Network Security

Raj Jain

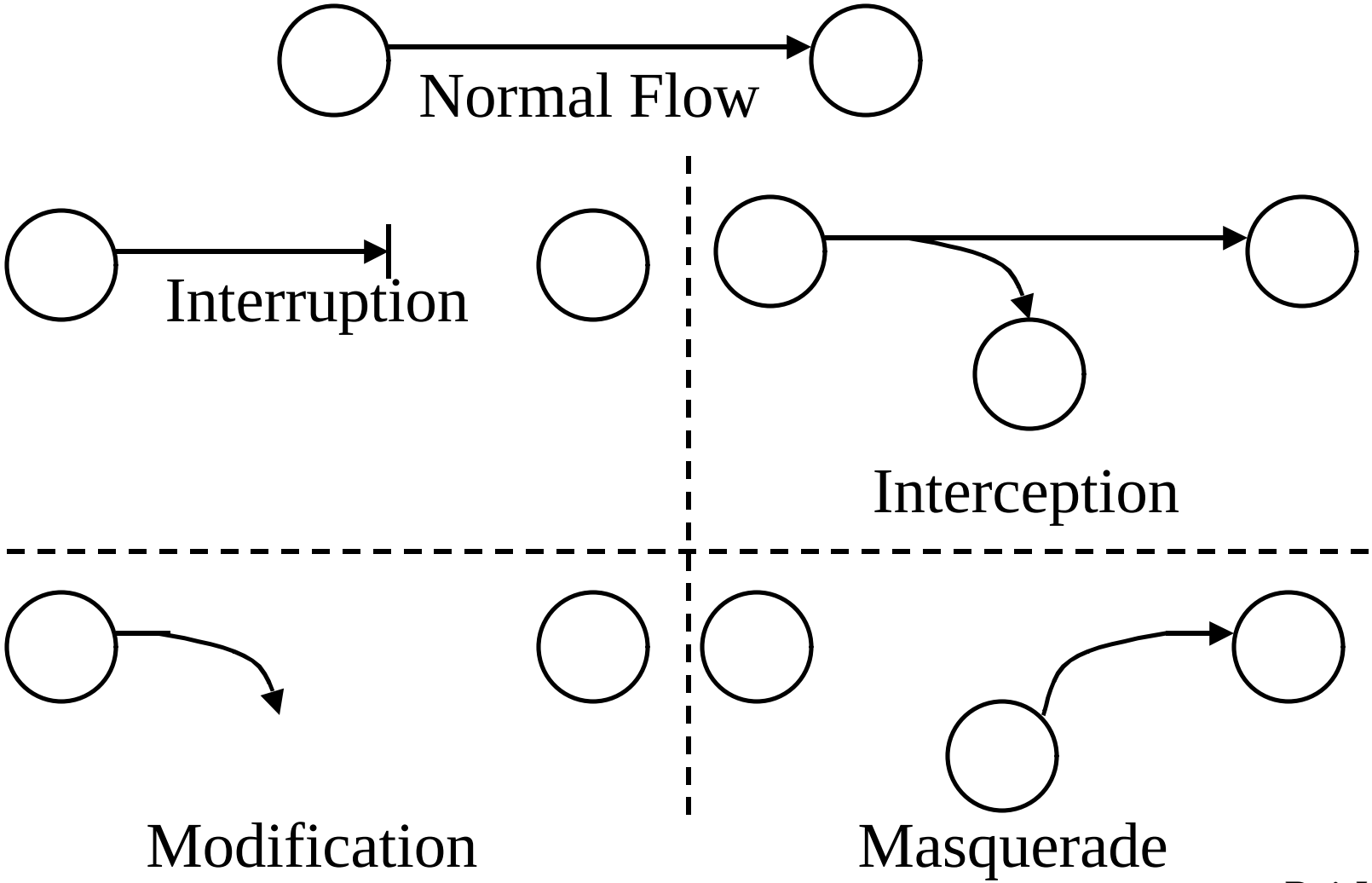
Raj Jain is now at
Washington University in Saint Louis
Jain@cse.wustl.edu
http://www.cse.wustl.edu/~jain/

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

Security Aspects

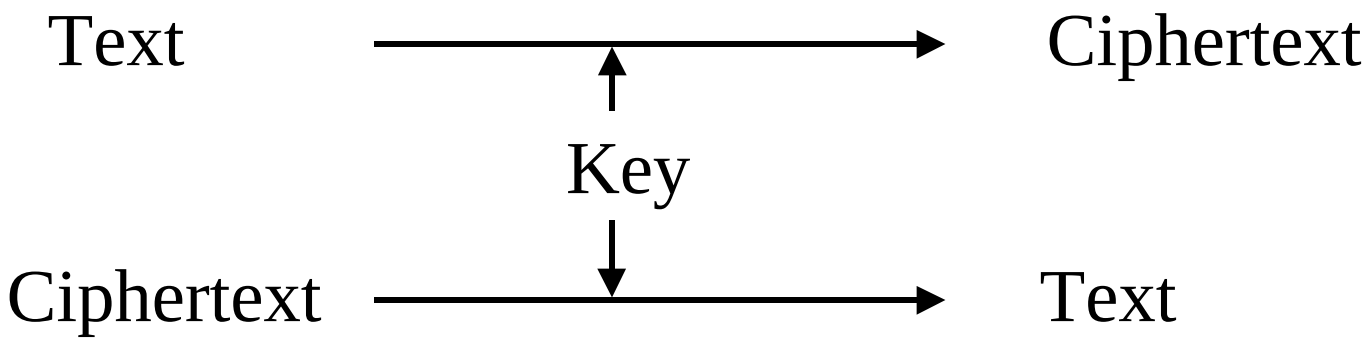
- Data Integrity: Received = sent?
- Data Availability: Legal users should be able to use. Ping continuously ⇒ No useful work gets done.
- Data Confidentiality and Privacy: No snooping or wiretapping
- Authentication: You are who you say you are. A student at Dartmouth posing as a professor canceled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

Security Threats



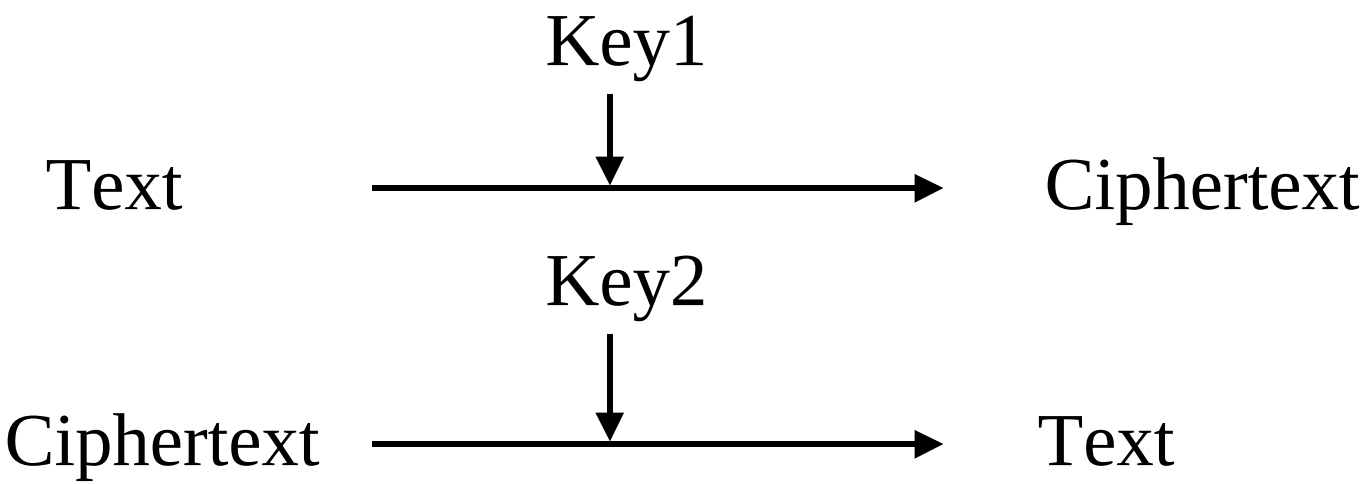
Secret Key Encryption

- Encrypted_Message = Encrypt(Key, Message)
- Message = Decrypt(Key, Encrypted_Message)
- Example: Encrypt = division
- 433 = 48 R 1 (using divisor of 9)



Public Key Encryption

- Invented in 1975 by Diffie and Hellman
- Encrypted_Message = Encrypt(Key1, Message)
- Message = Decrypt(Key2, Encrypted_Message)



Public Key Encryption: Example

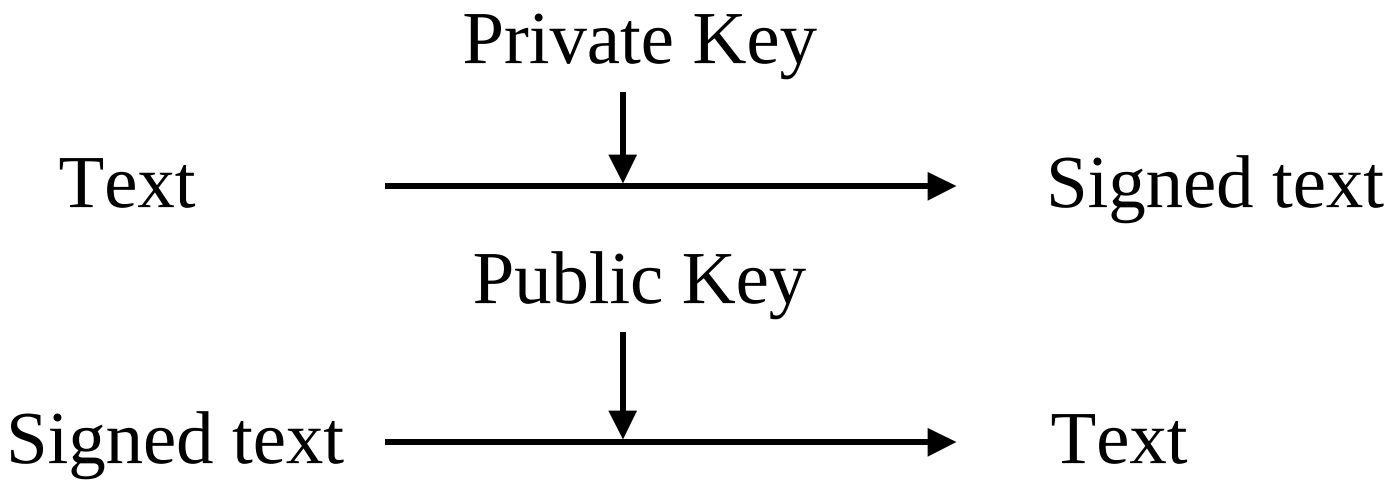
- RSA: Encrypted_Message = m^3 mod 187
- Message = Encrypted_Message^{107} mod 187
- Key1 = <3,187>, Key2 = <107,187>
- Message = 5
- Encrypted Message = $5^3 = 125$
- Message = 125^{107} mod 187
  $= 125^{(64+32+8+2+1)}$ mod 187
  $= [(125^{64} \text{ mod } 187)(125^{32} \text{ mod } 187)...$
  $(125^2 \text{ mod } 187)(125)] \text{ mod } 187 = 5$
- $125^4 \text{ mod } 187 = (125^2 \text{ mod } 187)^2 \text{ mod } 187$

Public Key (Cont)

- One key is private and the other is public
- Message = Decrypt(Public_Key, Encrypt(Private_Key, Message))
- Message = Decrypt(Private_Key, Encrypt(Public_Key, Message))

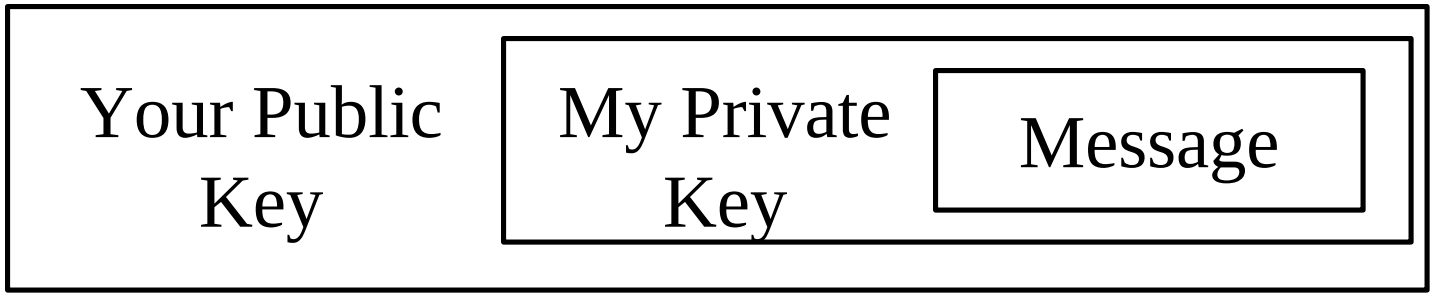
Digital Signature

- Encrypted_Message
  = Encrypt(Private_Key, Message)
- Message = Decrypt(Public_Key, Encrypted_Message)
  ⇒ Authentic

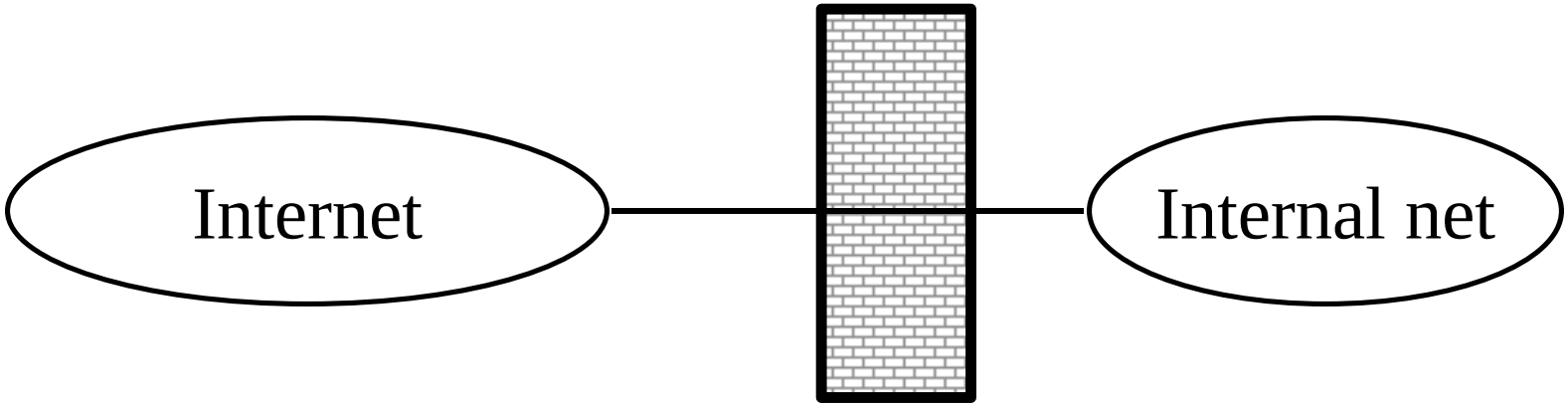


Confidentiality

- User 1 to User 2:
- Encrypted_Message = Encrypt(Public_Key2, Encrypt(Private_Key1, Message))
- Message = Decrypt(Public_Key1, Decrypt(Private_Key2, Encrypted_Message)
  ⇒ Authentic and Private



Simple Firewall: Packet Filter

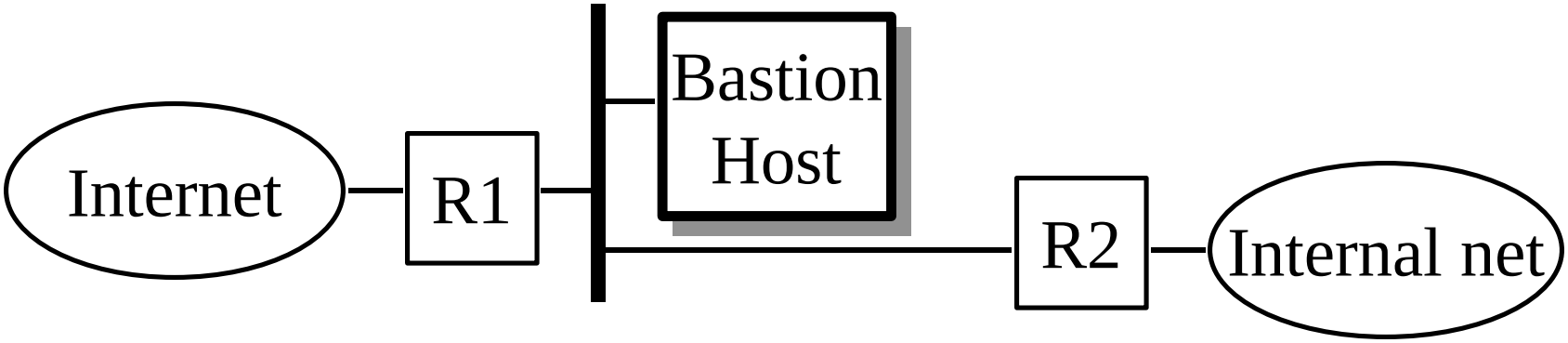


- Example: Only email gets in/out
  ftp to/from nodes x, y, z, etc.
- Problem: Filter is accessible to outside world

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

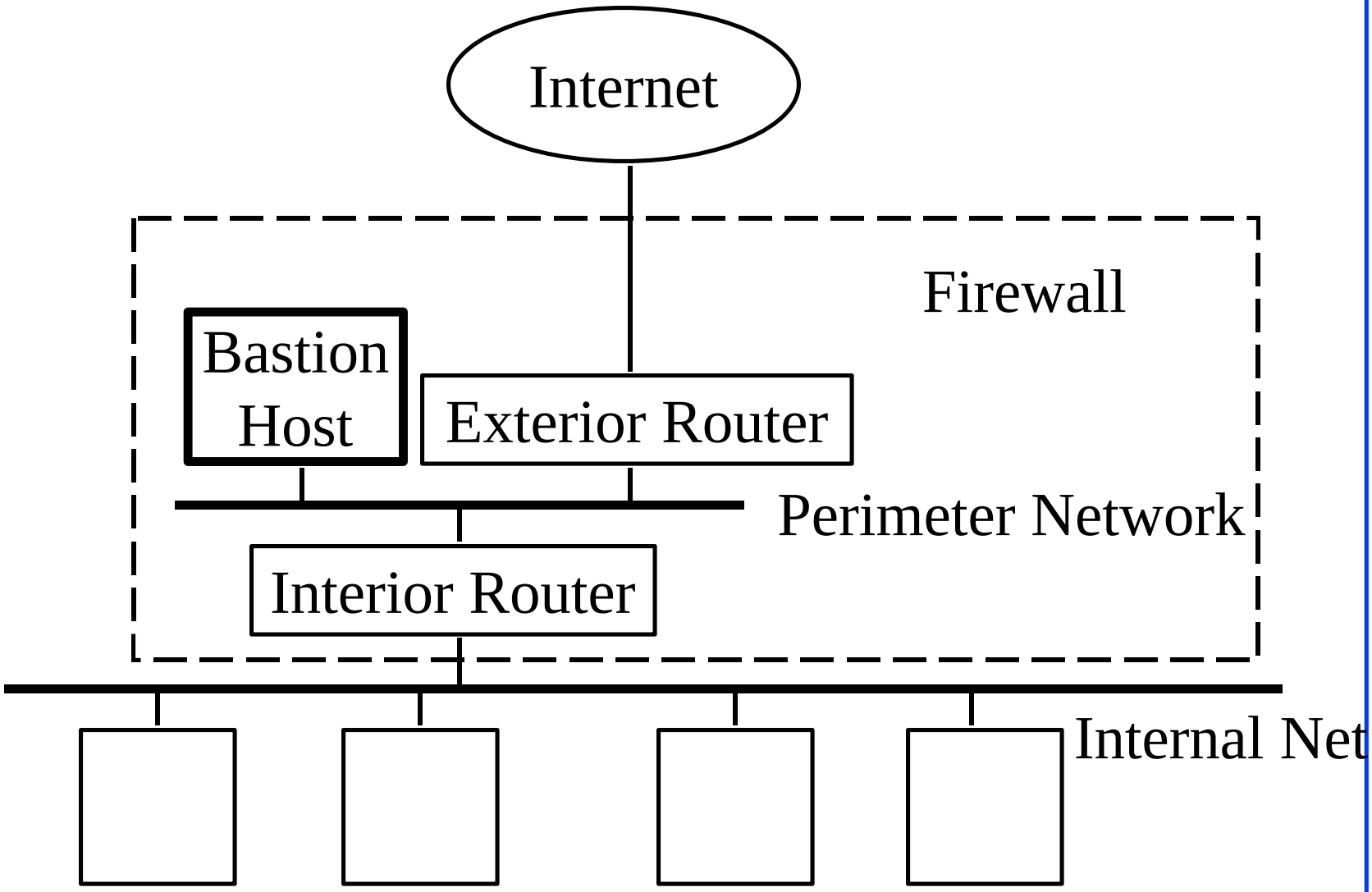


- Bastions overlook critical areas of defense, usually having stronger walls
- Inside users need a mechanism to get outside services
- Inside users log on the Bastion Host and use outside services.
- Later they pull the results inside.

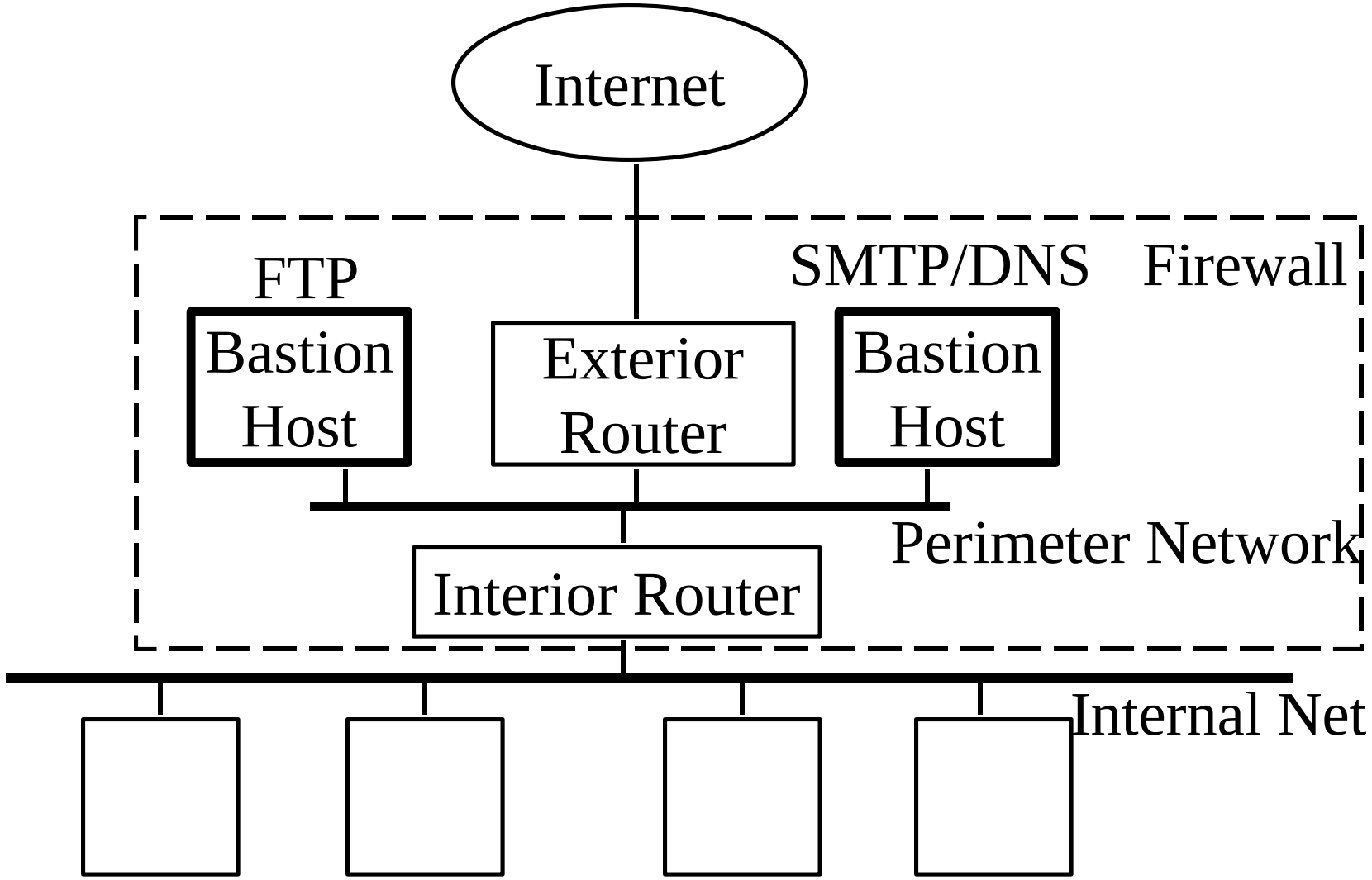
Bastion Host (Cont)

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

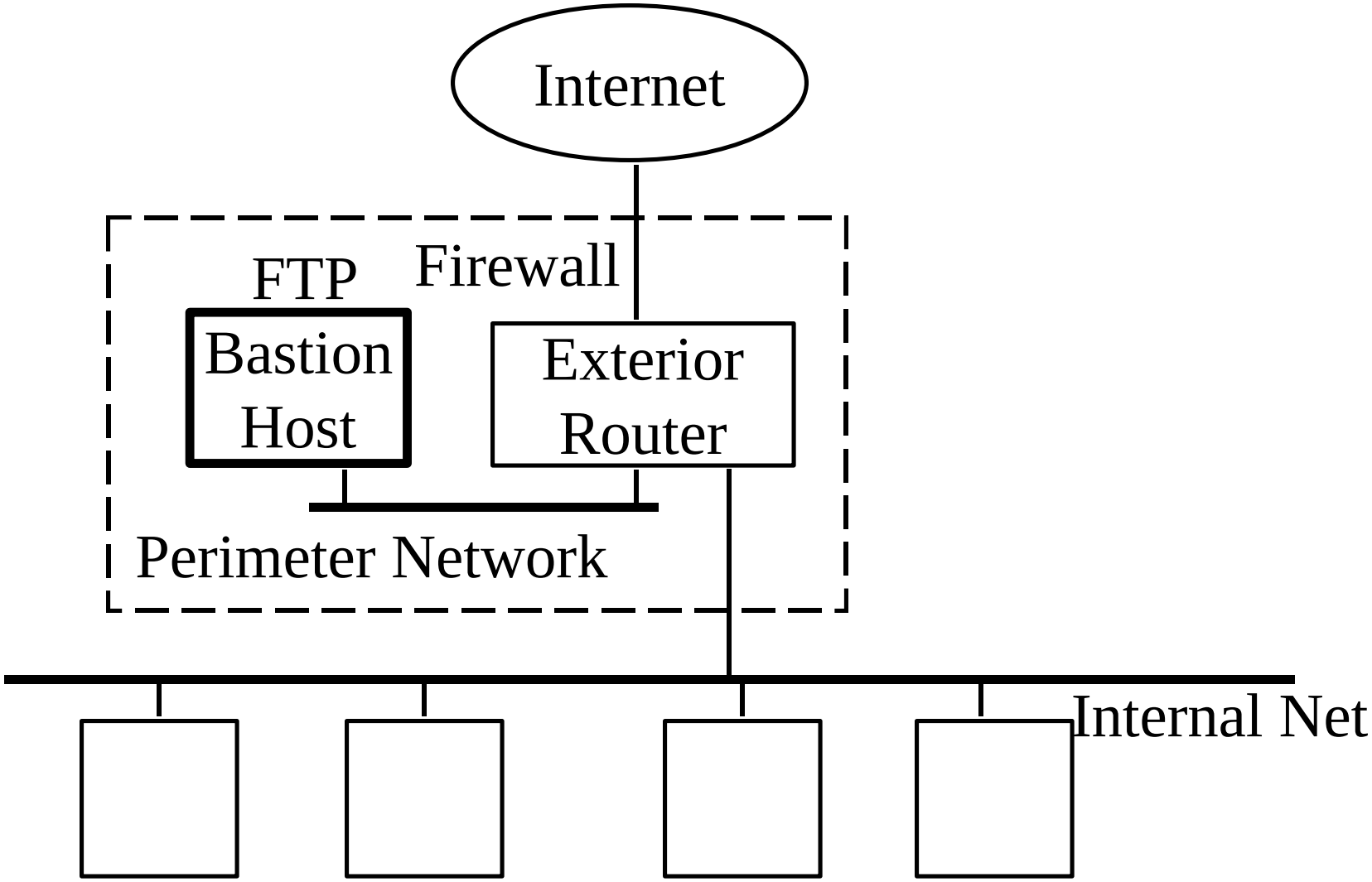
Screened Subnet Architecture



Multiple Bastion Hosts

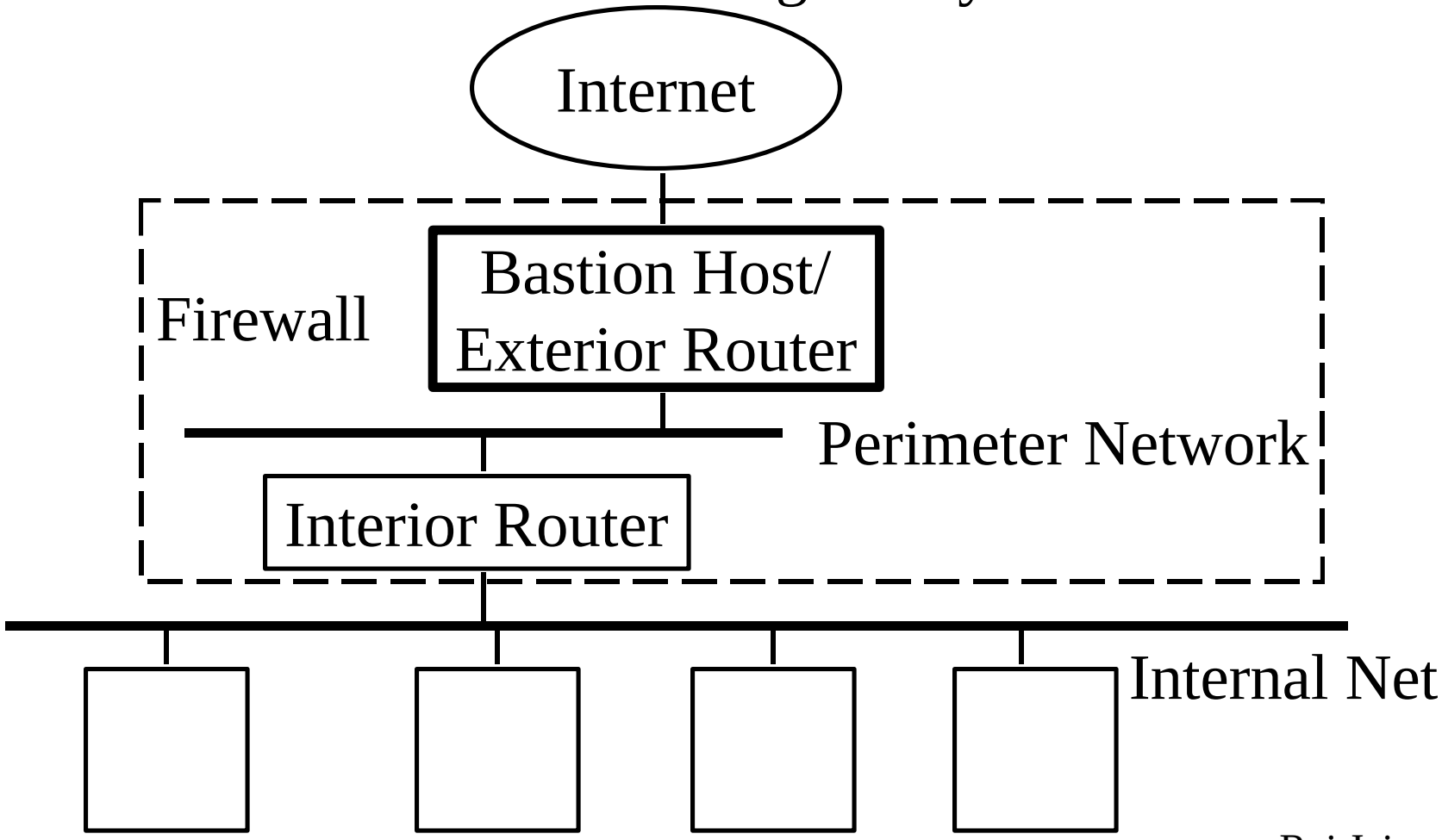


Merged Interior and Exterior Routers

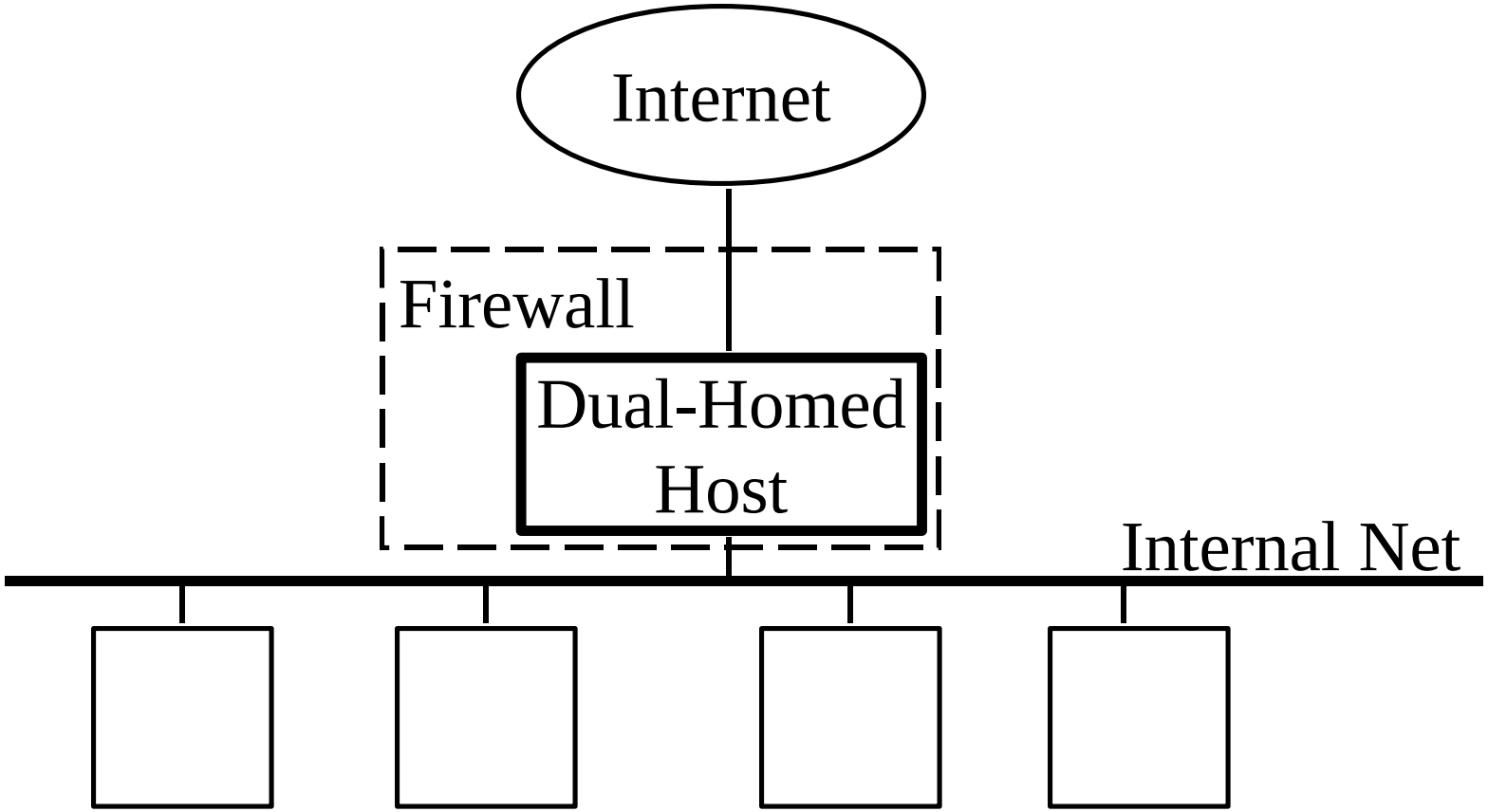


Merged Bastion Host and Exterior Router

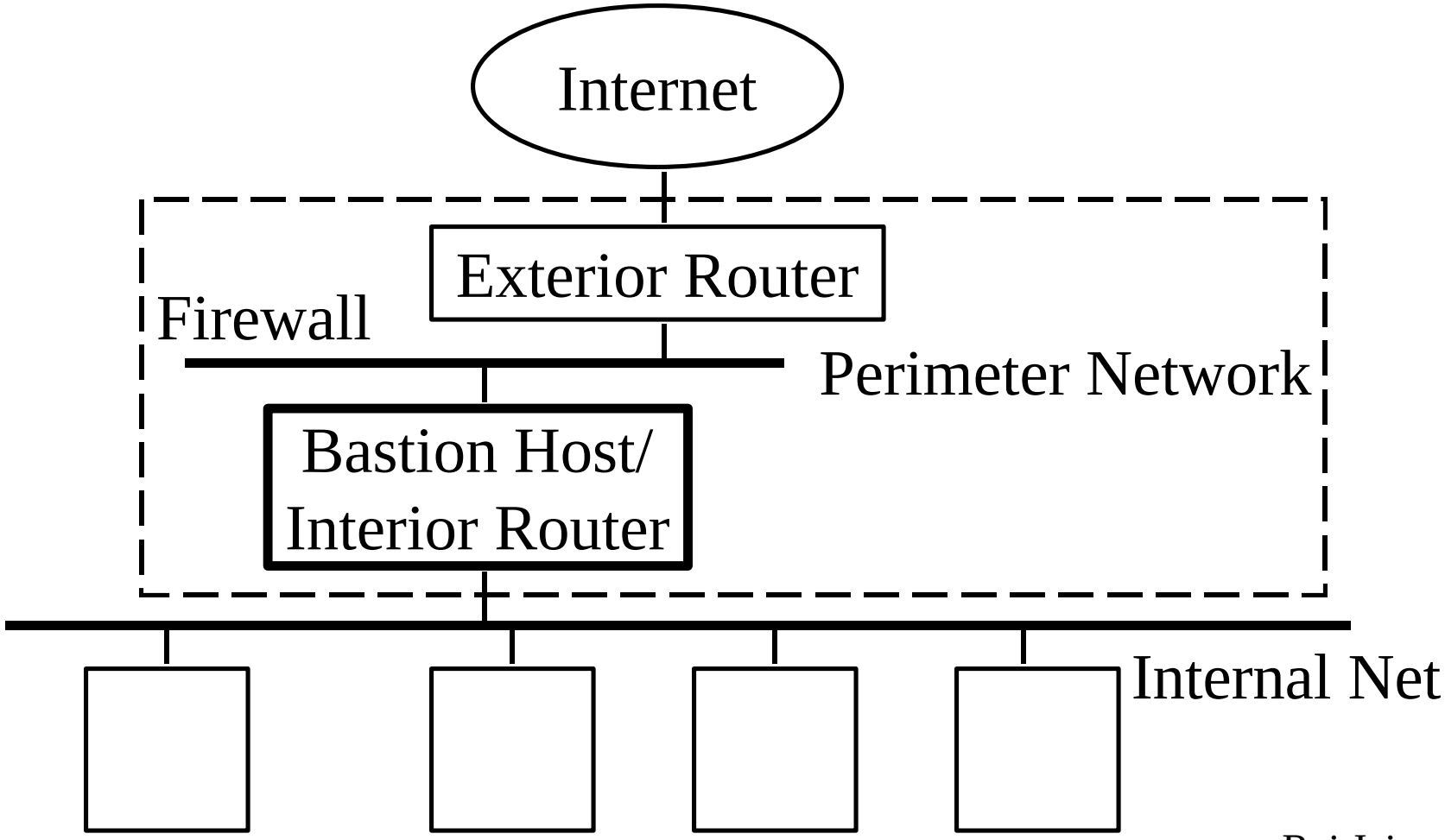
- Also known as a dual-homed gateway



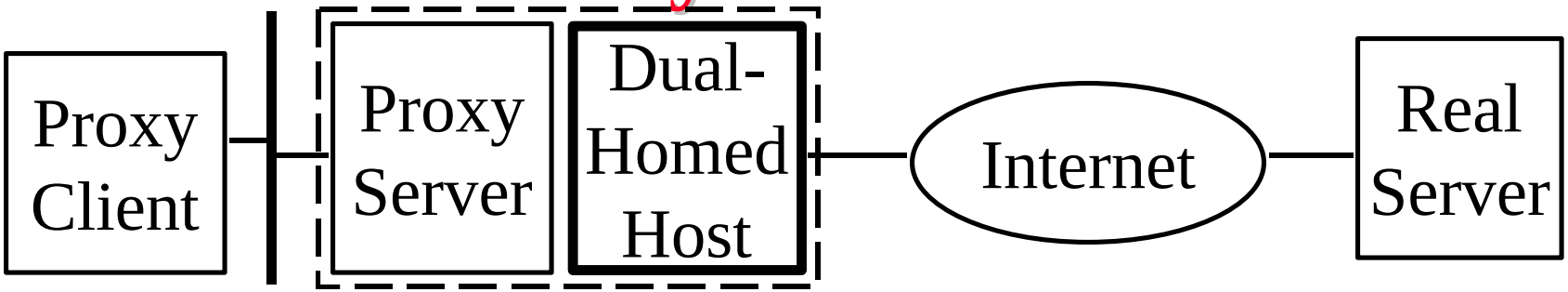
Dual-Homed Host Architecture



Merged Bastion Host and Interior Router (Not Recommended)



Proxy Servers



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

What Firewalls Can't Do

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

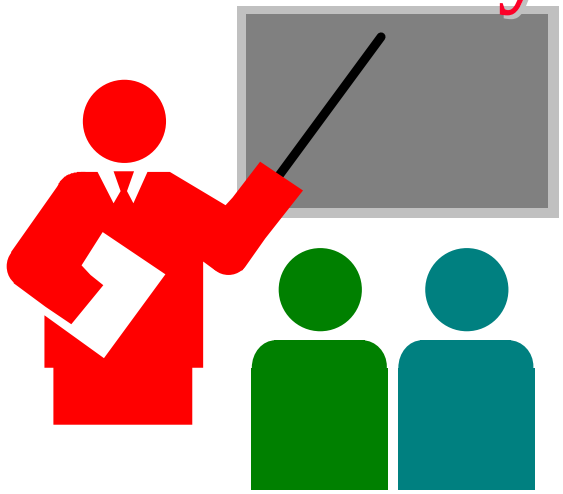
Security Mechanisms on The Internet

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

Pretty Good Privacy (PGP)

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

Summary



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