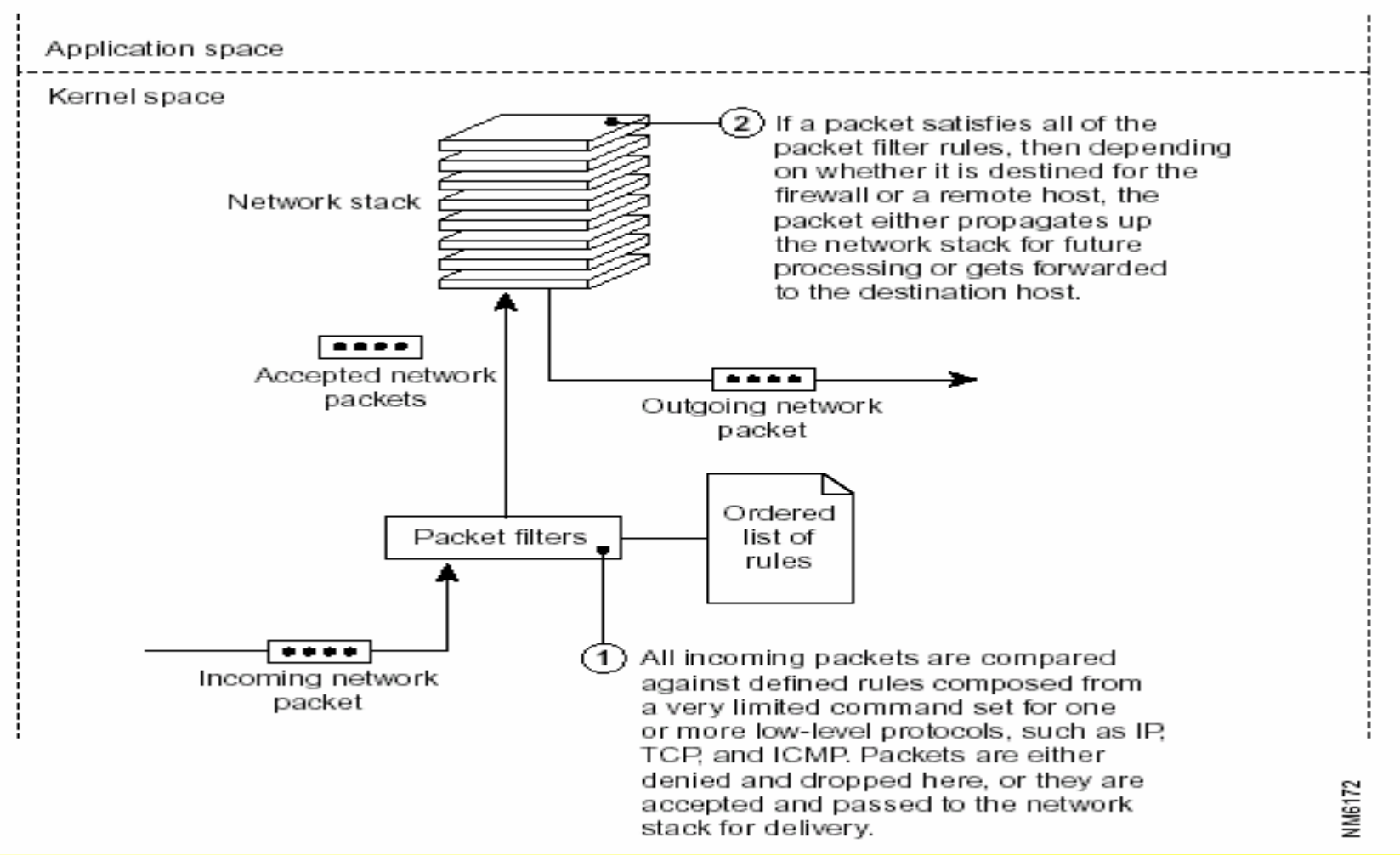
2. Firewall techniques

I. **Packet filter**
II. **Circuit level firewall**
III. **Application Layer Firewall**
IV. **Dynamic Packet Filter**

2.1 Packet filter



Packet Filter Architecture



Packet filter control data transfer based on

- The address the data is (supposedly) coming from
- The address the data ia going to
- The session and application ports being used to transfer the data

It let you can say

- Don’t let anybody use the port used by Telnet to log in from the outside
- Let everybody send us data over the port used for electronic mail by SMTP.

It won’t let you say

- This user can Telnet in from outside , but no other users can do so.
- You can transfer these files byt not those files.
- Only allow people to send us electronic mail over the port used by SMTP.

Advantages of the packet filtering

- Packet filters are generally faster than other firewall technologies;
- They can easily be implemented as hardware solutions;
- A single rule can help protect an entire network by prohibiting connections between specific Internet sources and internal computers;
- Packet filters do not require client computers to be specifically configured;
- In conjunction with network address translation, you can use packet filter firewalls to shield internal IP addresses from external users.

Disadvantages of the packet filtering

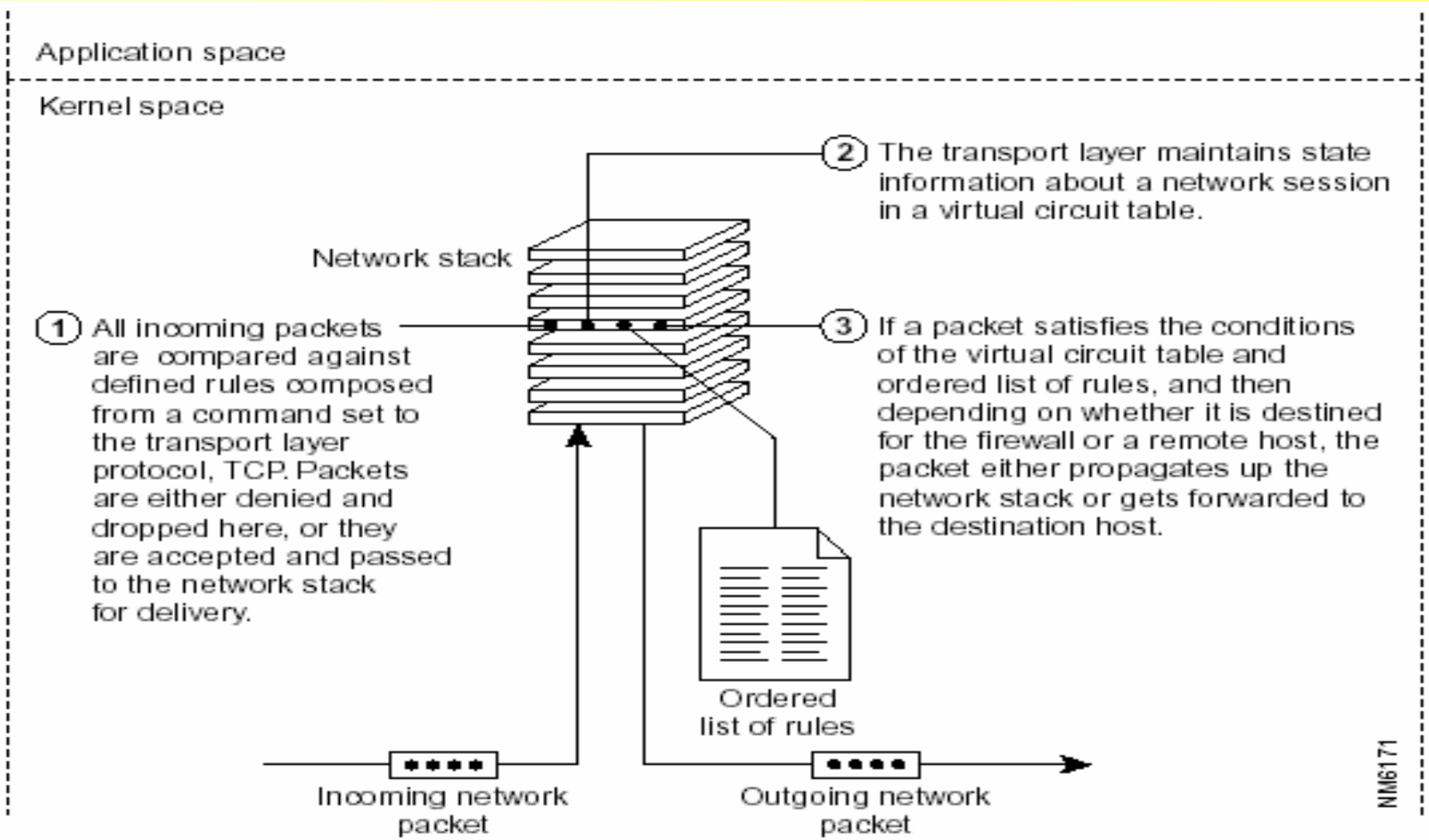
- They are less secure than application layer and circuit level firewalls.
  - **They cannot restrict access to protocol subsets for even the most basic services, such as the PUT or GET commands in FTP.**
- They do not keep information about a session or application-derived information.
- Packet filters do not offer value-added features, such as HTTP object caching, URL filtering, and authentication because they do not understand the protocols being used and cannot discern one from another.

2.2 Circuit level firewall

- Operate at the network transport layer
- Authorized based on addresses
- Prevent direct connections between one network and another

- Cannot look at data traffic flowing between one network and another

Circuit Level Firewall Architecture



- To validate a session, a circuit level firewall examines each connection setup to ensure that it follows a legitimate handshake for the transport layer protocol being used
- The firewall maintains a table of valid connections and lets network packets pass through when it matches an entry in the virtual circuit table.
- Once a connection is terminated, its table entry is removed, and that virtual circuit between the two peer transport layers is closed.

advantages of circuit level firewalls

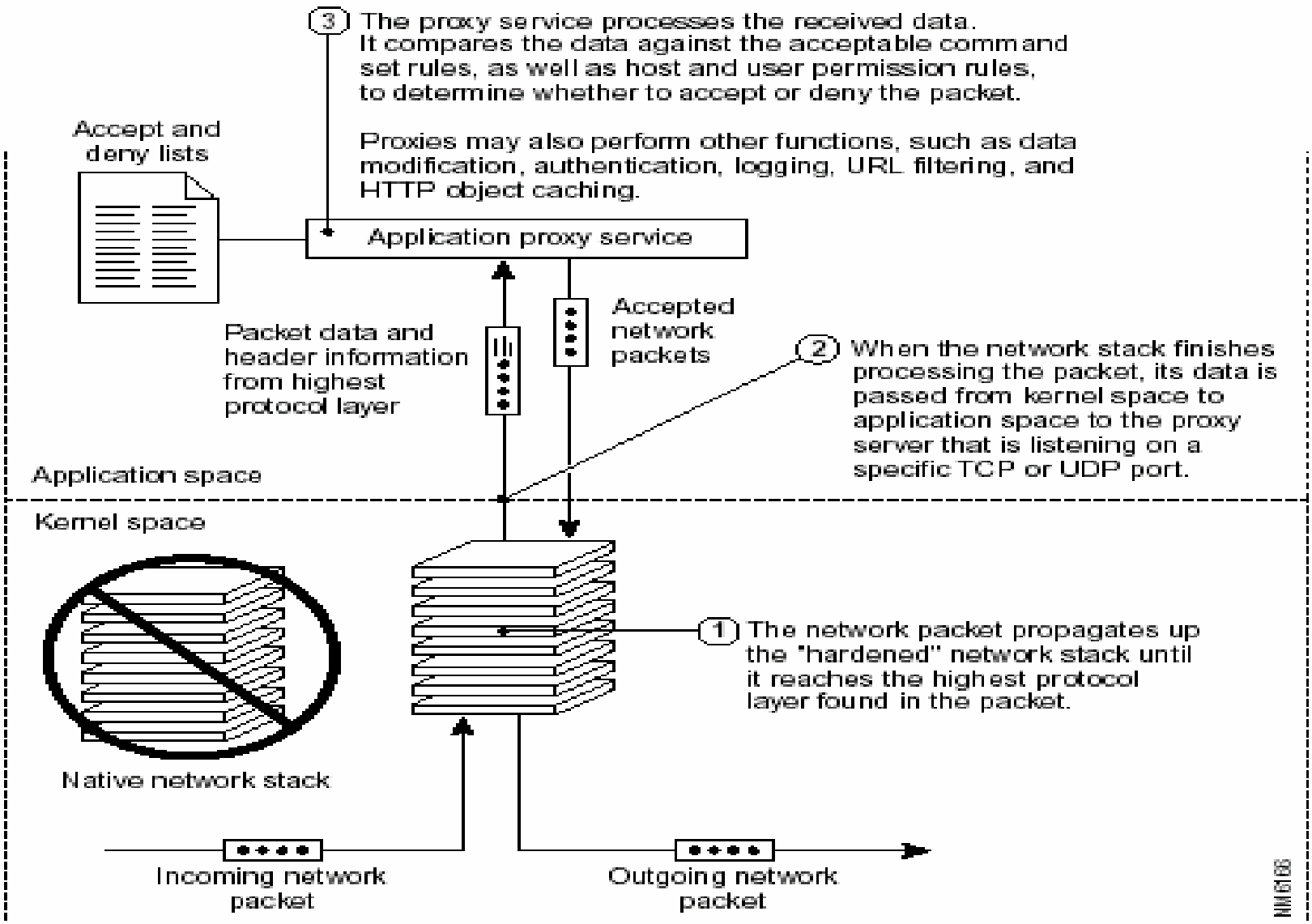
- Circuit level firewalls are generally faster than application layer firewalls.
- A circuit level firewall can help protect an entire network by prohibiting connections between specific Internet sources and internal computers.
- In conjunction with network address translation, you can use circuit level firewalls to shield internal IP addresses from external users.

disadvantages of circuit level firewalls

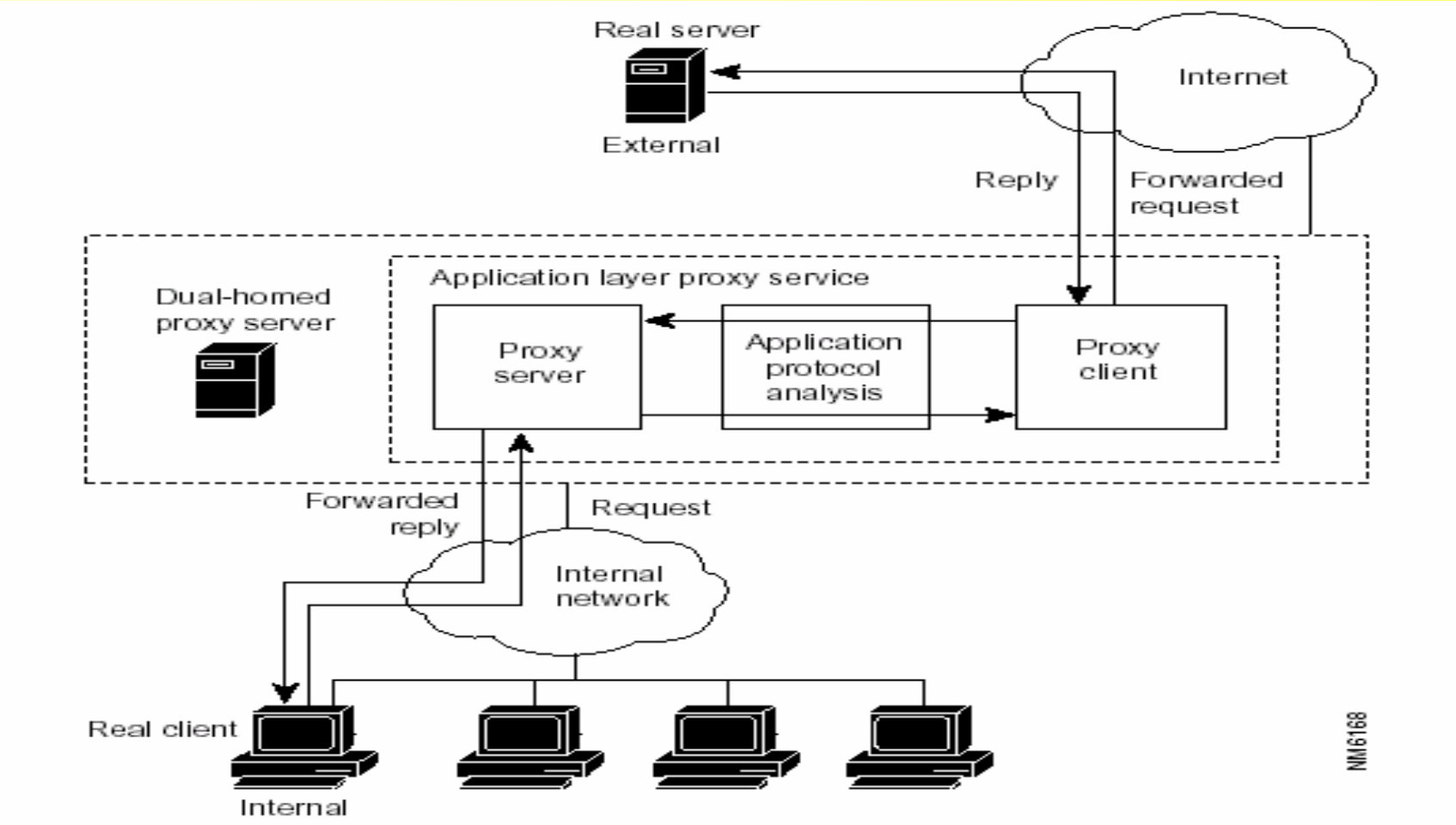
- Circuit level firewalls cannot perform strict security checks on a higher-level protocol should the need arise.
- Circuit level firewalls have limited audit event generation abilities but can typically tie a network data packet to an application layer protocol by building limited forms of session state.
- Circuit level firewalls do not offer value-added features, such as HTTP object caching, URL filtering, and authentication because they do not understand the protocols being used and cannot discern one from another.
- It can be difficult to test “accept” and “deny” rules.

2.3 Application Layer Firewall

Application Layer Firewall Architecture



How a Proxy Service Works



How a Proxy Service Works

- Proxy services are specific to the protocol
  - Forward
  - provide increased access control
  - careful detailed checks for valid data
  - generate audit records about the traffic

How a Proxy Service Works

- Each application proxy requires two components that are typically implemented as a single executable: a proxy server and a proxy client.
- A *proxy server* acts as the end server for all connection requests originated on a trusted network by a real client.
- Proxy servers understand the protocol of the service. they only allow those packets through that comply with the protocol definitions.
- They also enable additional benefits, such as detailed audit records of session information, user authentication, and caching.
- A *proxy client* is part of a user application that talks to the real server on the external network on behalf of the real client.

Advantages of proxy services

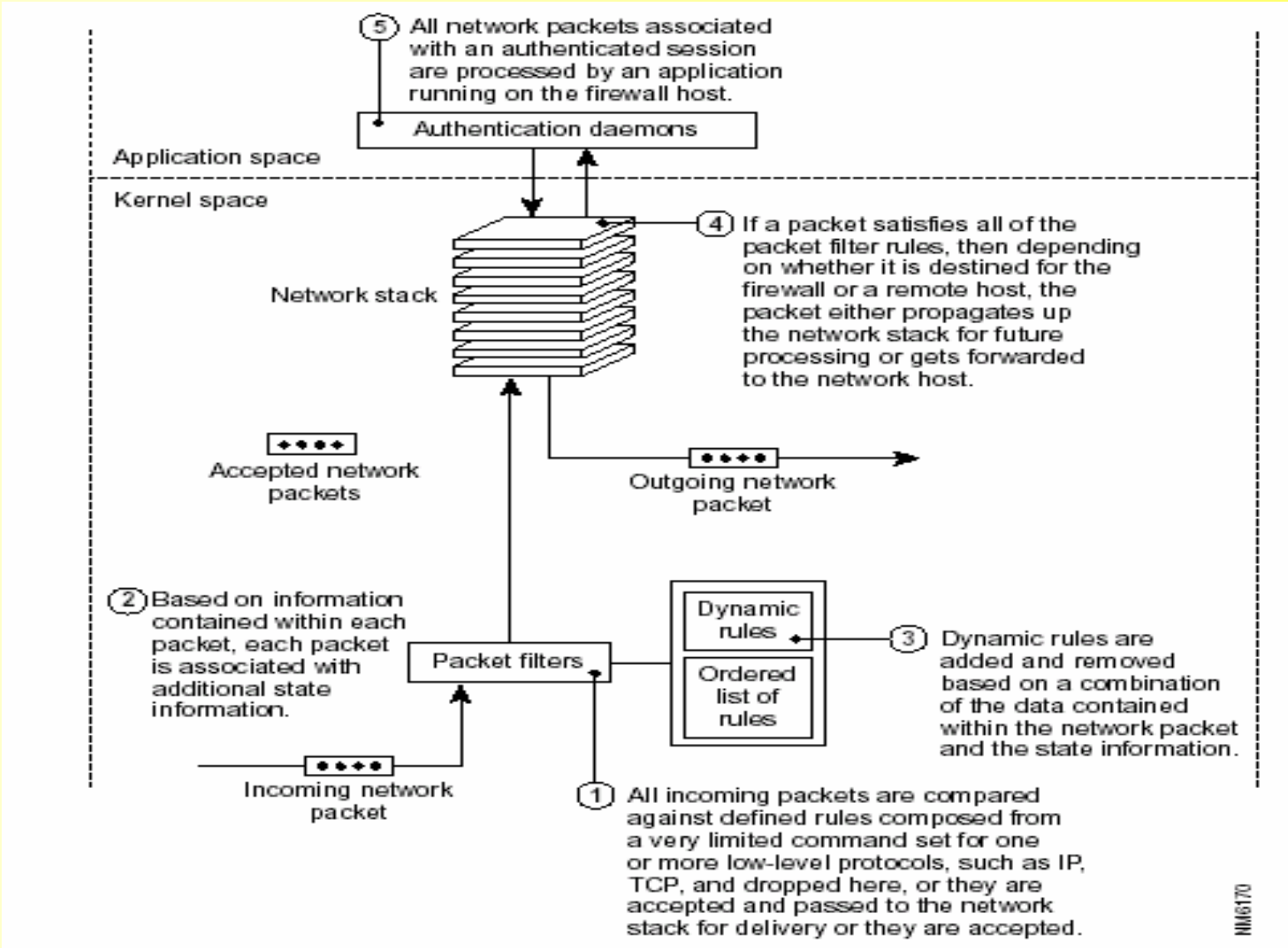
- Proxy services understand and enforce high-level protocols, such as HTTP and FTP.
- Proxy services are also capable of processing and manipulating packet data.
- Proxy services do not allow direct communications between external servers and internal computers
- Proxy services are good at generating audit records, allowing administrators to monitor attempts to violate the firewall's security policies.

Disadvantages of Proxy services

- Proxy services require you to replace the native network stack on the firewall server.
- a new proxy must be written for each protocol that you want to pass through the firewall.

2.4 Dynamic Packet Filter

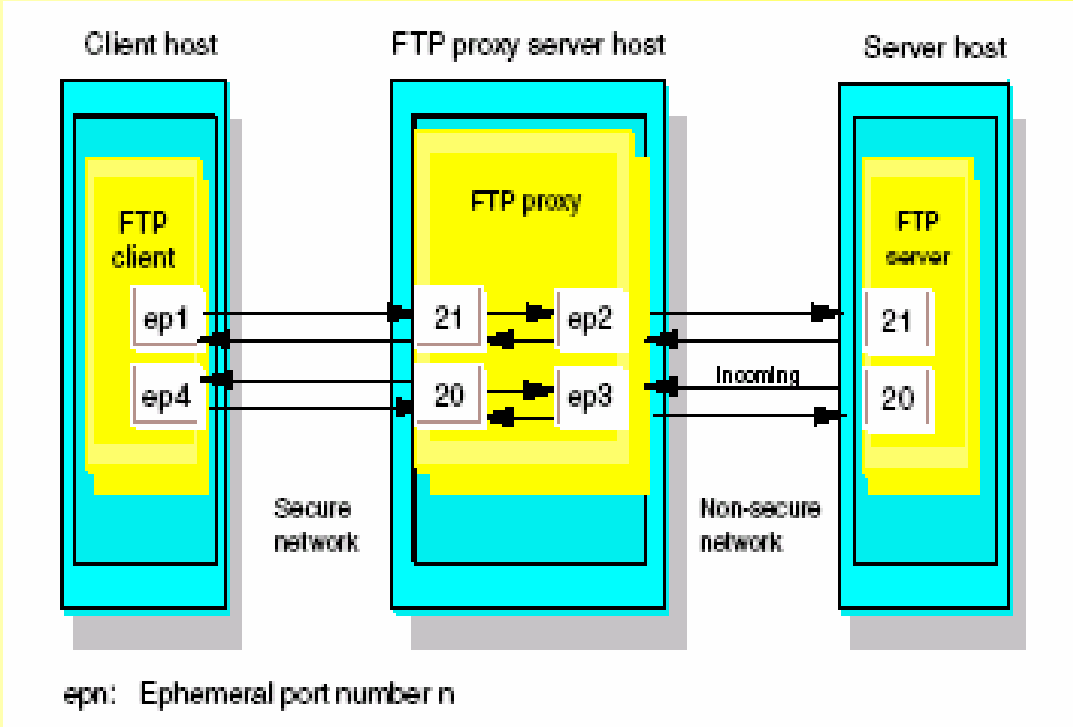
Dynamic Packet Filter Architecture



Normal mode FTP

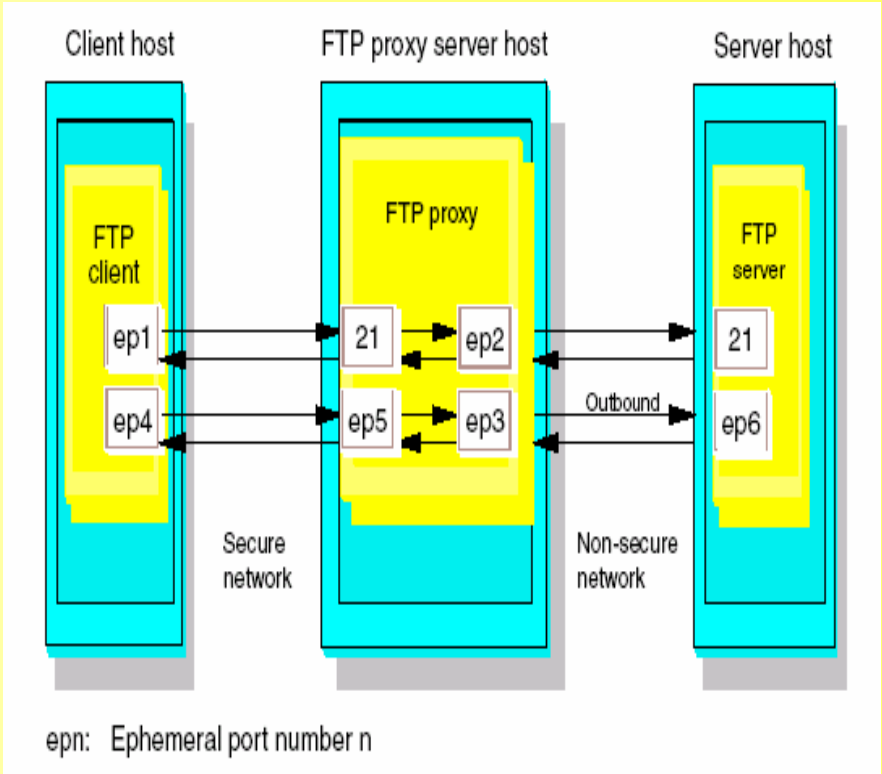
- A connection is established from the FTP server port 20 in the non-secure network to the FTP proxy server's ephemeral port number. To allow this to happen, IP filtering rules are used that allow inbound connection requests from port 20 to an ephemeral port number on the FTP proxy host.

- It would allow a cracker to run a program on port 20 and scan all the port numbers above 1023.



Passive mode FTP

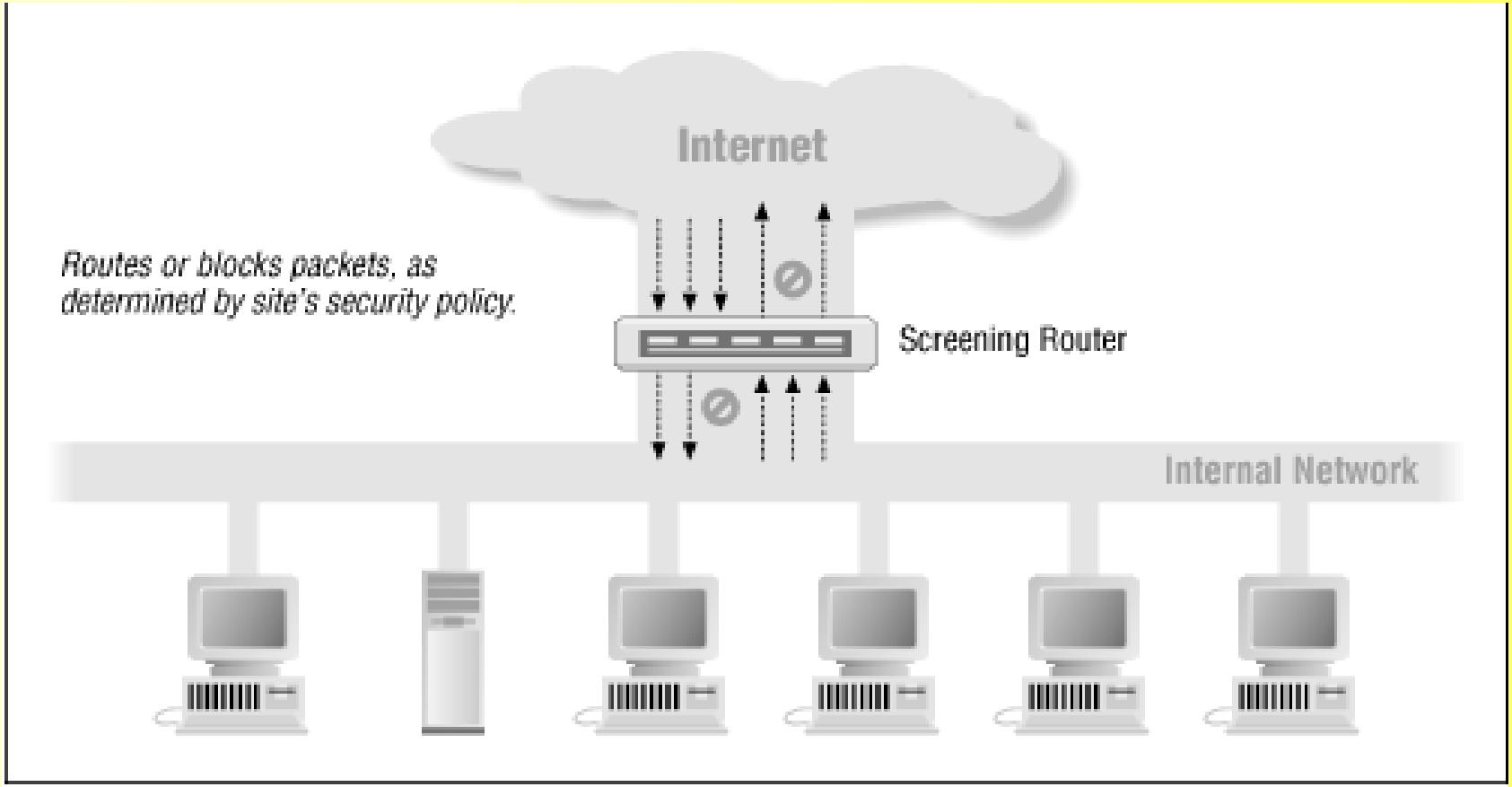
- In passive mode, the FTP client again establishes a control connection to the server's port 21.
- When data transfer has to start, the client sends a PASV command to the server.
- The server responds with a port number for the client to contact.
- In order to establish the data connection, and the client then initiates the data connection.



3. Firewall Architectures

I. **Single-box architecture**
II. **Screened Host Architecture**
III. **Screened Subnet Architecture**

3.1.1 Screening router



3.1.1 Screening router

- A low-cost system
- You can permit or deny protocols by port number.
- It is hard to allow some operations while denying others in the same protocol
- It gives you no depth of defense
  - If the screen router is compromised, you have no further security

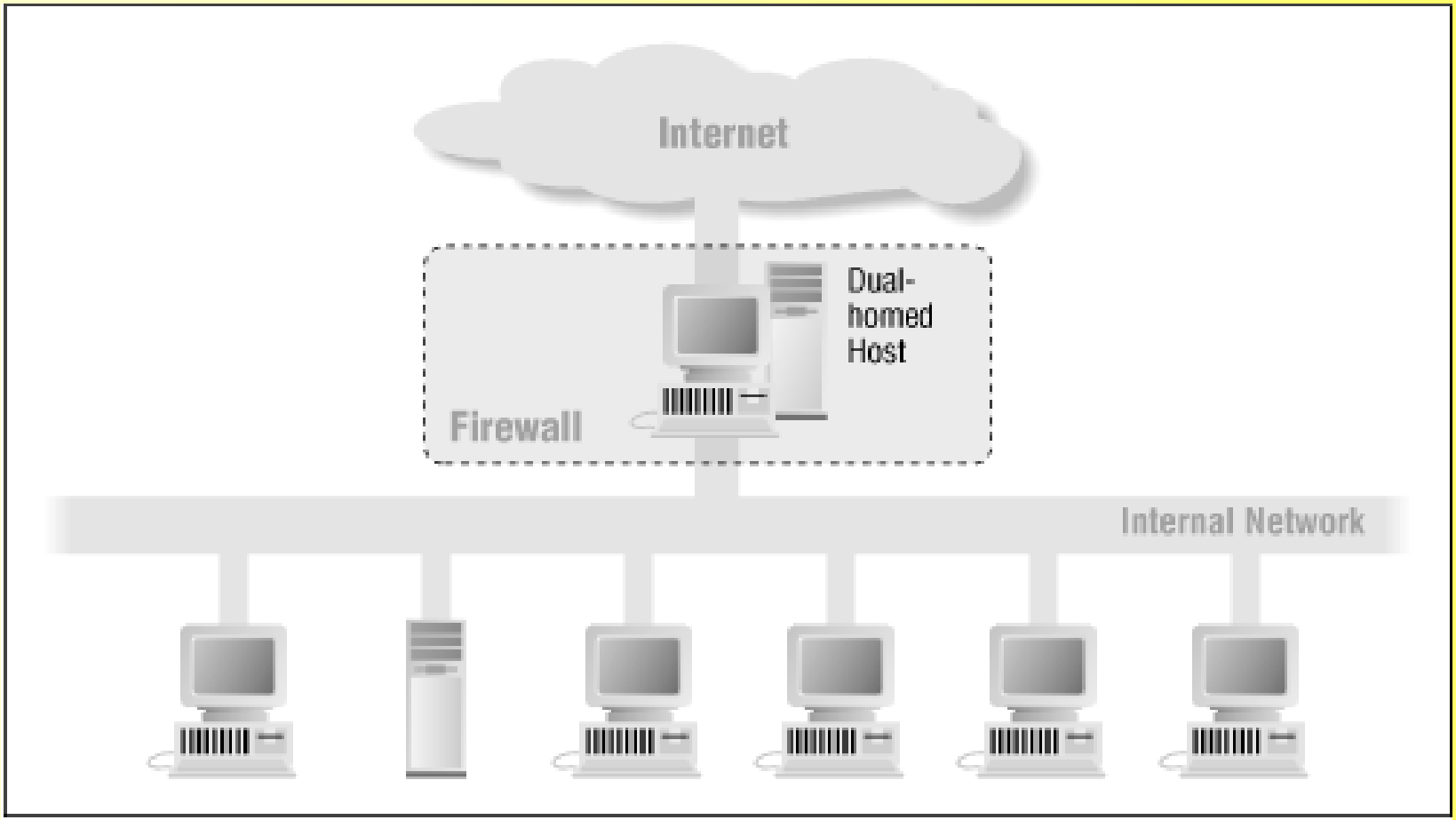
3.1.1 Screening router

- A screening router is an appropriate firewall for a situation:
  - The network being protected already has a high level of host security;
  - The number of protocols being used is limited;
  - You require maximum performance and redundancy.

3.1.1 Screening router

- Useful for internal firewalls
- Useful for networks that are dedicated to providing services to the Internet;
- It is common for internet service providers to use nothing but a screening router between their services hosts and the Internet.

3.1.2 A dual-homed host architecture



3.1.2 A dual-homed host architecture

- To implement a dual-homed host type of firewalls architecture, you disable its routing function.
  - IP packets from one network are not directly routed to the other network;
  - Systems inside the firewall can communicate with the dual-homed host;
  - Systems outside the firewall (on the Internet) can communicate with the dual-homed host;
  - These systems can't communicate directly with each other. IP traffic between them is completely blocked.

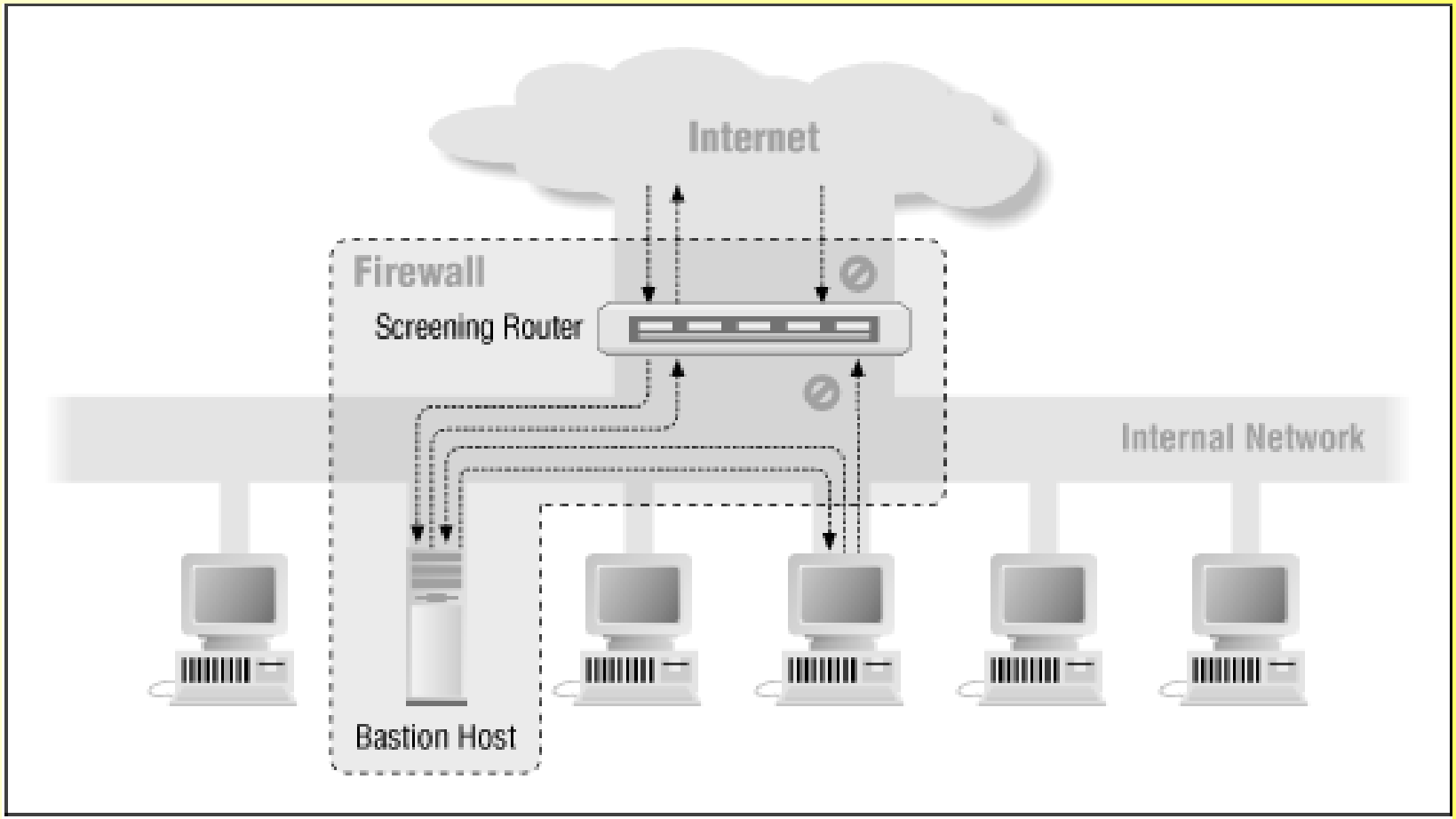
3.1.2 A dual-homed host architecture

- Since a dual-homed host is a single point of failure, it's important to make certain that its host security is absolutely impeccable;
- A dual-homed host can only provide services by proxying them;
- Proxing is much better at supporting outbound services than inbound services;

3.1.2 A dual-homed host architecture

- A dual-homed host is an appropriate firewall for a situation where
  - Traffic to the Internet is small;
  - Traffic to the Internet is not business-critical;
  - No services are being provided to Internet-based users;

3.2 a screened host architecture (1)



3.2 a screened host architecture (2)

- a *screened host architecture* provides services from a host that's attached to only the internal network, using a separate router.
- In this architecture, the primary security is provided by packet filtering.
  - For example, packet filtering is what prevents people from going around proxy servers to make direct connections.

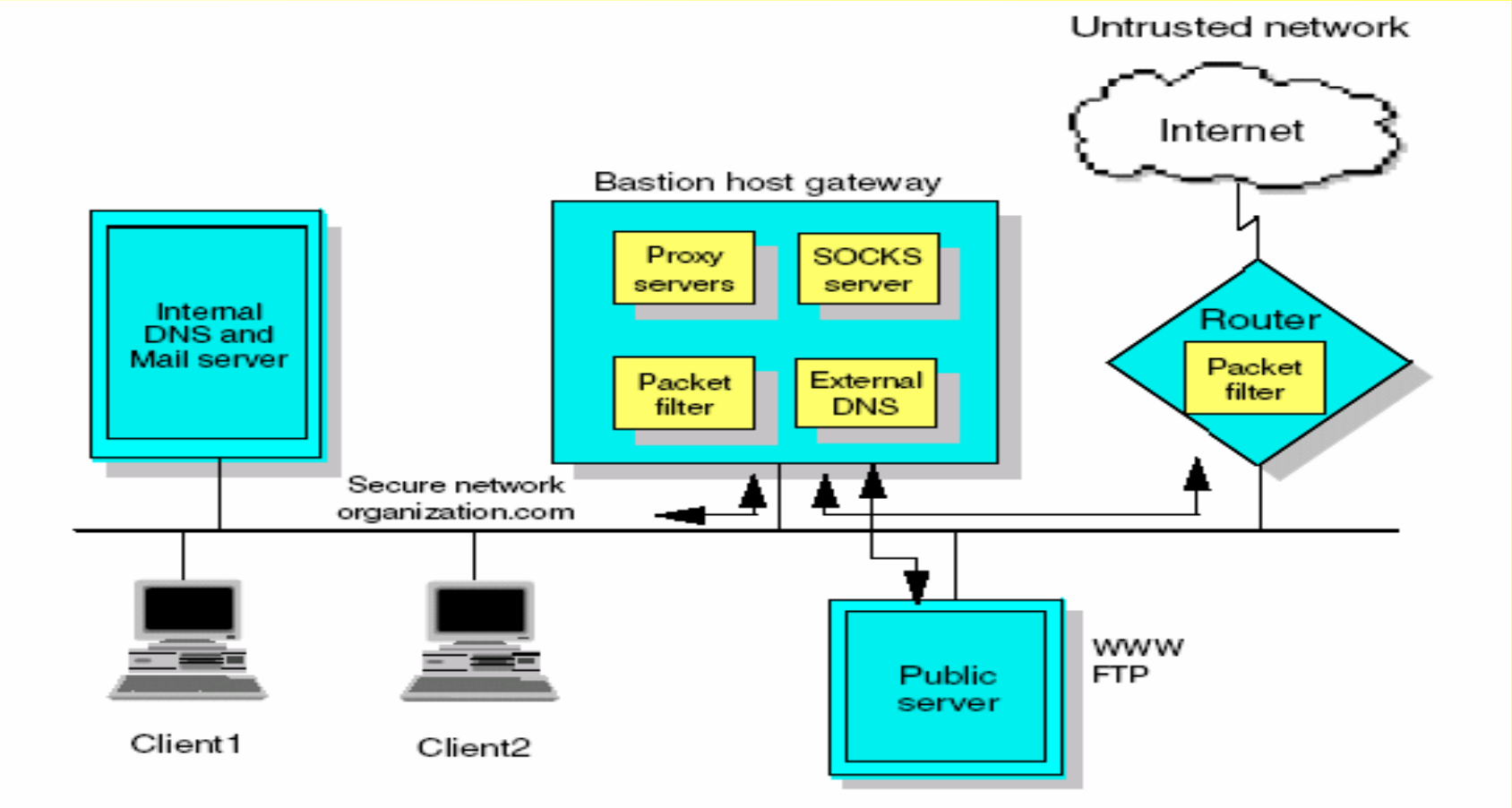
3.2 a screened host architecture (3)

- The bastion host sits on the internal network.
- The packet filtering on the screening router is set up in such a way that
  - the bastion host is the only system on the internal network that hosts on the Internet can open connections to (for example, to deliver incoming email).
  - only certain types of connections are allowed.
  - Any external system trying to access internal systems or services will have to connect to this host.

3.2 a screened host architecture (4)

- The packet filtering also permits the bastion host to open allowable connections (what is "allowable" will be determined by your site's particular security policy) to the outside world.

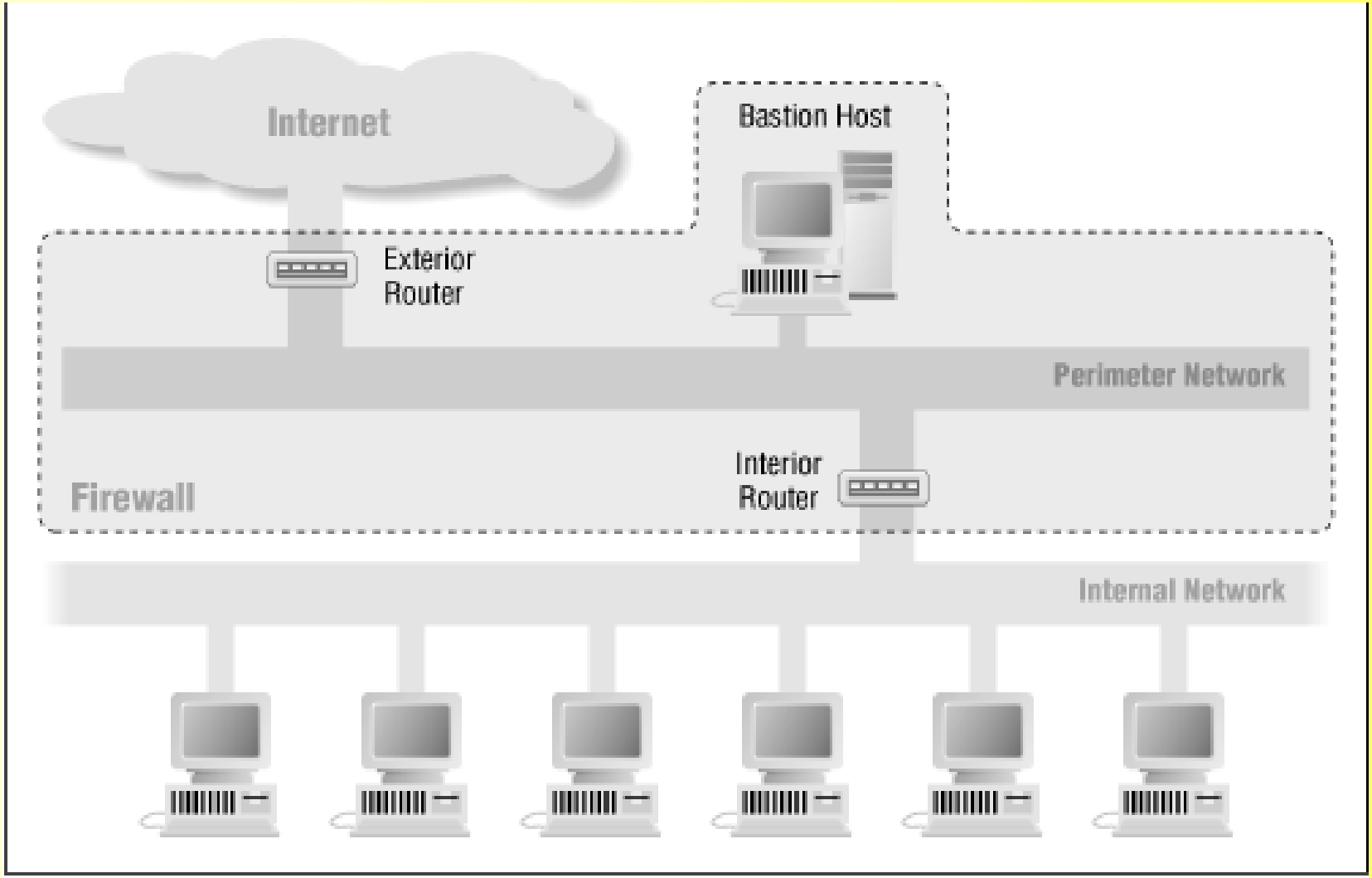
3.2 a screened host architecture (5)



3.2 a screened host architecture (6)

- some disadvantages to the screened host architecture
  - if an attacker manages to break in to the bastion host, there is nothing left in the way of network security between the bastion host and the rest of the internal hosts.
  - The router also presents a single point of failure; if the router is compromised, the entire network is available to an attacker.
  - For this reason, the screened subnet architecture has become increasingly popular.

3.3 Screened subnet architecture（1）



3.3 Screened subnet architecture（2）

- The *screened subnet architecture* adds an extra layer of security to the screened host architecture
  - adding a perimeter network that further isolates the internal network from the Internet
- Why do this?
  - By their nature, bastion hosts are the most vulnerable machines on your network.
  - By isolating the bastion host on a perimeter network, you can reduce the impact of a break-in on the bastion host.

3.3 Screened subnet architecture（3）

- There are two screening routers .
- To break into the internal network with this type of architecture, an attacker would have to get past *both* routers.
- There is no single vulnerable point that will compromise the internal network.

3.3 Screened subnet architecture（4）

perimeter network

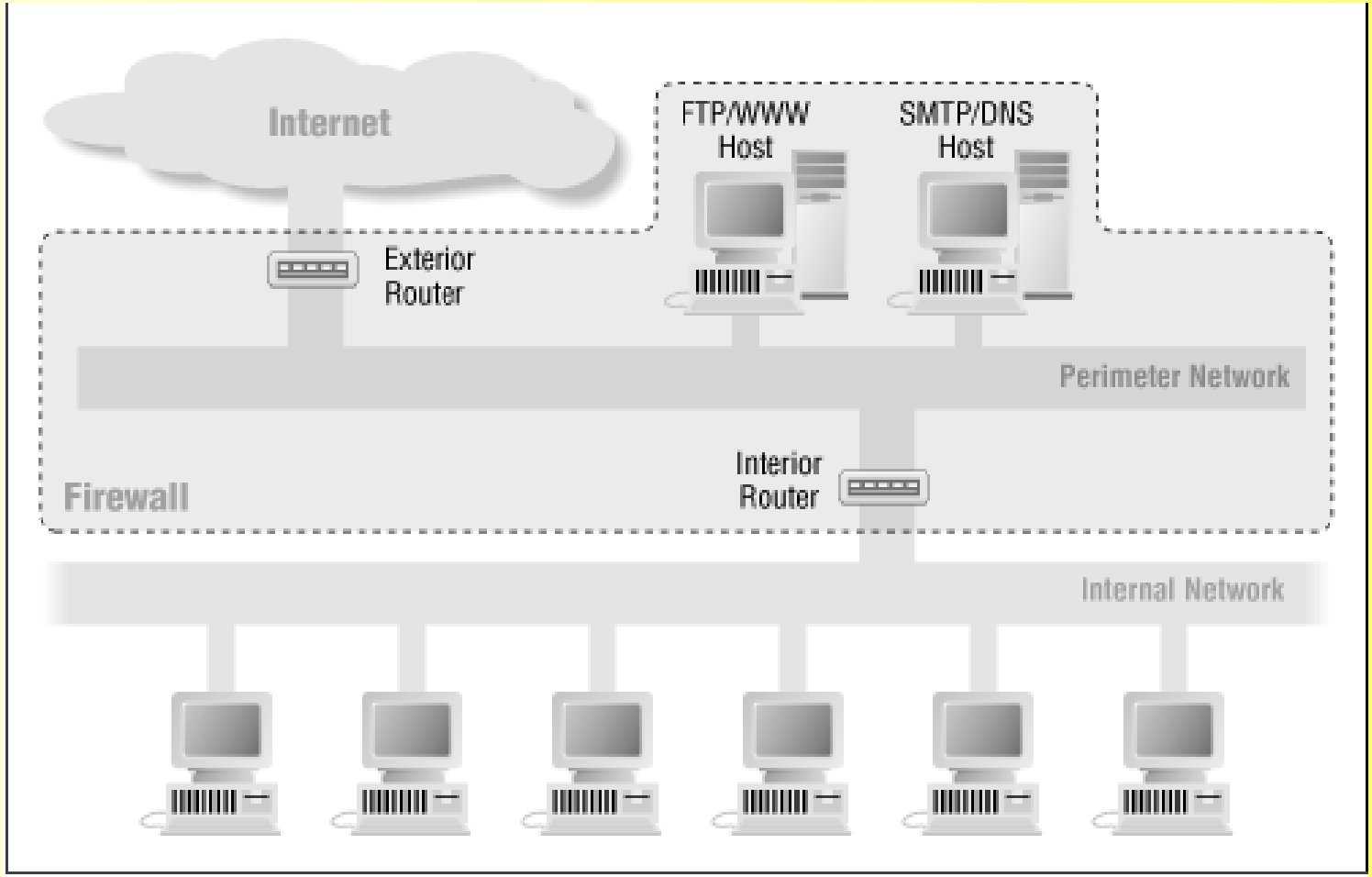
- If an attacker successfully breaks into the outer reaches of your firewall, the perimeter net offers an additional layer of protection between that attacker and your internal systems.
- the snooper can essentially "watch over the shoulder" of anyone using the network on the perimeter network, it he breaks into a bastion host.

3.3 Screened subnet architecture（5）

Bastion host

- Set up packet filtering on both the exterior and interior routers to allow internal clients to access external servers directly.
- Set up proxy servers to run on the bastion host to allow internal clients to access external servers indirectly.

3.4 Architecture using two bastion hosts



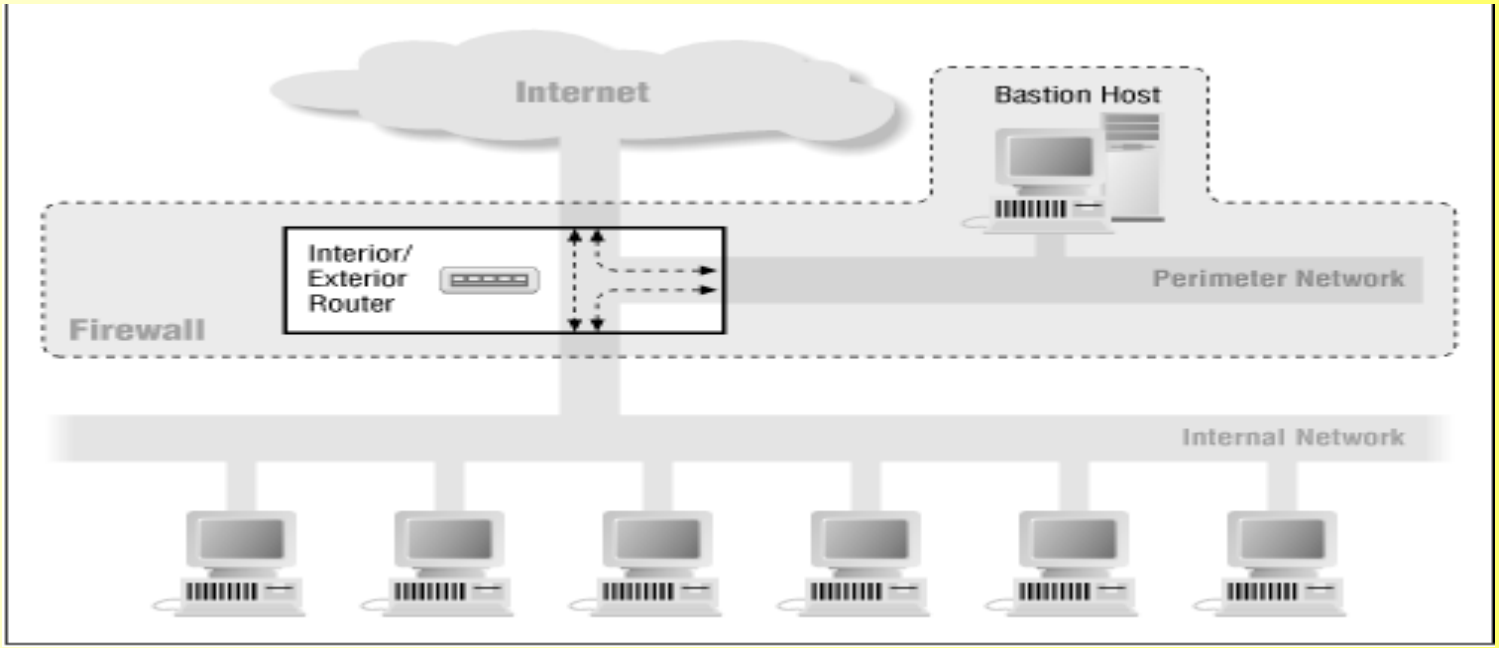
3.4 Architecture using two bastion hosts

- Reasons you might want to do this include performance, redundancy, and the need to separate data or servers.
  - one bastion host handle the services that are important to your own users (such as SMTP servers, proxy servers, and so on)
  - another host handles the services that you provide to the Internet, but which your users don't care about (for example, an anonymous FTP server).
  - In this way, performance for your own users won't be dragged down by the activities of outside users.
- You may have performance reasons to create multiple bastion hosts

3.4 Architecture using two bastion hosts

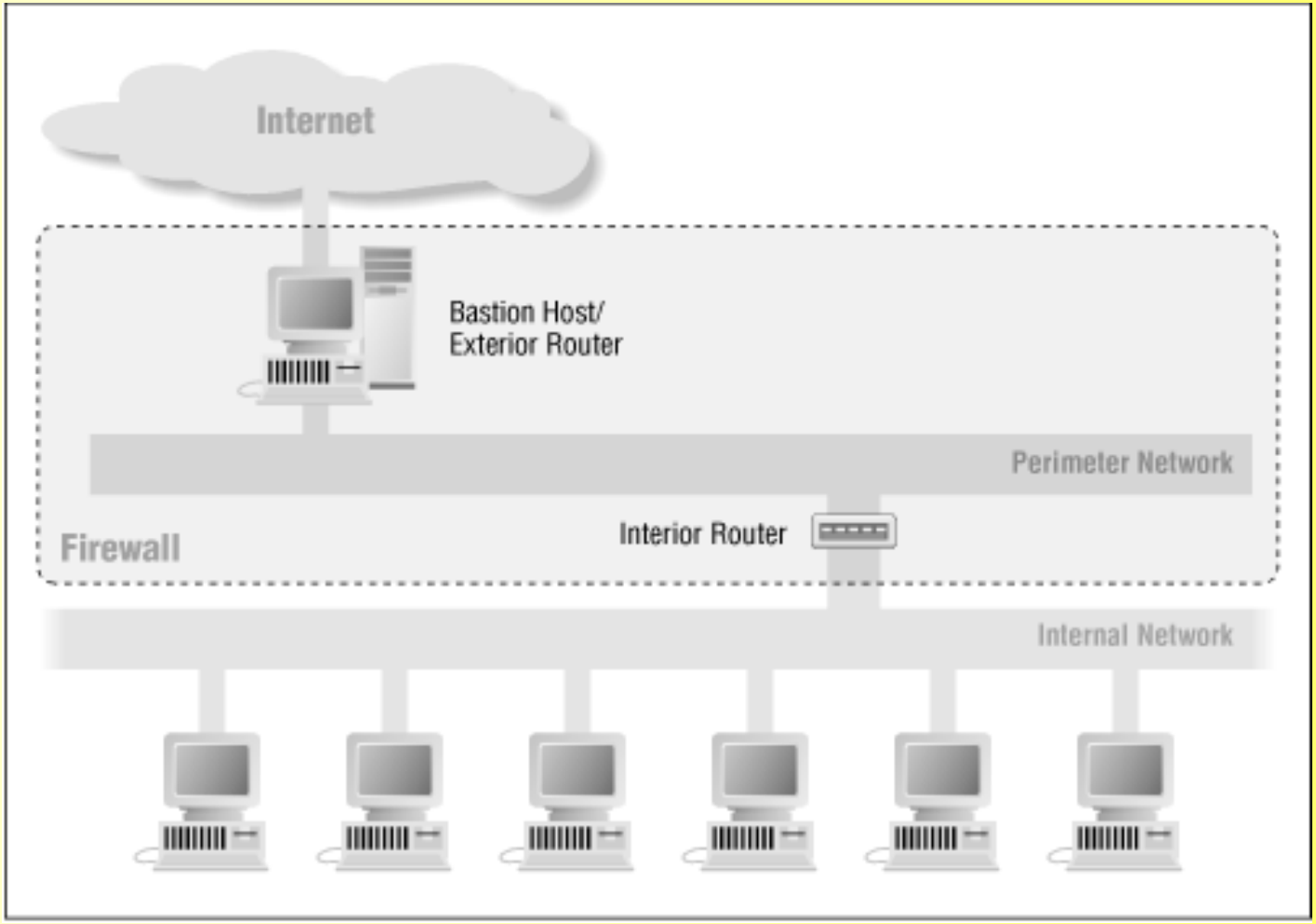
- You might also use multiple bastion hosts to keep the data sets of services from interfering with each other.

3.5 Architecture using a merged interior and exterior router



- This architecture makes the site vulnerable to the compromise of a single router.
- In general, routers are easier to protect than hosts, but they are not impenetrable.

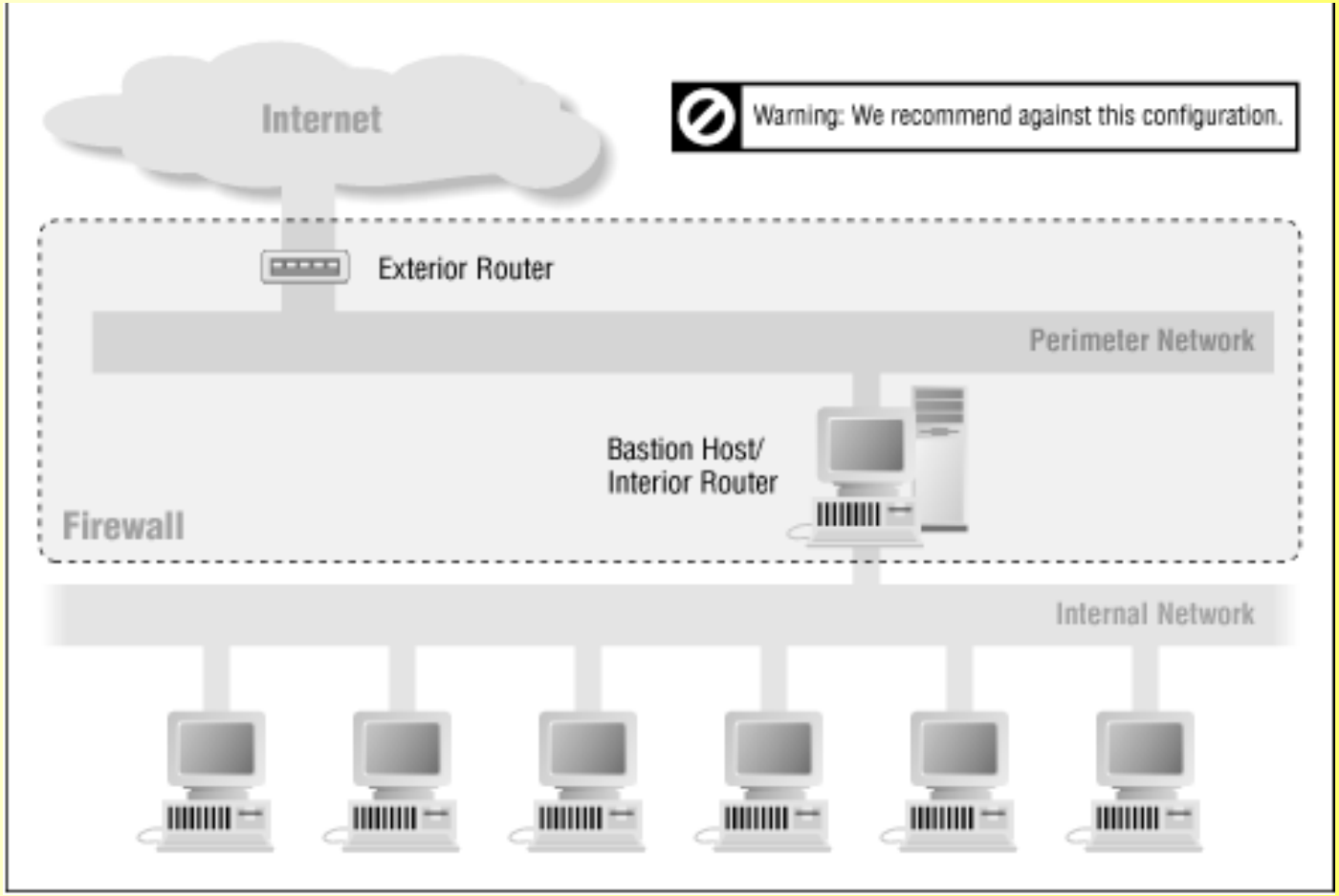
3.6 Architecture using a merged bastion host and exterior router



- It does not open significant new vulnerabilities.

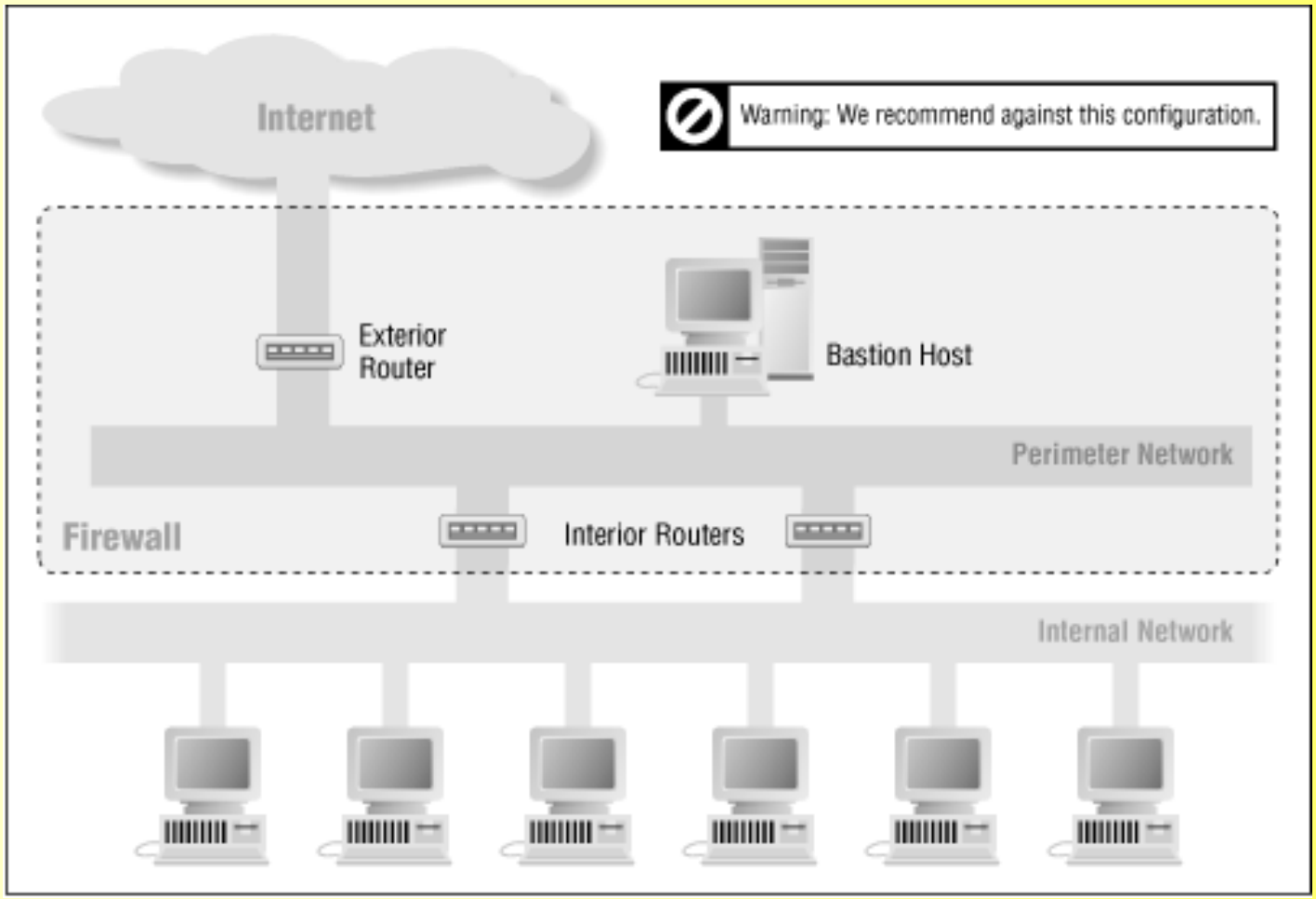
- It does expose the bastion host further.
  - In this architecture, the bastion host is more exposed to the Internet, protected only by whatever filtering (if any) its own interface package does, and you will need to take extra care to protect it.

3.7 It's Dangerous to Merge the Bastion Host and the Interior Router



- It's not a good idea to merge the bastion host and the interior router.
- In case of a separate bastion host and interior router， you have a screened subnet firewall architecture.
  - With this type of configuration, the perimeter net for the bastion host doesn't carry any strictly internal traffic
  - so this traffic is protected from snooping even if the bastion host is successfully penetrated;
  - to get at the internal network, the attacker still must get past the interior router.
- In the case of with a merged bastion host and interior router, you have a screened host firewall architecture.
  - With this type of configuration, if the bastion host is broken into, there's nothing left in the way of security between the bastion host and the internal network.

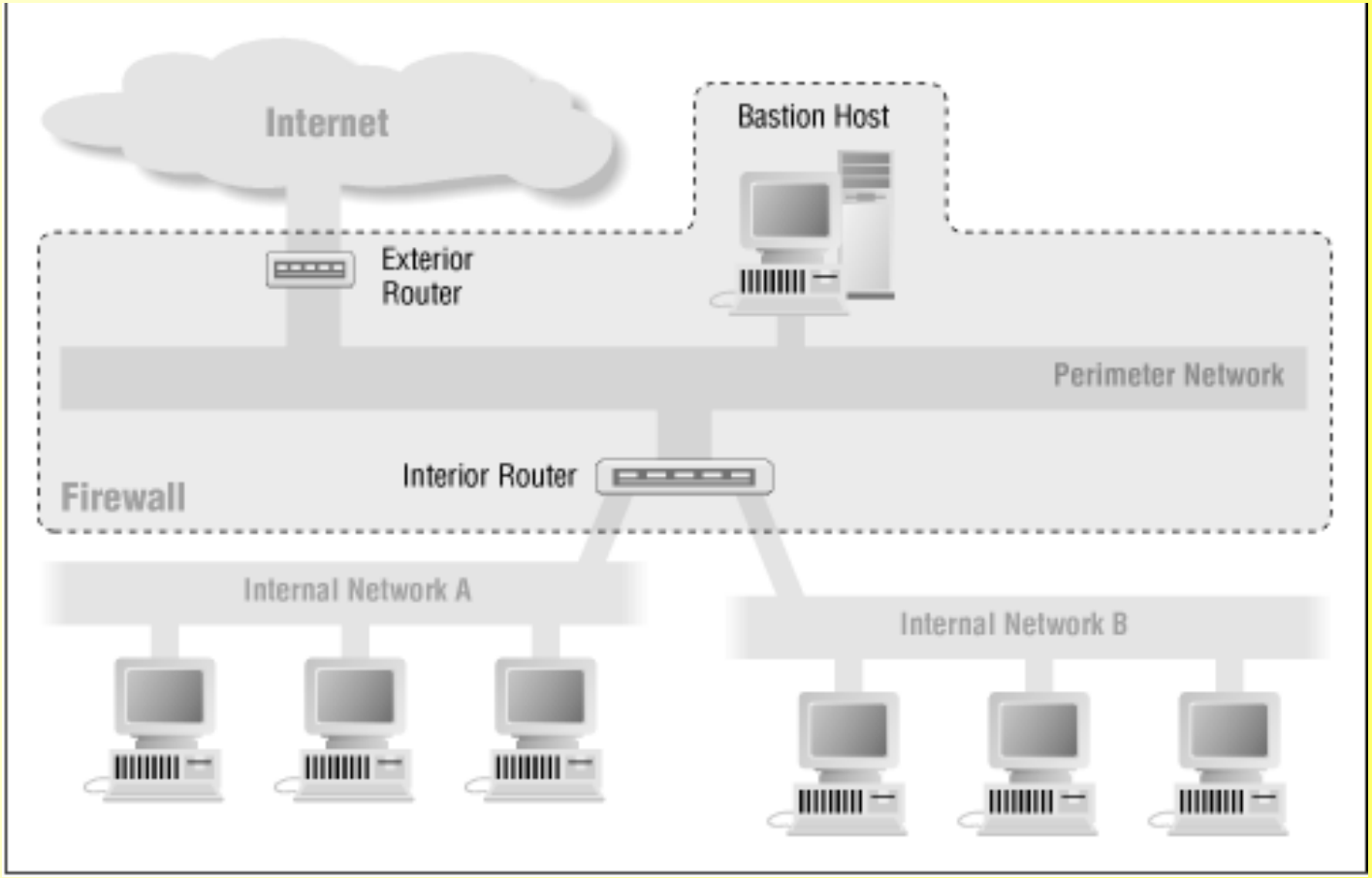
3.8 It's Dangerous to Use Multiple Interior Routers



- Using multiple interior routers to connect your perimeter net to multiple parts of your internal net can cause a lot of problems, and is generally a bad idea.
  - **you'll have sensitive, strictly internal traffic flowing across your perimeter net, where it can be snooped on if somebody has managed to break in to the bastion host.**
- It's also difficult to keep multiple interior routers correctly configured.
  - **The interior router is the one with the most important and the most complex set of packet filters**
  - **having two of them doubles your chances of getting the rule sets wrong.**

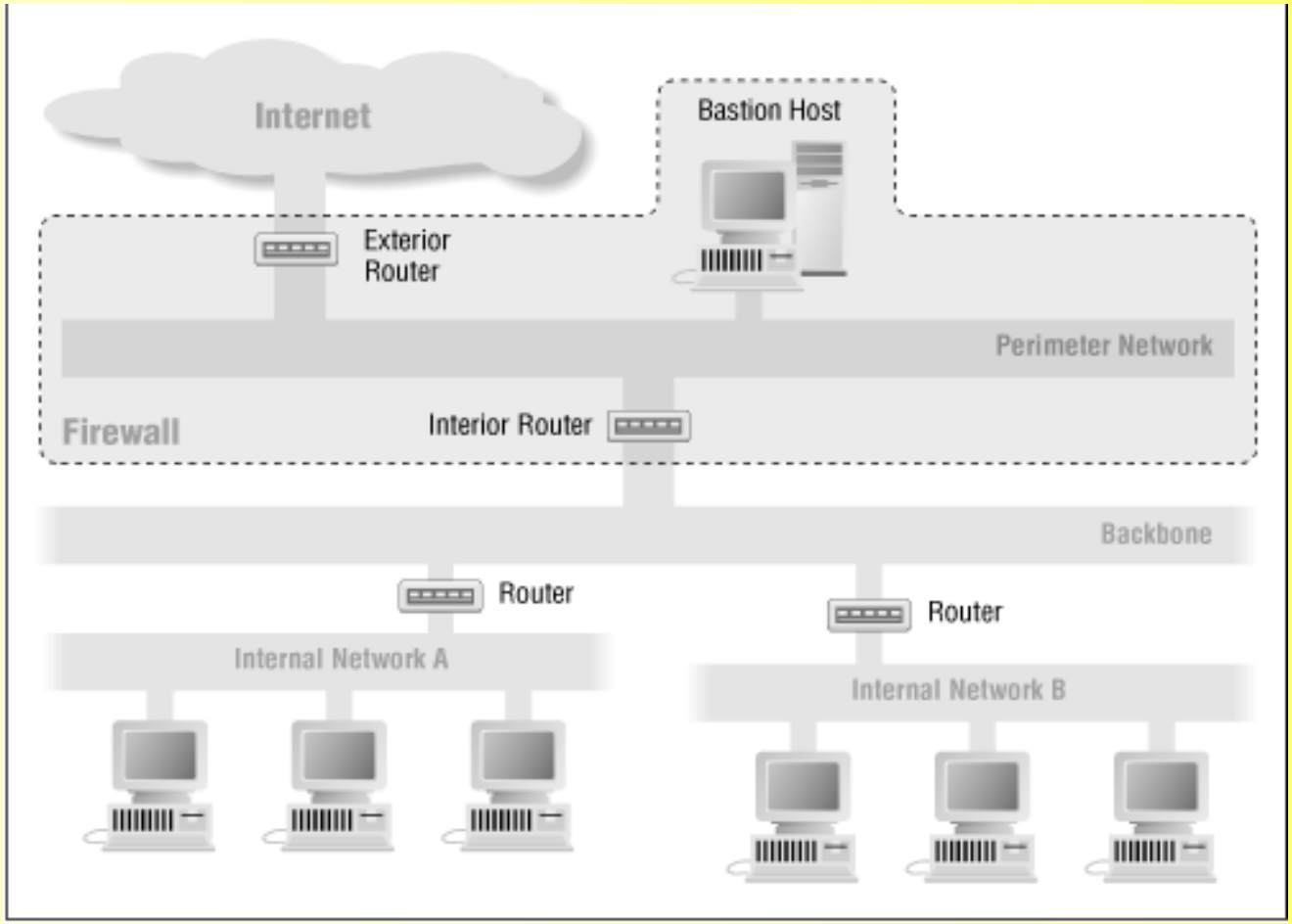
3.9 Multiple internal networks

- **separate interfaces in a single router**

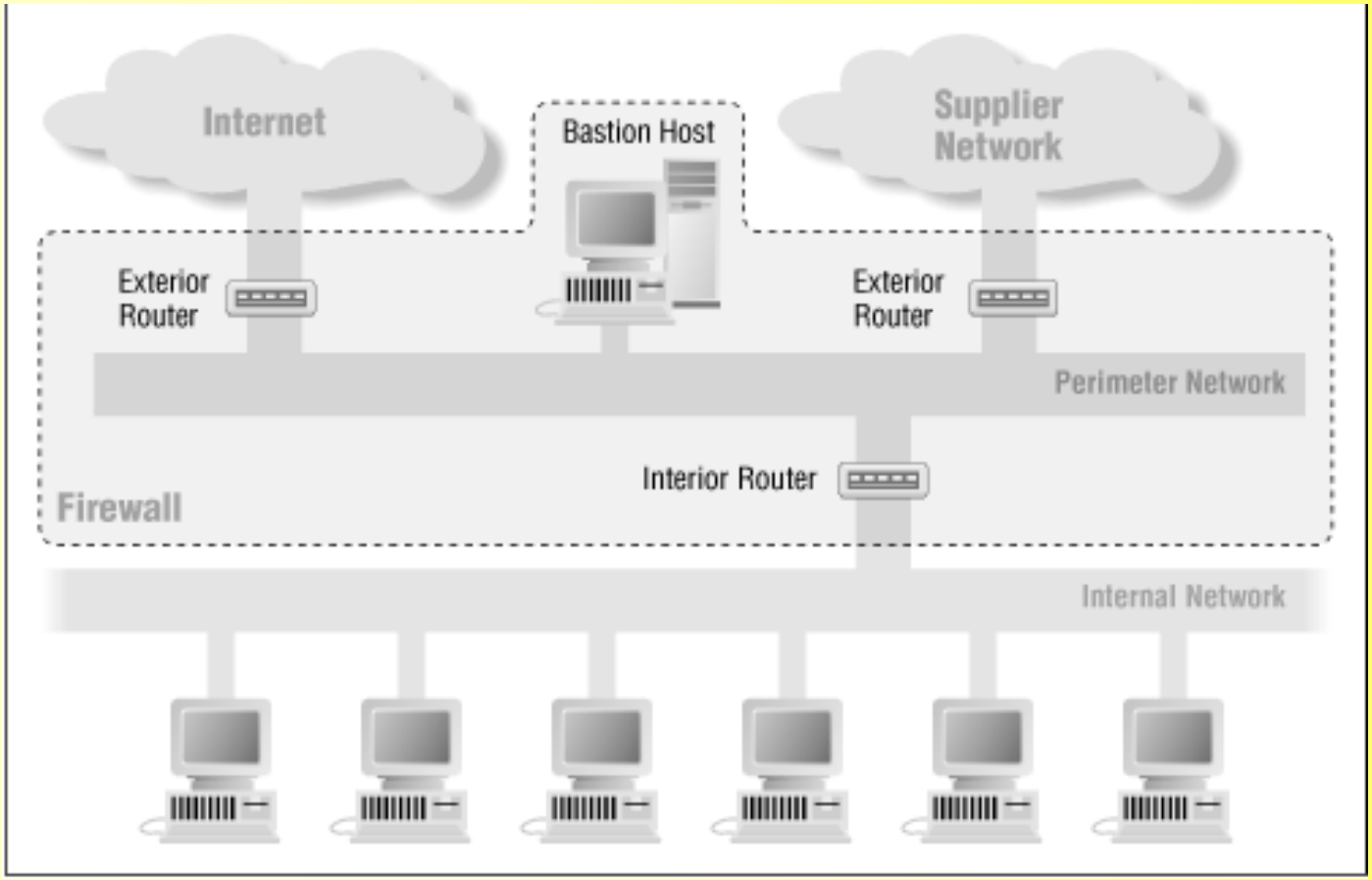


3.10 Multiple internal networks

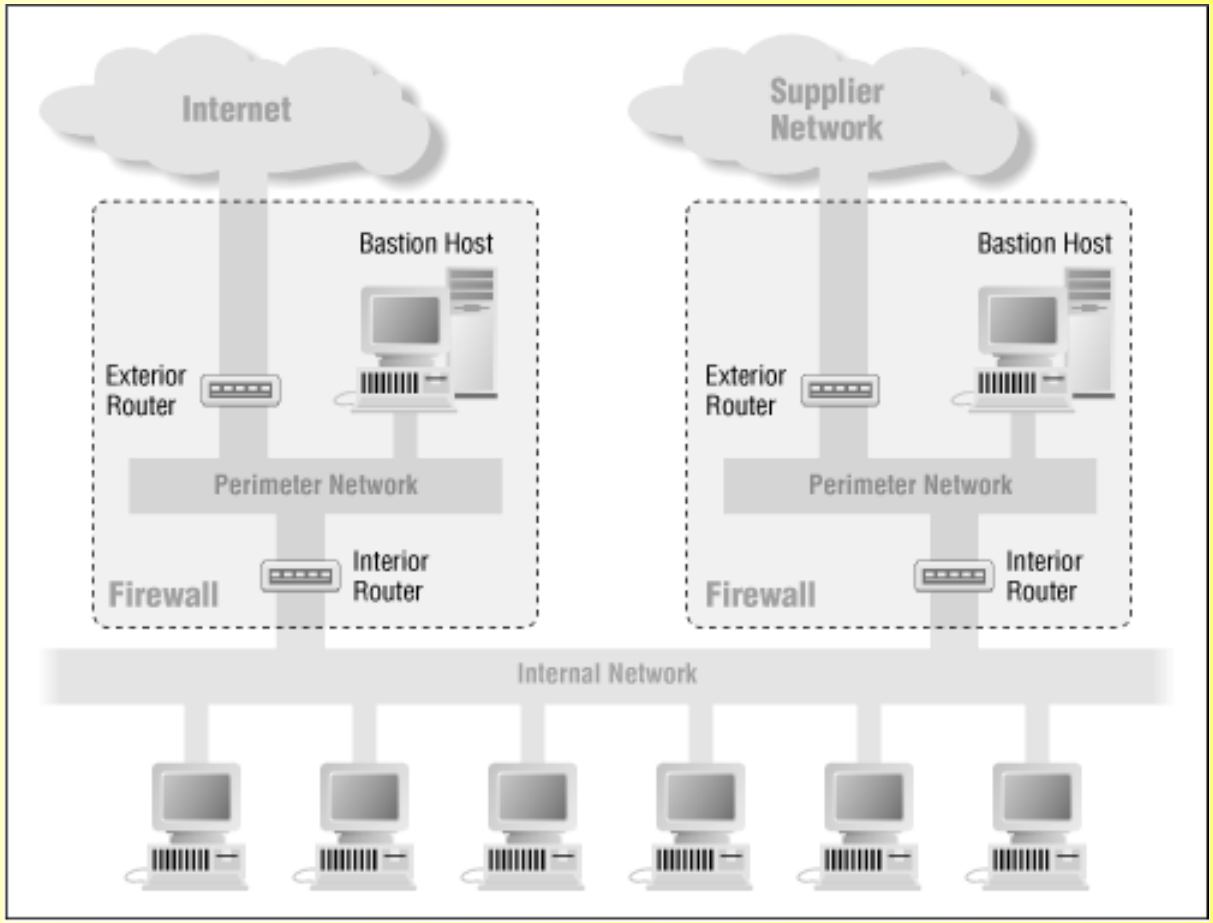
- **backbone architecture**



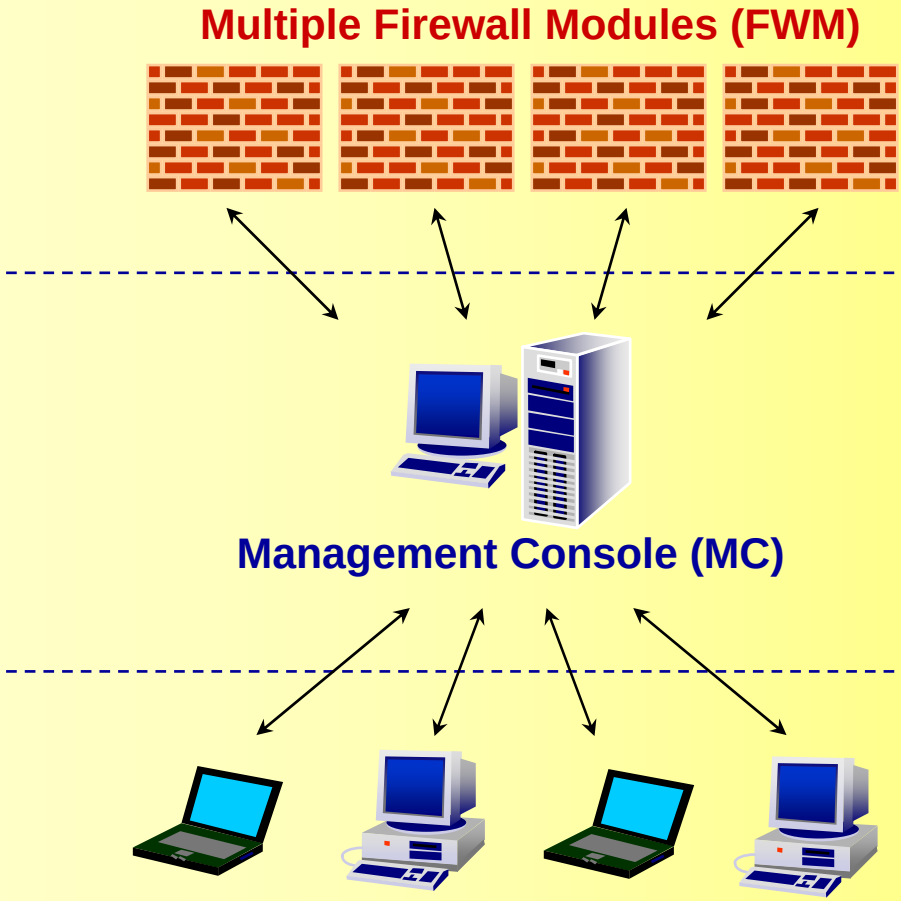
3.11 Architecture using multiple exterior routers



3.12 Architecture using multiple perimeter nets



4. Components of firewall



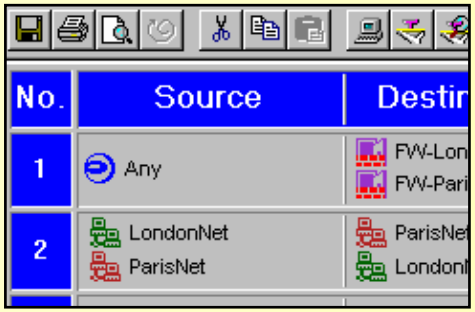
- Enforces security policy
- Reports status and log data to its management server

- Manages object DBs, rule bases, log files.
- Concurrent administrative access with varying rights

- Builds objects, rules.
- Views logs and FW status.

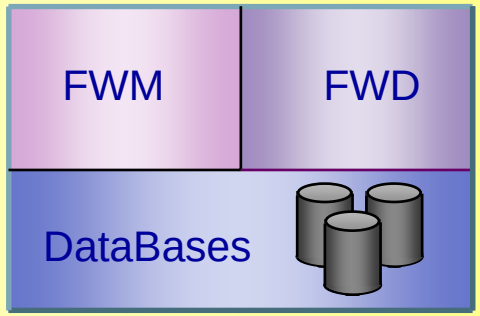
4.1 Product Components

GUI Client



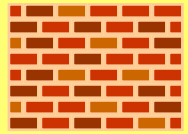
- Win 95
- Win NT
- X/Motif

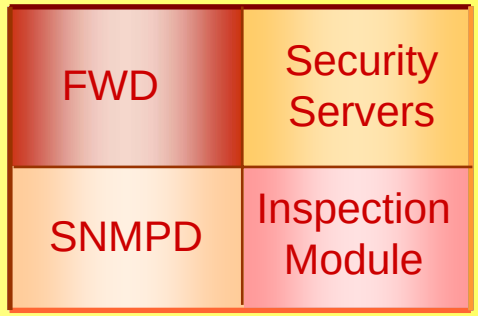
Management Console



- Solaris2
- SunOS4
- HP-UX
- AIX
- Windows NT

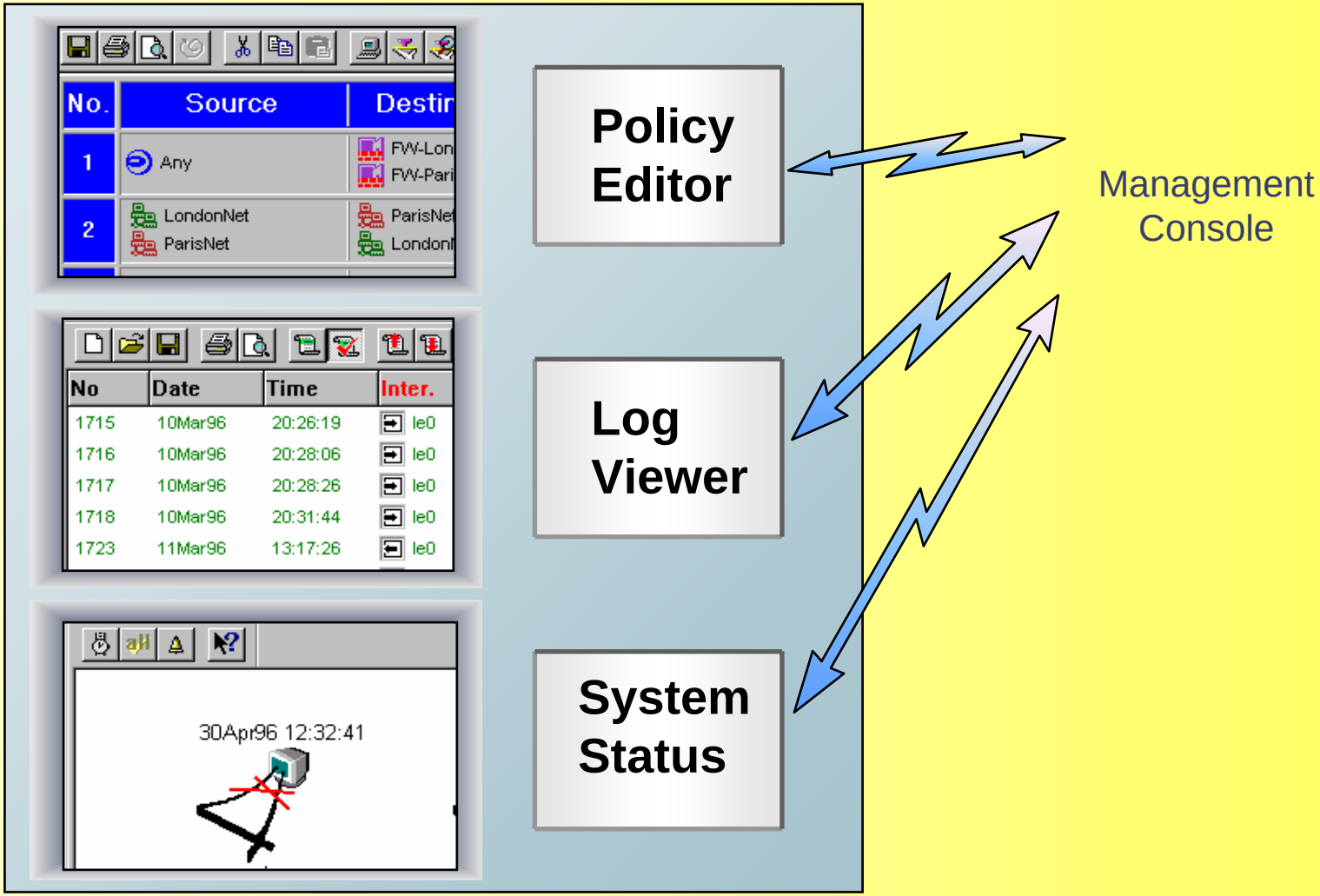
Firewall Module



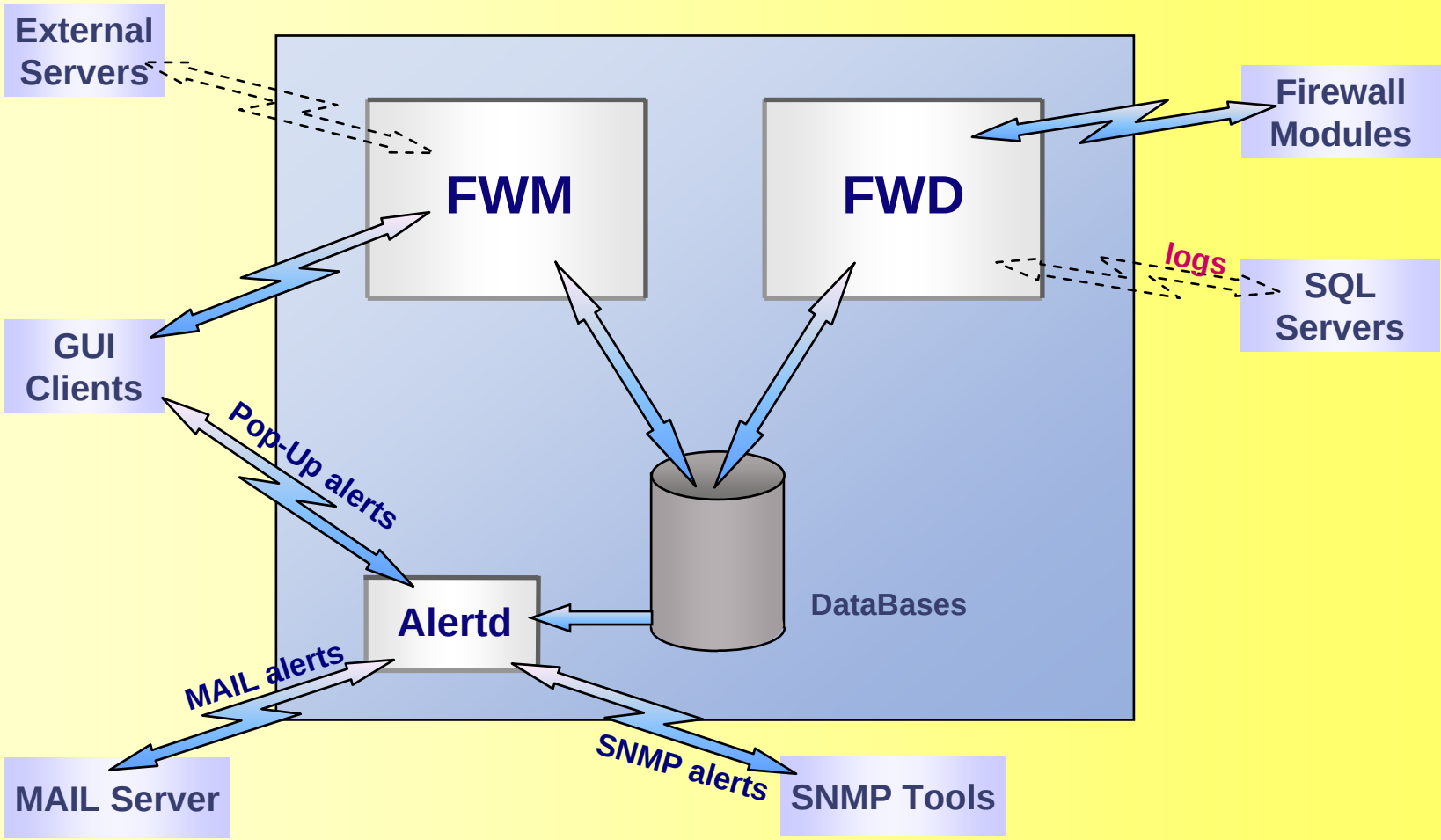


- Solaris2
- SunOS4
- HP-UX
- AIX
- Windows NT
- Bay Networks Routers
- Xylan Switches
- Ipsilon Switches

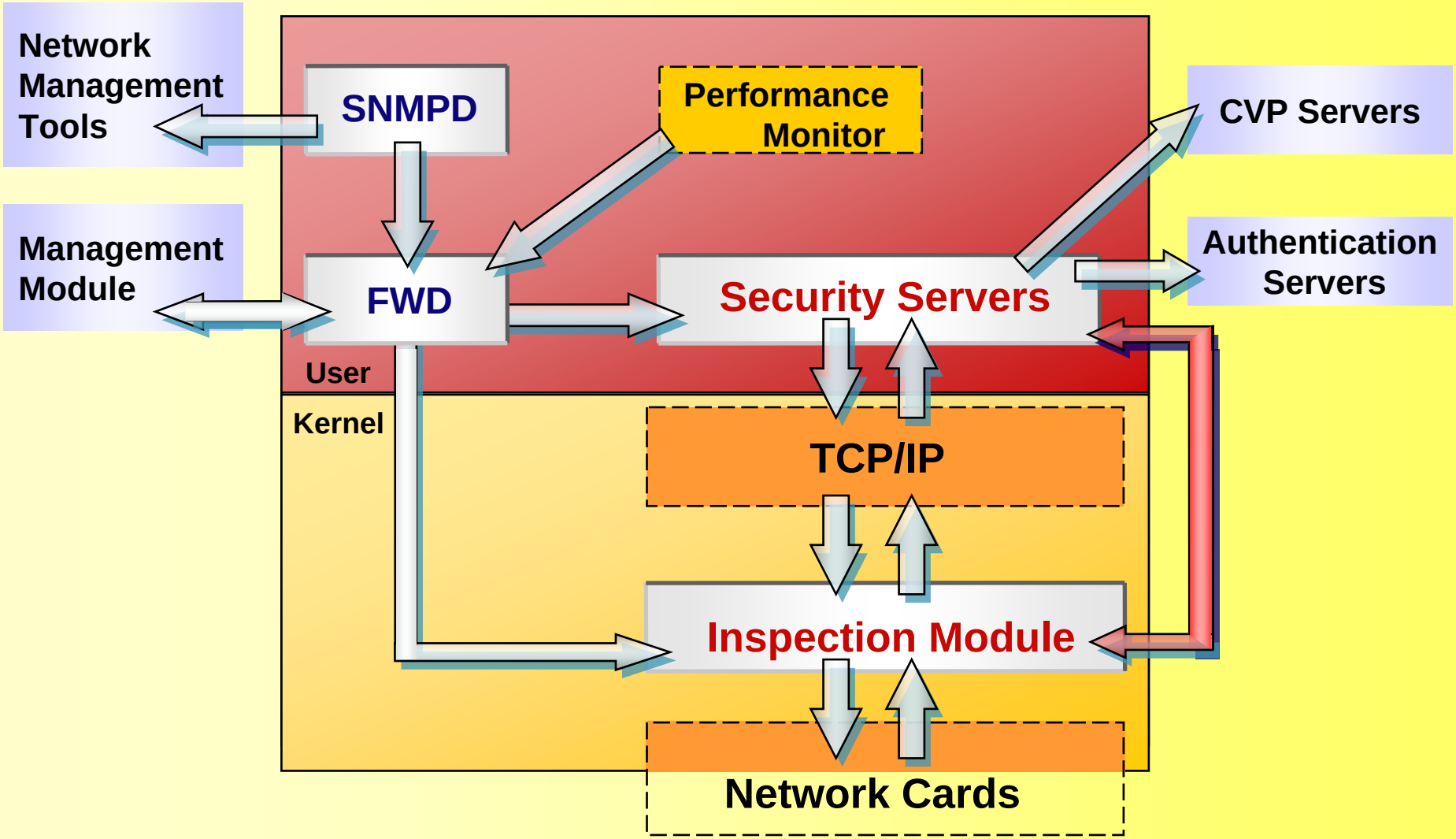
4.2 GUI Components



4.3 The management console components



4.4 The Firewall Module Components



4.5 Security Policy Flow