

# Network Security

Raj Jain

The Ohio State University

Columbus, OH 43210

Jain@CIS.Ohio-State.Edu

<http://www.cis.ohio-state.edu/~jain/>

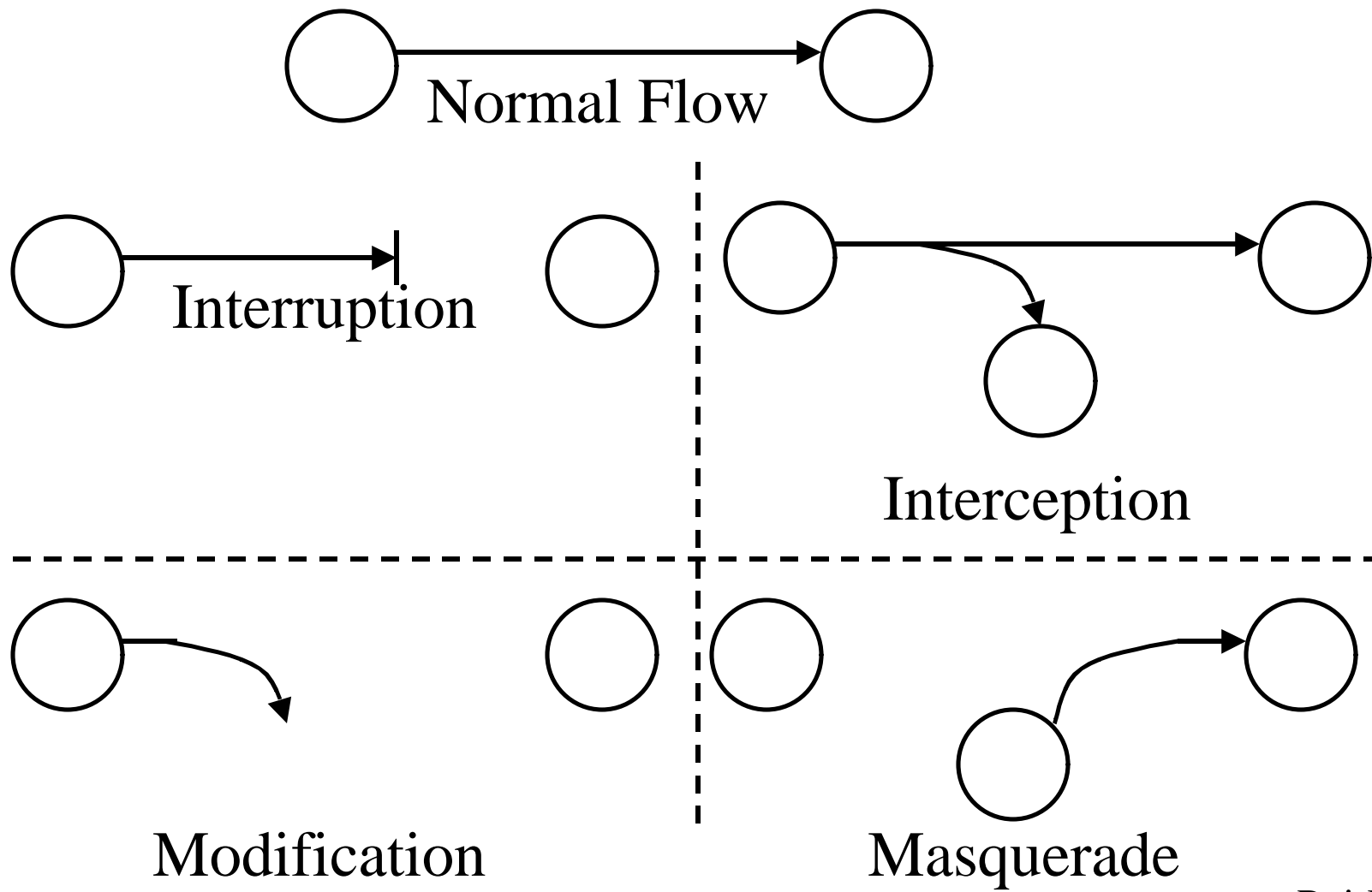


- q Security Aspects
- q Secret Key and Public Key Encryption
- q Firewalls: Packet Filter, Bastion Host, Perimeter Nets
- q Variations of firewalls
- q Proxy servers

# Security Aspects

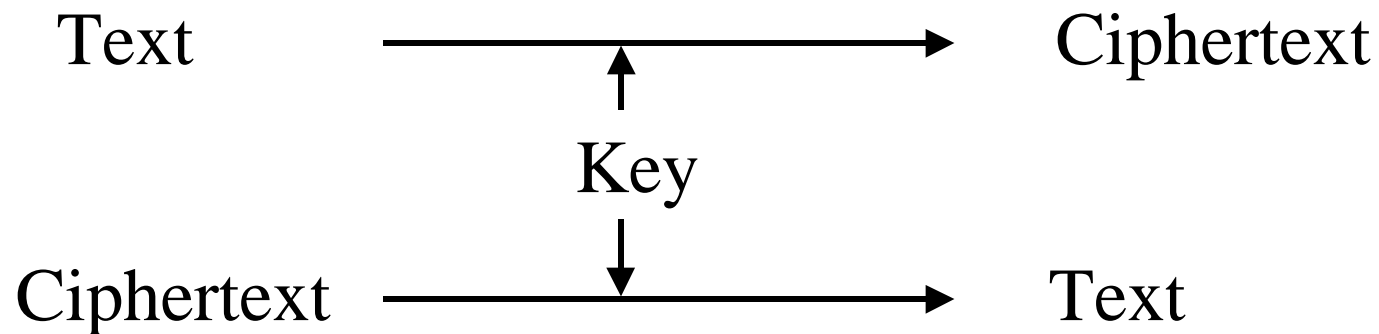
- q Data Integrity: Received = sent?
- q Data Availability: Legal users should be able to use. Ping continuously  $\Rightarrow$  No useful work gets done.
- q Data Confidentiality and Privacy: No snooping or wiretapping
- q Authentication: You are who you say you are. A student at Dartmouth posing as a professor canceled the exam.
- q Authorization = Access Control: Only authorized users get to the data

# Security Threats



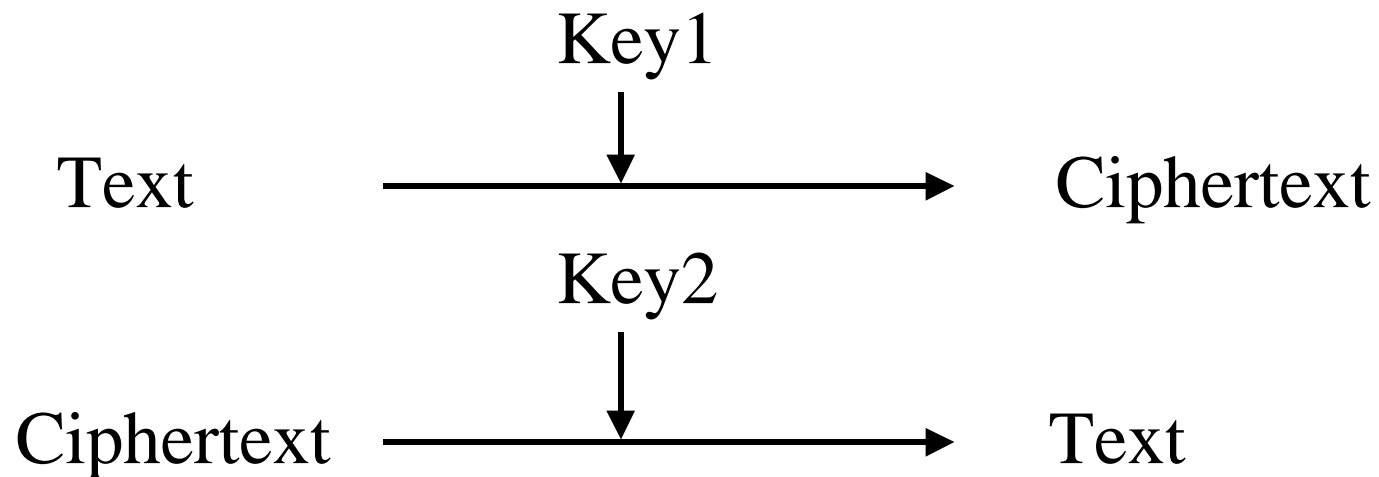
# Secret Key Encryption

- q  $\text{Encrypted\_Message} = \text{Encrypt}(\text{Key}, \text{Message})$
- q  $\text{Message} = \text{Decrypt}(\text{Key}, \text{Encrypted\_Message})$
- q Example: Encrypt = division
- q  $433 = 48 \text{ R } 1$  (using divisor of 9)



# Public Key Encryption

- q Invented in 1975 by Diffie and Hellman
- q  $\text{Encrypted\_Message} = \text{Encrypt}(\text{Key1}, \text{Message})$
- q  $\text{Message} = \text{Decrypt}(\text{Key2}, \text{Encrypted\_Message})$



# Public Key Encryption: Example

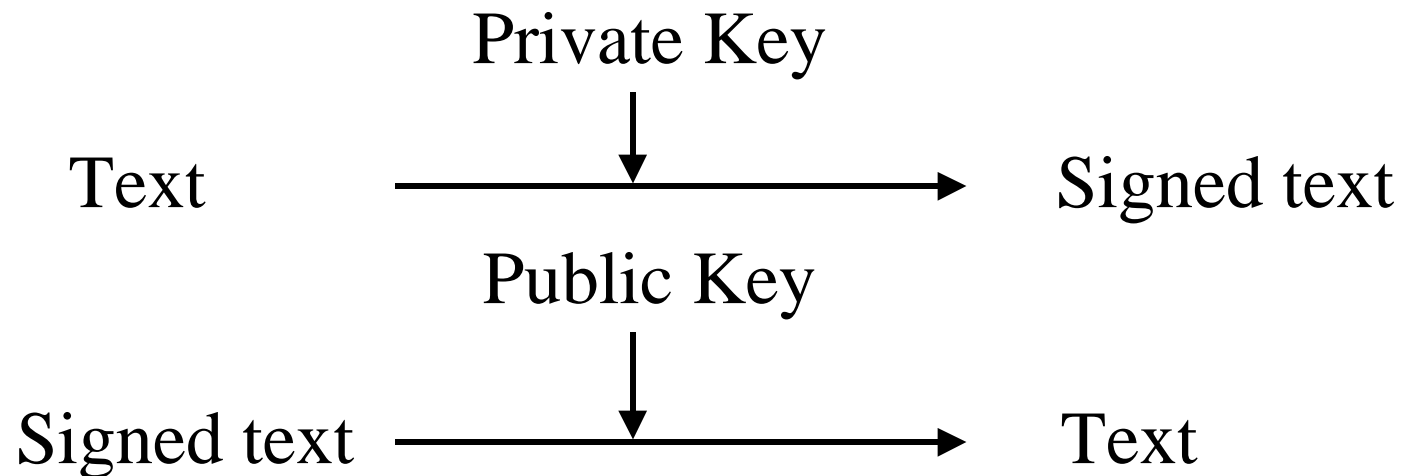
- q RSA: Encrypted\_Message =  $m^3 \bmod 187$
- q Message = Encrypted\_Message<sup>107</sup> mod 187
- q Key1 =  $\langle 3, 187 \rangle$ , Key2 =  $\langle 107, 187 \rangle$
- q Message = 5
- q Encrypted Message =  $5^3 = 125$
- q Message =  $125^{107} \bmod 187$   
=  $125^{(64+32+8+2+1)} \bmod 187$   
=  $[(125^{64} \bmod 187)(125^{32} \bmod 187) \dots$   
 $(125^2 \bmod 187)(125)] \bmod 187 = 5$
- q  $125^4 \bmod 187 = (125^2 \bmod 187)^2 \bmod 187$

## Public Key (Cont)

- q One key is private and the other is public
- q  $\text{Message} = \text{Decrypt}(\text{Public\_Key}, \text{Encrypt}(\text{Private\_Key}, \text{Message}))$
- q  $\text{Message} = \text{Decrypt}(\text{Private\_Key}, \text{Encrypt}(\text{Public\_Key}, \text{Message}))$

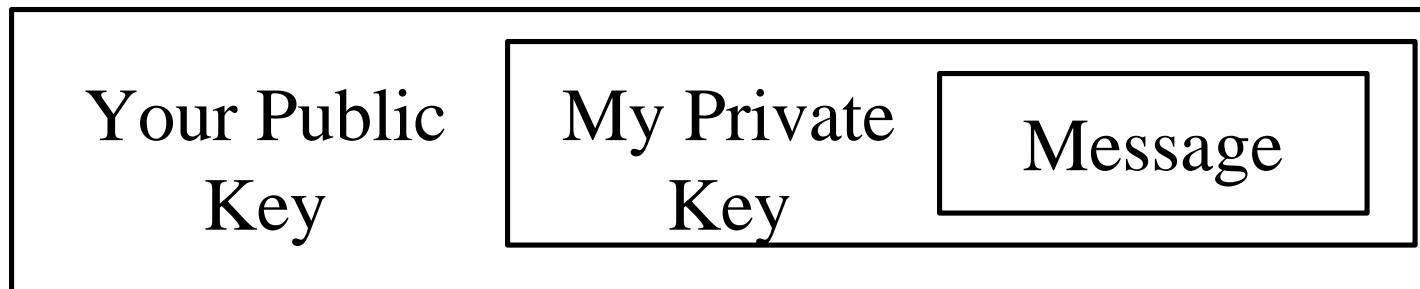
# Digital Signature

- q Encrypted\_Message  
= Encrypt(Private\_Key, Message)
- q Message = Decrypt(Public\_Key, Encrypted\_Message)  
⇒ Authentic

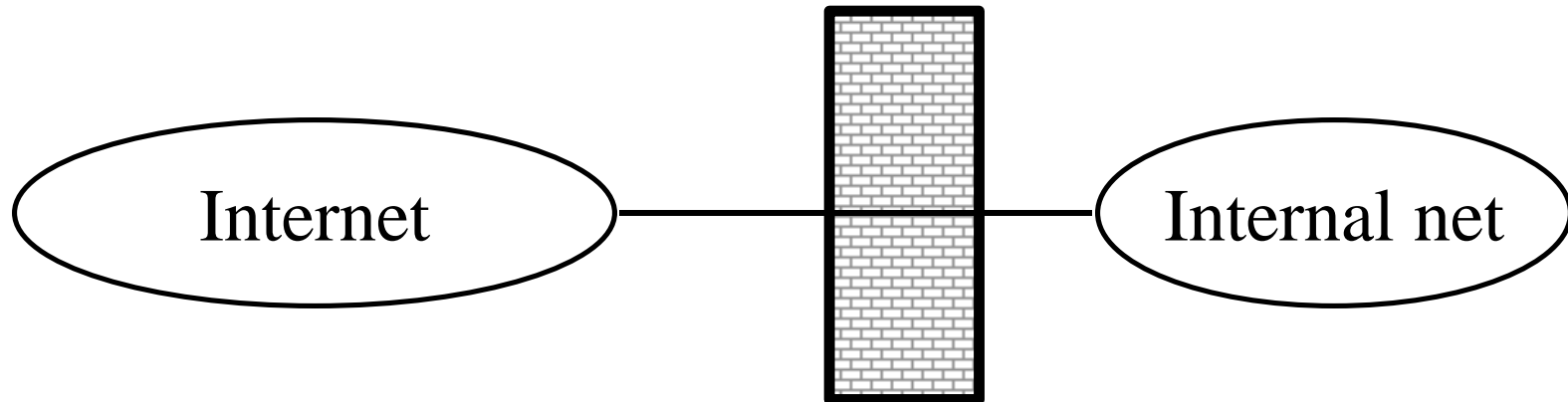


# Confidentiality

- q User 1 to User 2:
- q  $\text{Encrypted\_Message} = \text{Encrypt}(\text{Public\_Key2}, \text{Encrypt}(\text{Private\_Key1}, \text{Message}))$
- q  $\text{Message} = \text{Decrypt}(\text{Public\_Key1}, \text{Decrypt}(\text{Private\_Key2}, \text{Encrypted\_Message}))$   
 $\Rightarrow$  Authentic and Private



# Simple Firewall: Packet Filter

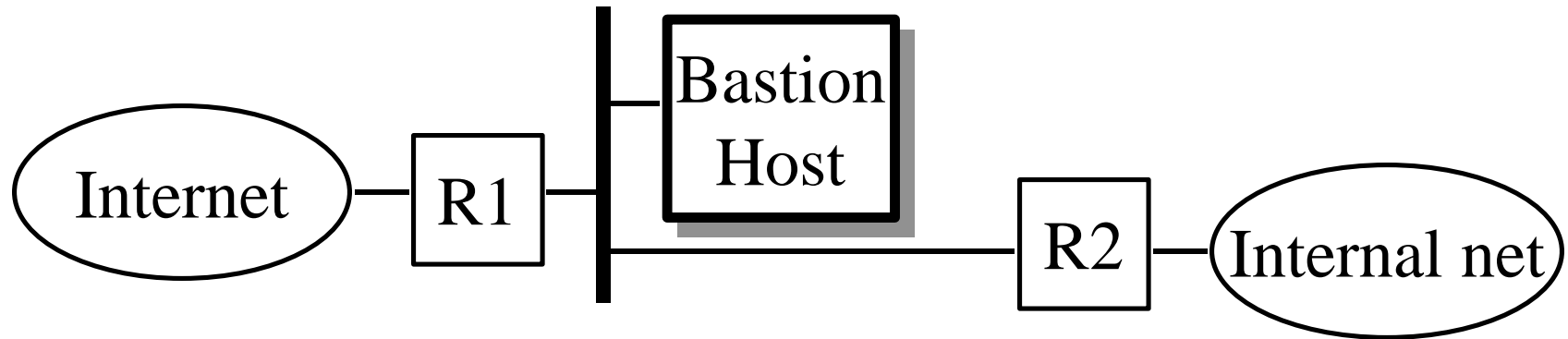


- q Example: Only email gets in/out ftp to/from nodes x, y, z, etc.
- q Problem: Filter is accessible to outside world

## Filter Table: Example

Interface	Source	Dest	Prot.	Src Port	Dest Port
2	*	*	TCP	*	21
2	*	*	TCP	*	23
1	128.5.*.*	*	TCP	*	25
2	*	*	UDP	*	43
2	*	*	UDP	*	69
2	*	*	TCP	*	79

## Bastion Host

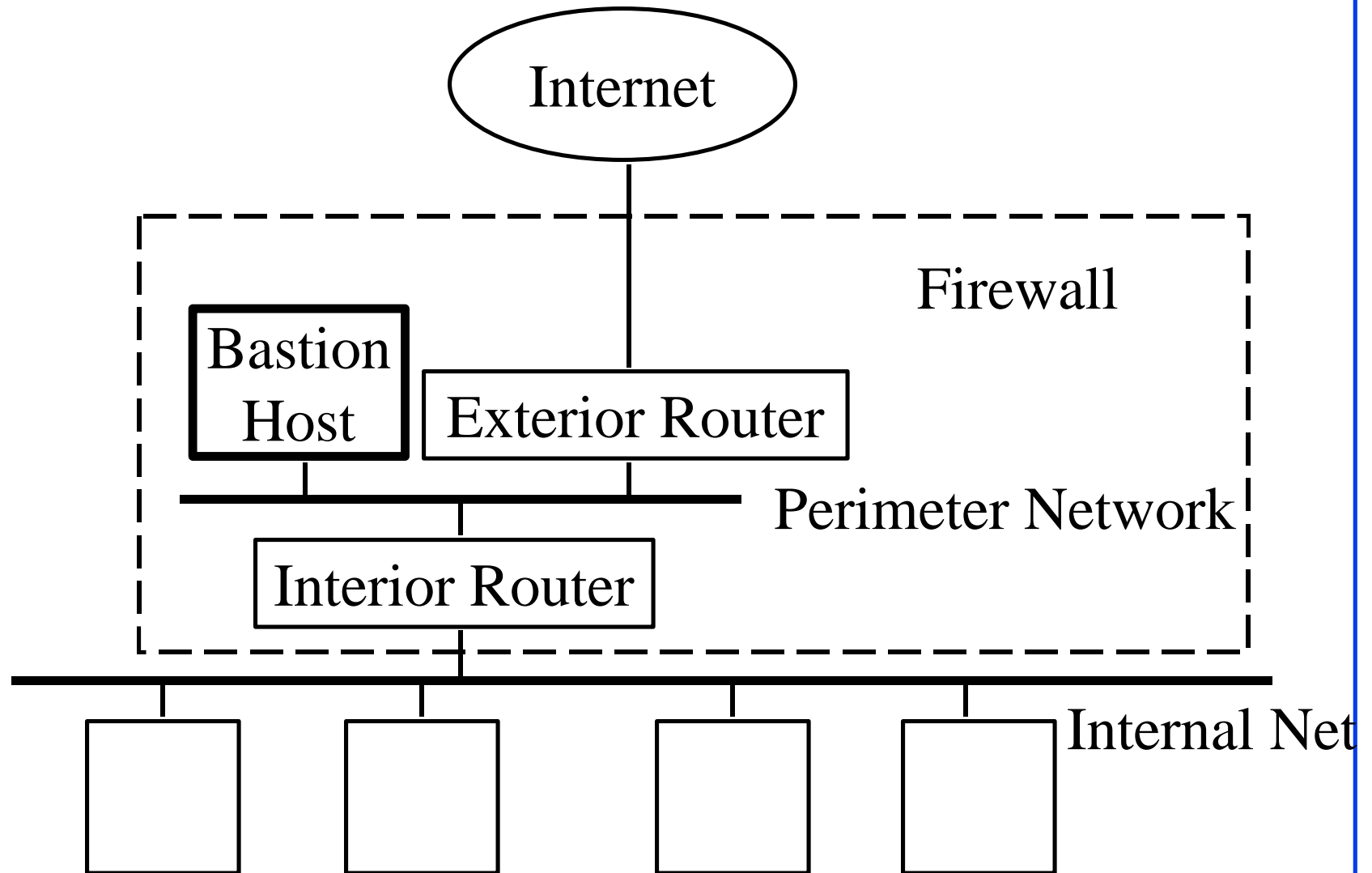


- q Bastions overlook critical areas of defense, usually having stronger walls
- q Inside users need a mechanism to get outside services
- q Inside users log on the Bastion Host and use outside services.
- q Later they pull the results inside.

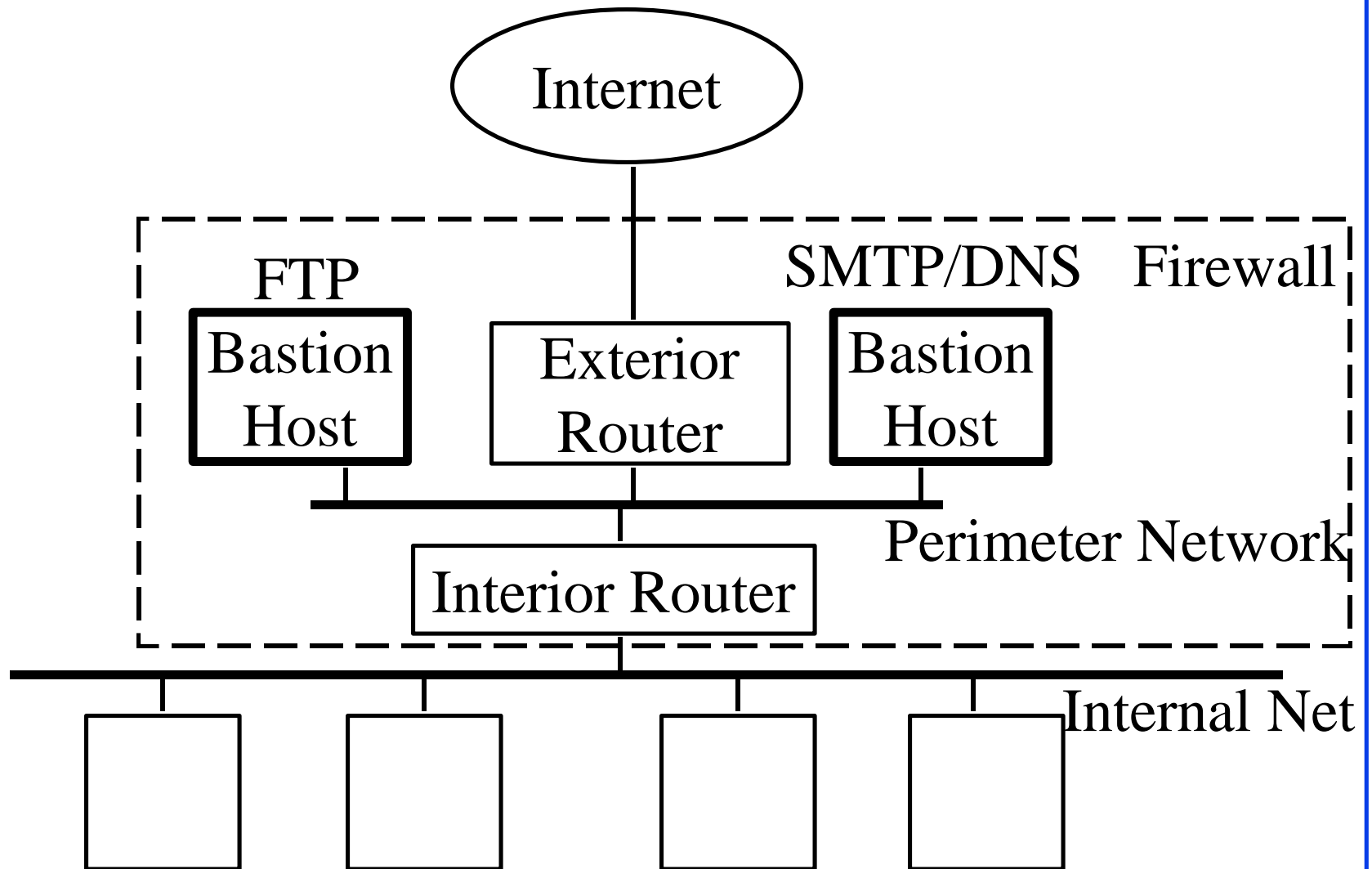
## **Bastion Host (Cont)**

- q Perimeter Network: Outside snoopers cannot see internal traffic even if they break in the firewall (Router 2)
- q Also known as "Stub network"

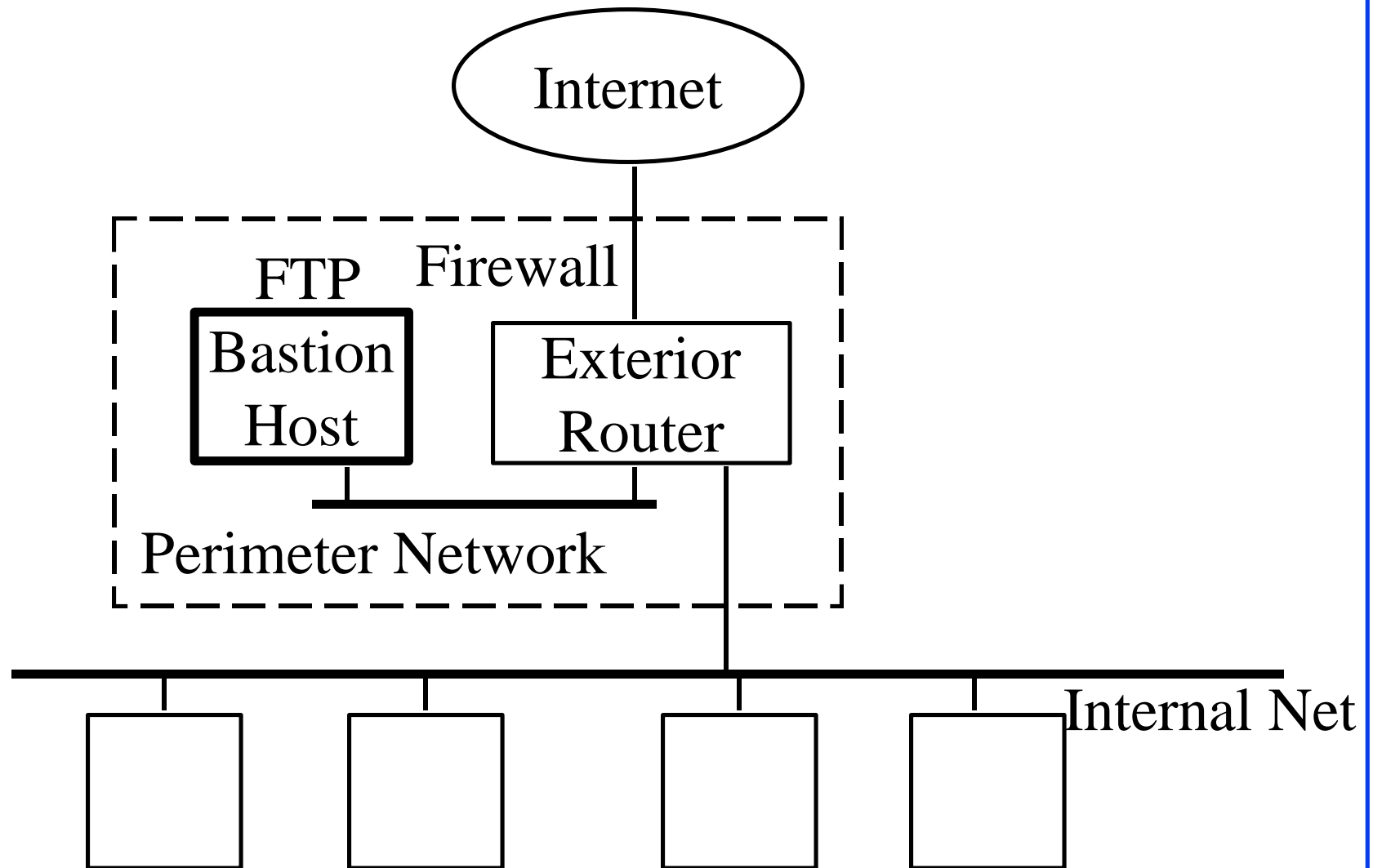
# Screened Subnet Architecture



# Multiple Bastion Hosts

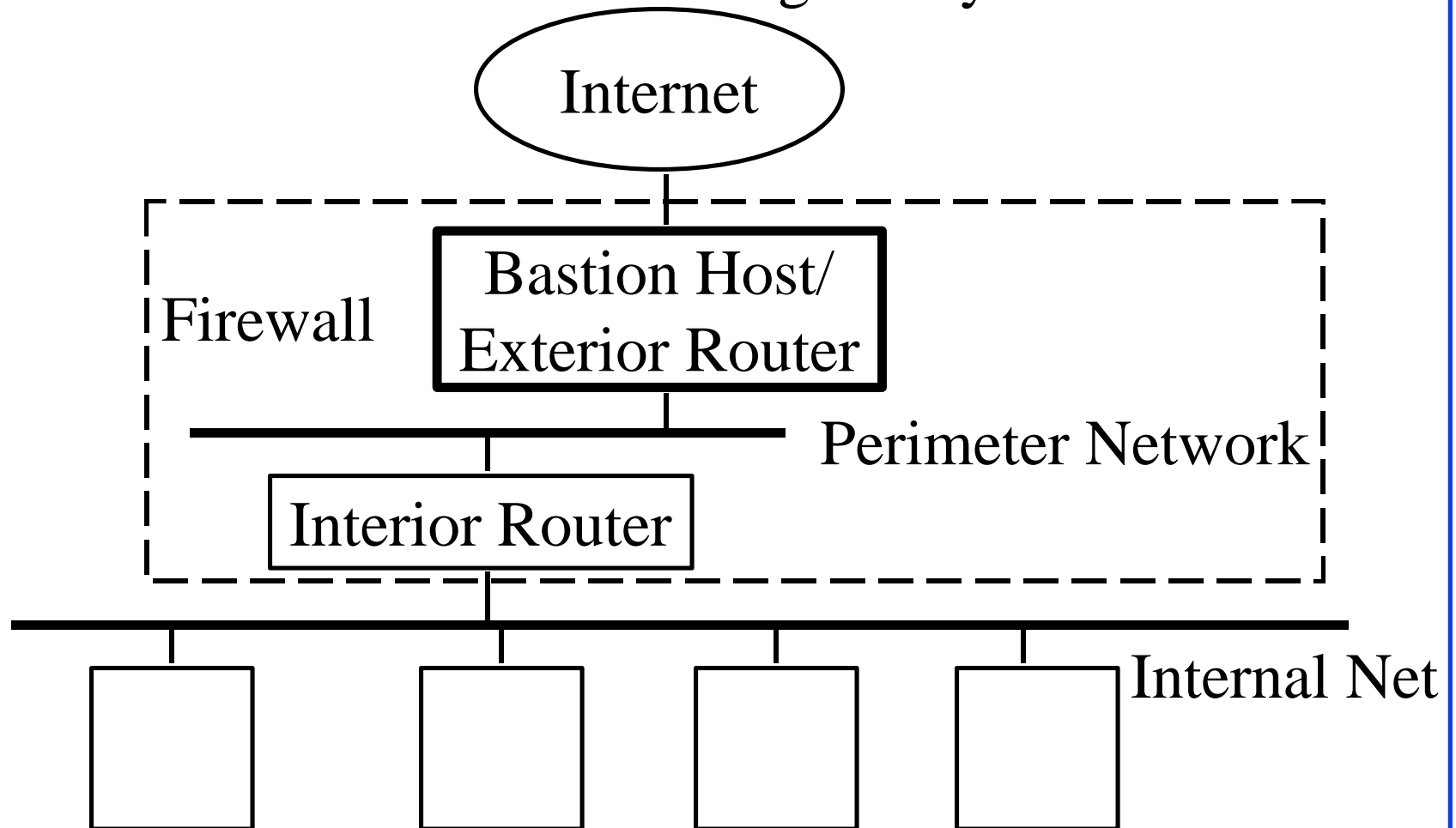


# Merged Interior and Exterior Routers

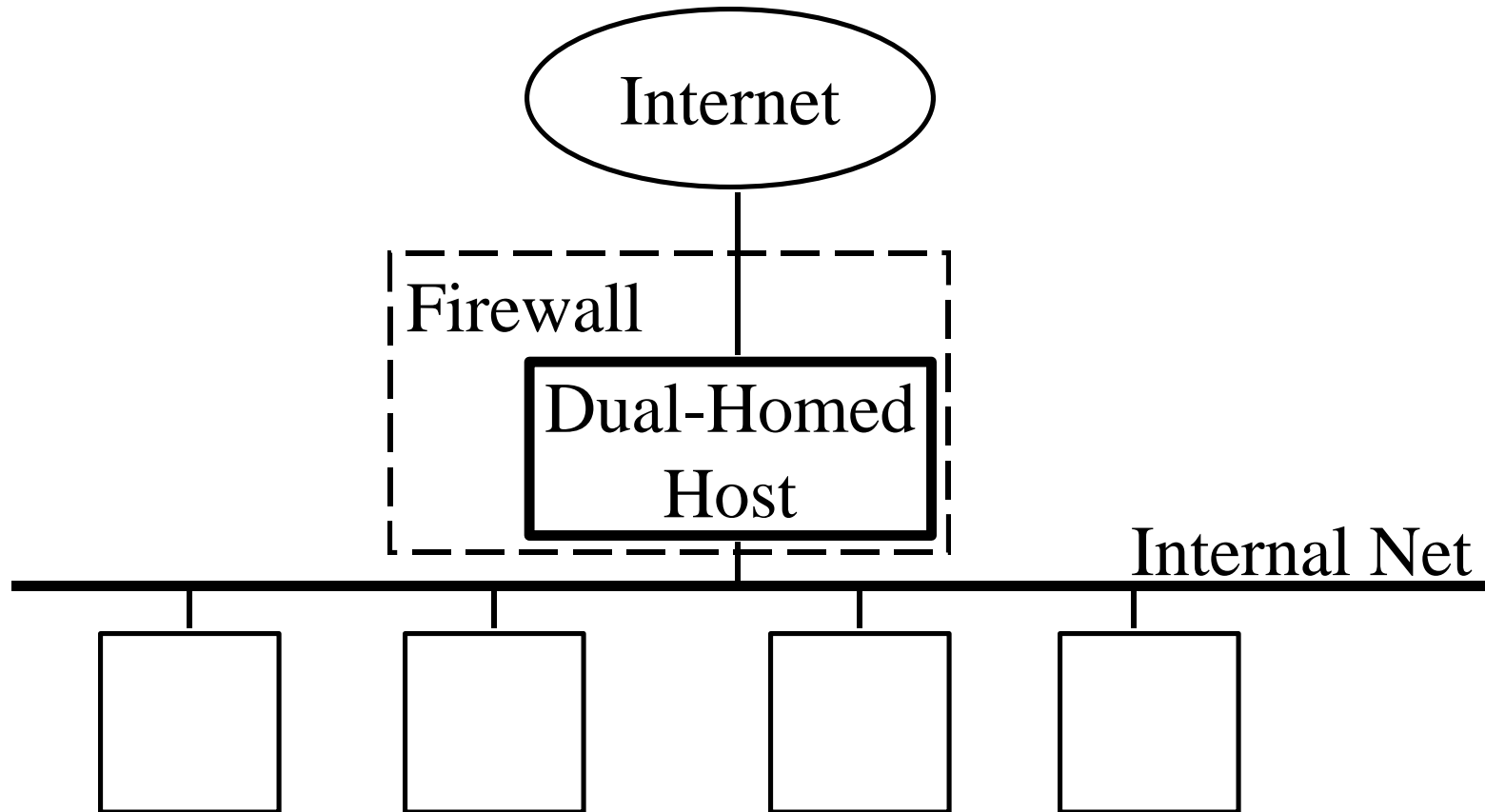


# Merged Bastion Host and Exterior Router

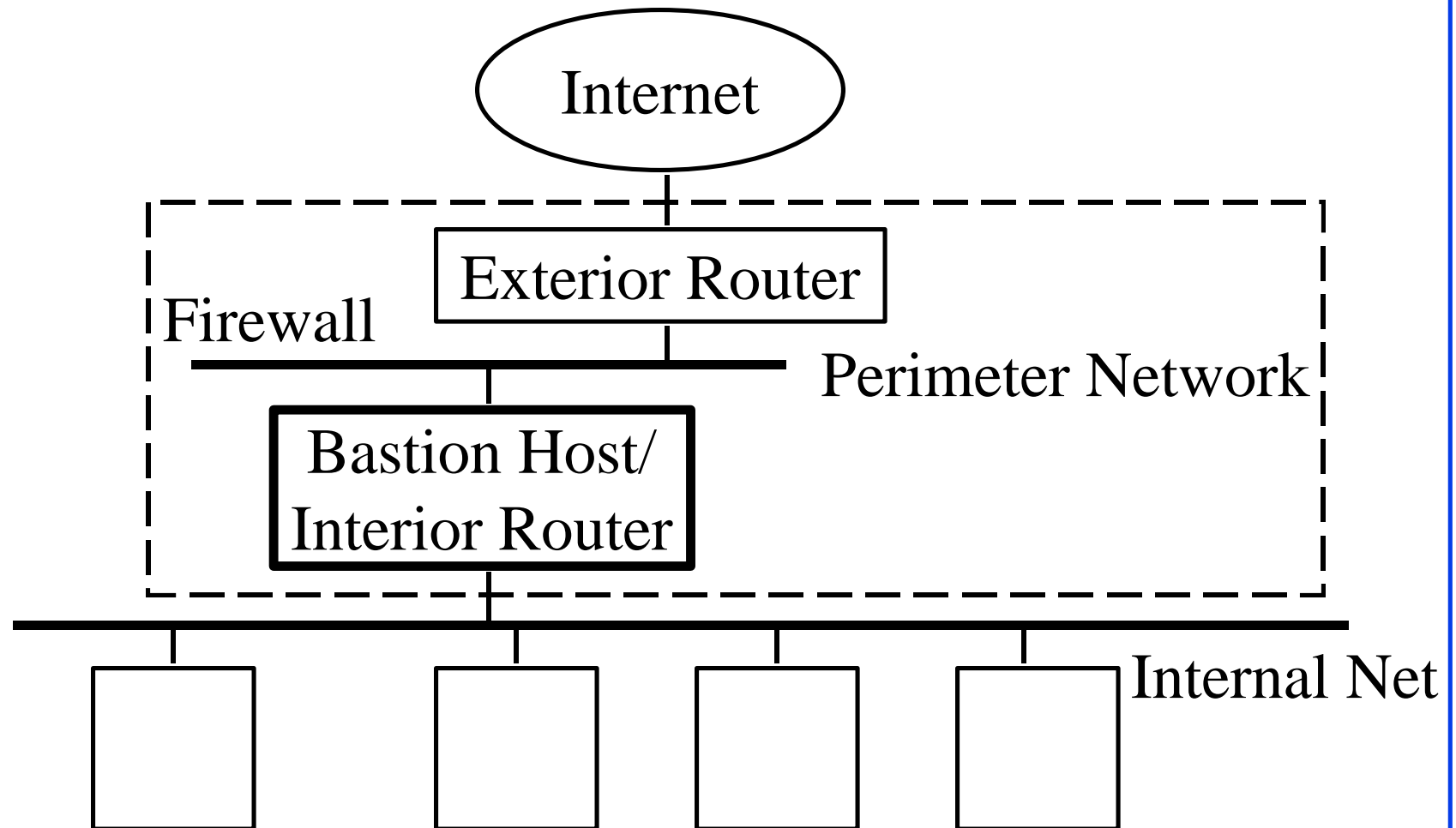
q Also known as a dual-homed gateway



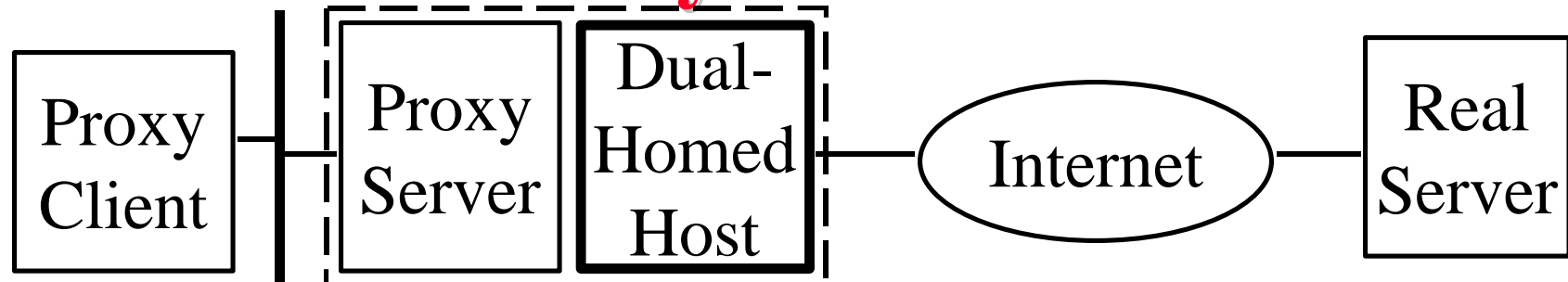
# Dual-Homed Host Architecture



# Merged Bastion Host and Interior Router (Not Recommended)



## Proxy Servers



- q Specialized server programs on bastion host
- q Take user's request and forward them to real servers
- q Take server's responses and forward them to users
- q Enforce site security policy  $\Rightarrow$  May refuse certain requests.
- q Also known as application-level gateways
- q With special "Proxy client" programs, proxy servers are almost transparent

# What Firewalls Can't Do

- q Can't protect against malicious insiders
- q Can't protect against connections that do not go through it, e.g., dial up
- q Can't protect completely new threats
- q Can't protect against viruses

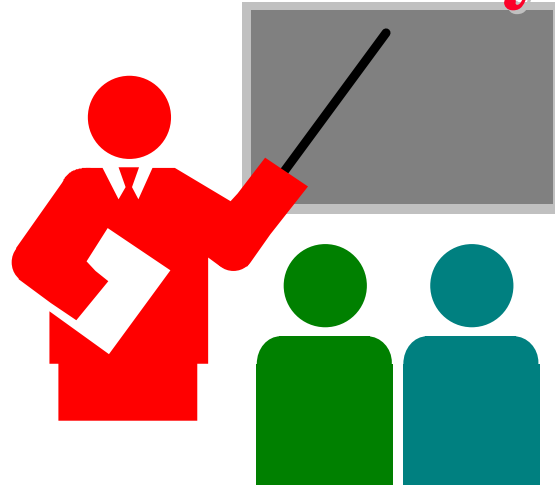
# Security Mechanisms on The Internet

- q Kerberos
- q Privacy Enhanced Mail (PEM)
- q Pretty Good Privacy (PGP)
- q MD5

# Pretty Good Privacy (PGP)

- q A popular version of the RSA algorithm.
- q PGP generates a random “session key” to encrypt each message using IDEA algorithm
- q Session key is encrypted using public key of the recipient
- q The encrypted message and the session key are passed on to the application (e.g., mail)
- q A file called key ring (pubring.pgp) contains public keys of all correspondents
- q Another file called secret ring (secring.pgp) contains secret keys of the sender. A pass phrase is required to decrypt the secret keys.

# Summary



- q Integrity, Availability, Authentication, Confidentiality
- q Private Key and Public Key encryption
- q Packet filter, Bastion node, perimeter network, internal and external routers