Chapter 31
Network Security

Raj Jain

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

Overview

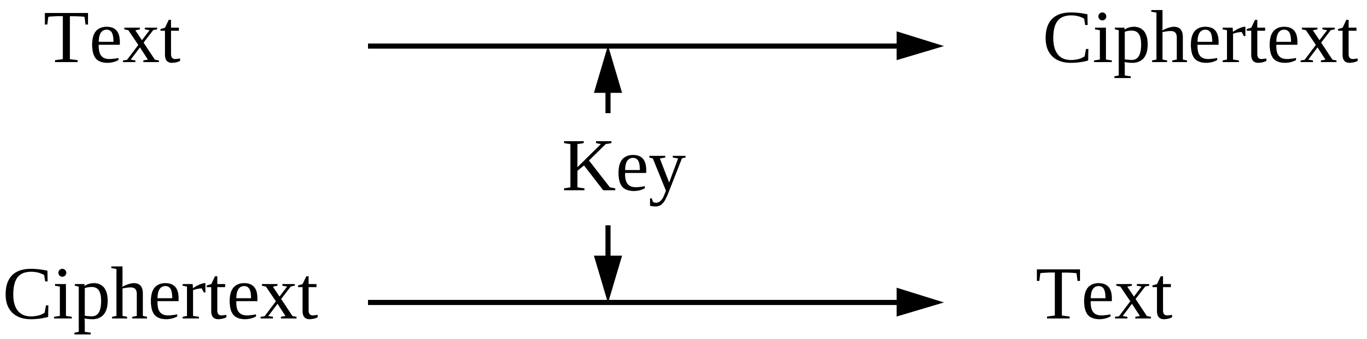
- Security Aspects
- Secret Key and Public Key Encryption
- Firewalls: Packet Filter, Bastion Host, Perimeter Nets
- Variations of firewalls
- Proxy servers

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

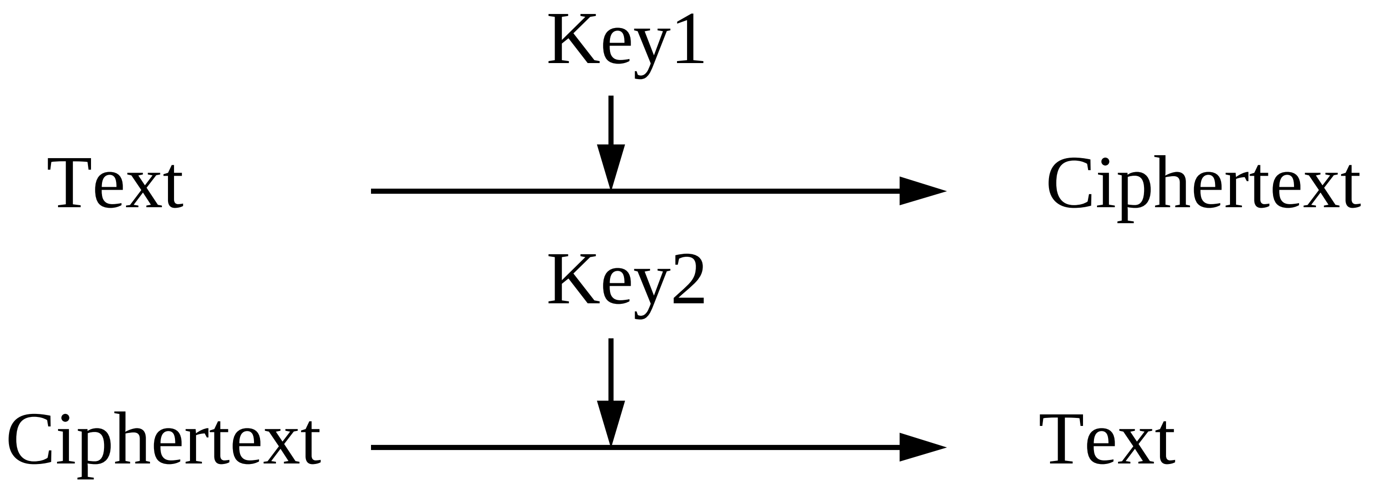
Secret Key Encryption

- 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)



Key1

Text → Ciphertext

Key2

Ciphertext → Text

Public Key Encryption: Example

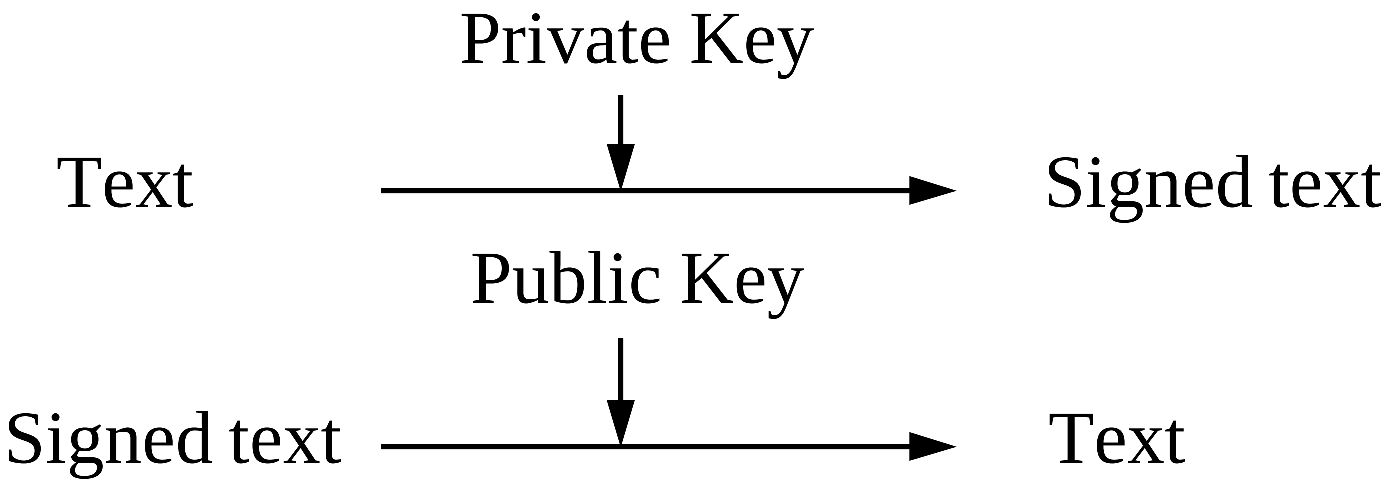
- RSA: Encrypted_Message = m^3 mod 187
- Message = Encrypted_Message^{107} mod 187
- Key1 = <3,187>, Key2 = <107,187>
- Message = 5
- Encrypted Message = $5^3 = 125$
- Message = 125^{107} mod 187
  = $125^{(64+32+8+2+1)}$ mod 187
  = (125^{64} mod 187)(125^{32} mod 187)...
  (125^2 mod 187)(125)
  =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

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



Private Key

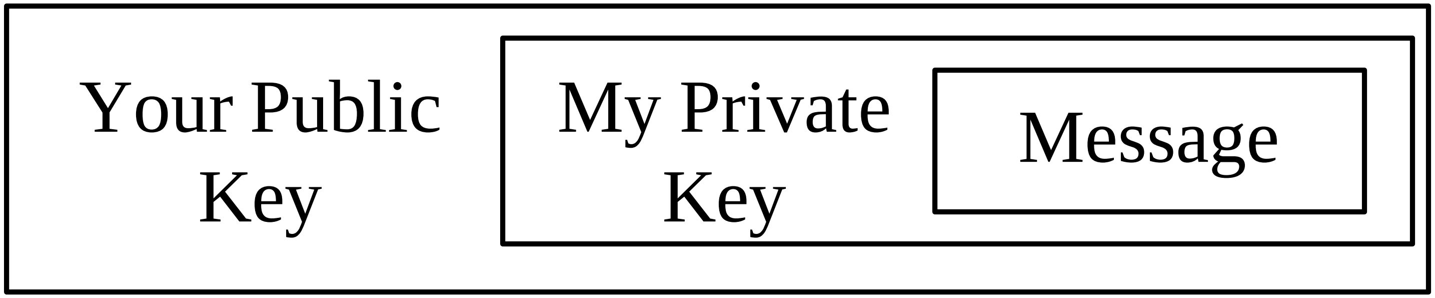
Text → Signed text

Public Key

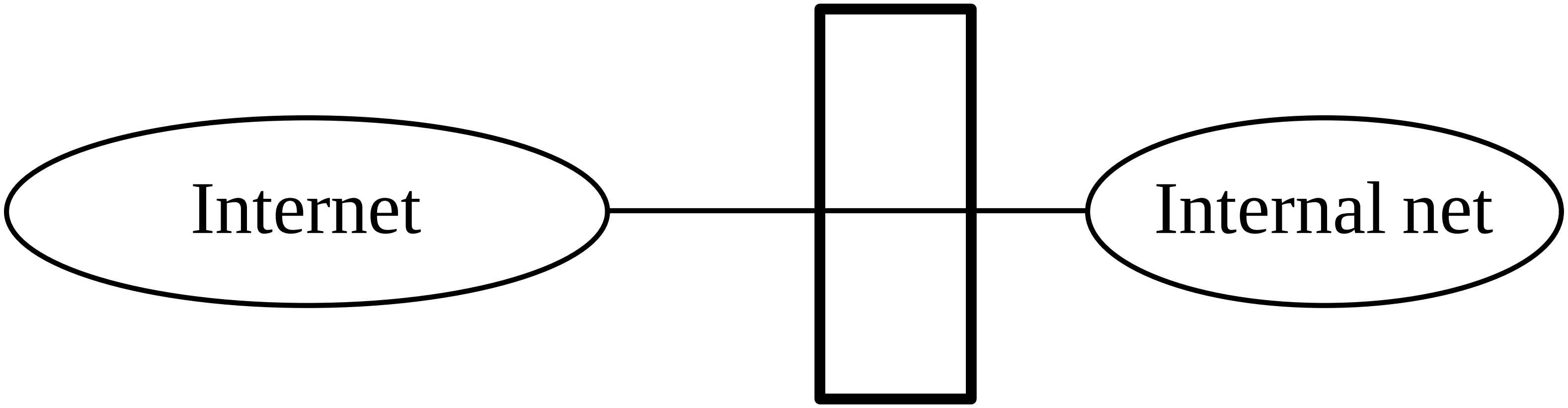
Signed text → Text

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

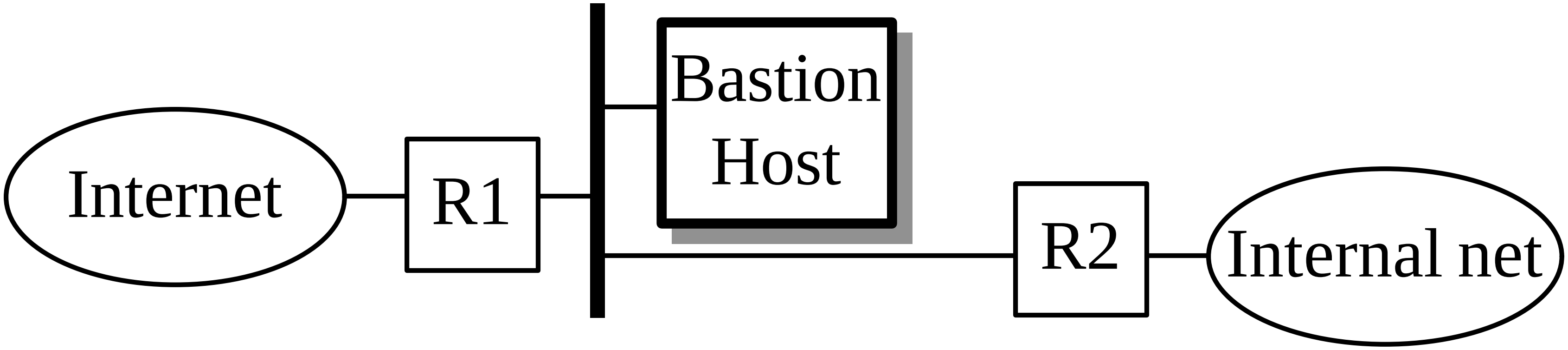


- Example: Only email gets in/out
  ftp to/from nodes x, y, z, etc.
- Problem: Filter is accessible to outside world

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

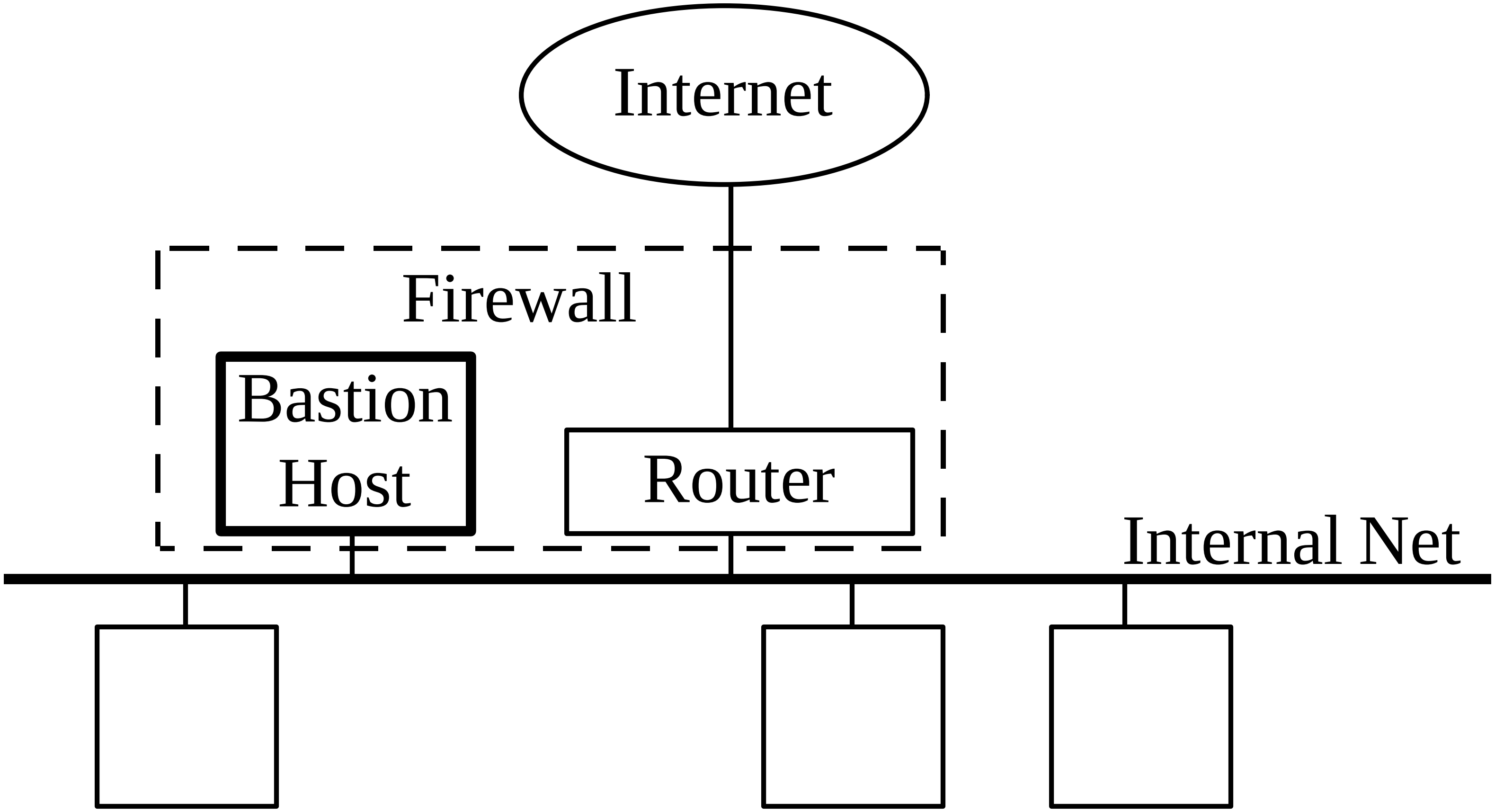


- Bastions overlook critical areas of defense, usually having stronger walls
- Inside users need a mechanism to get outside services
- Inside users log on the Bastion Host and use outside services.
- Later they pull the results inside.

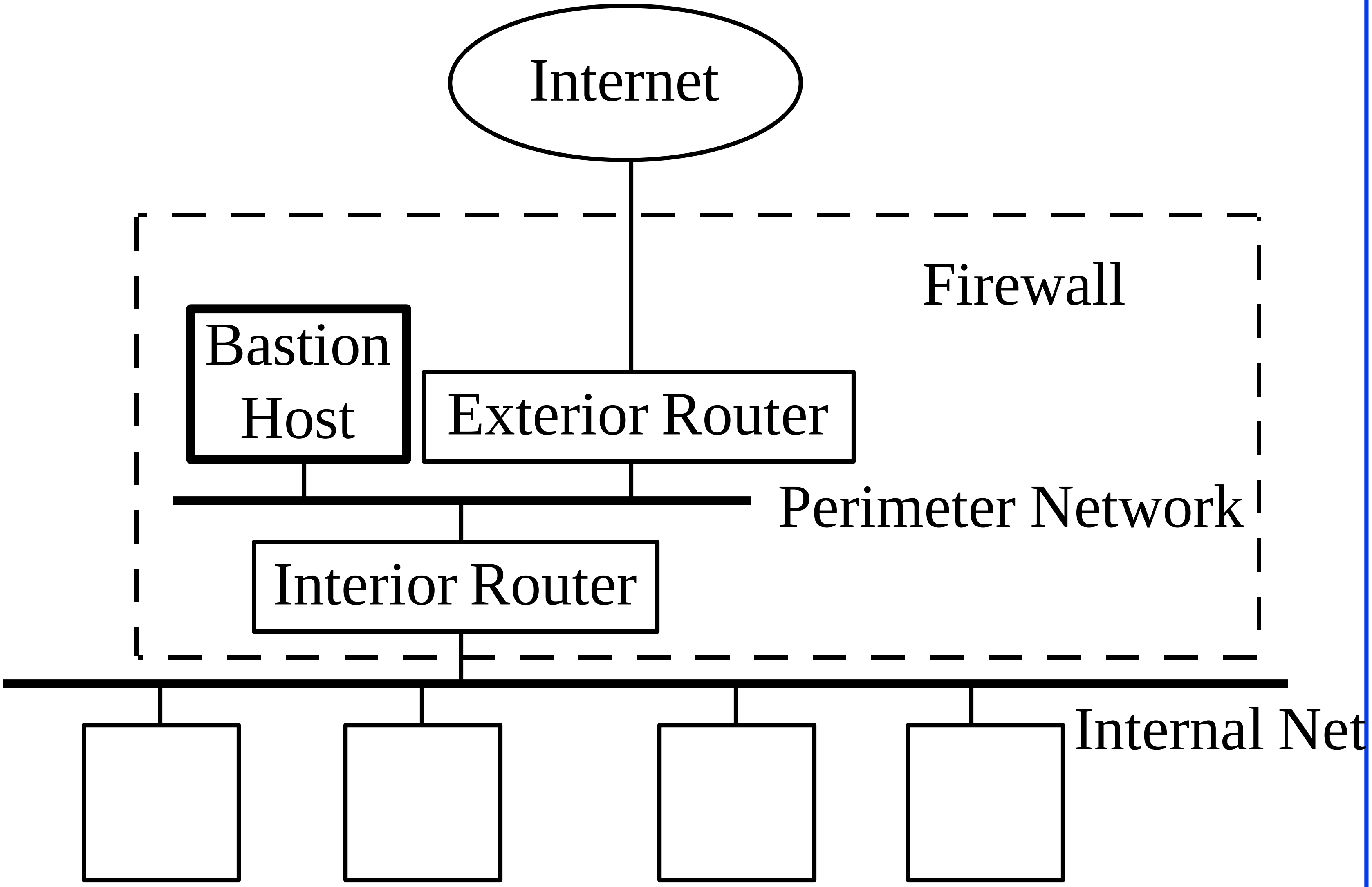
Bastion Host (Cont)

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

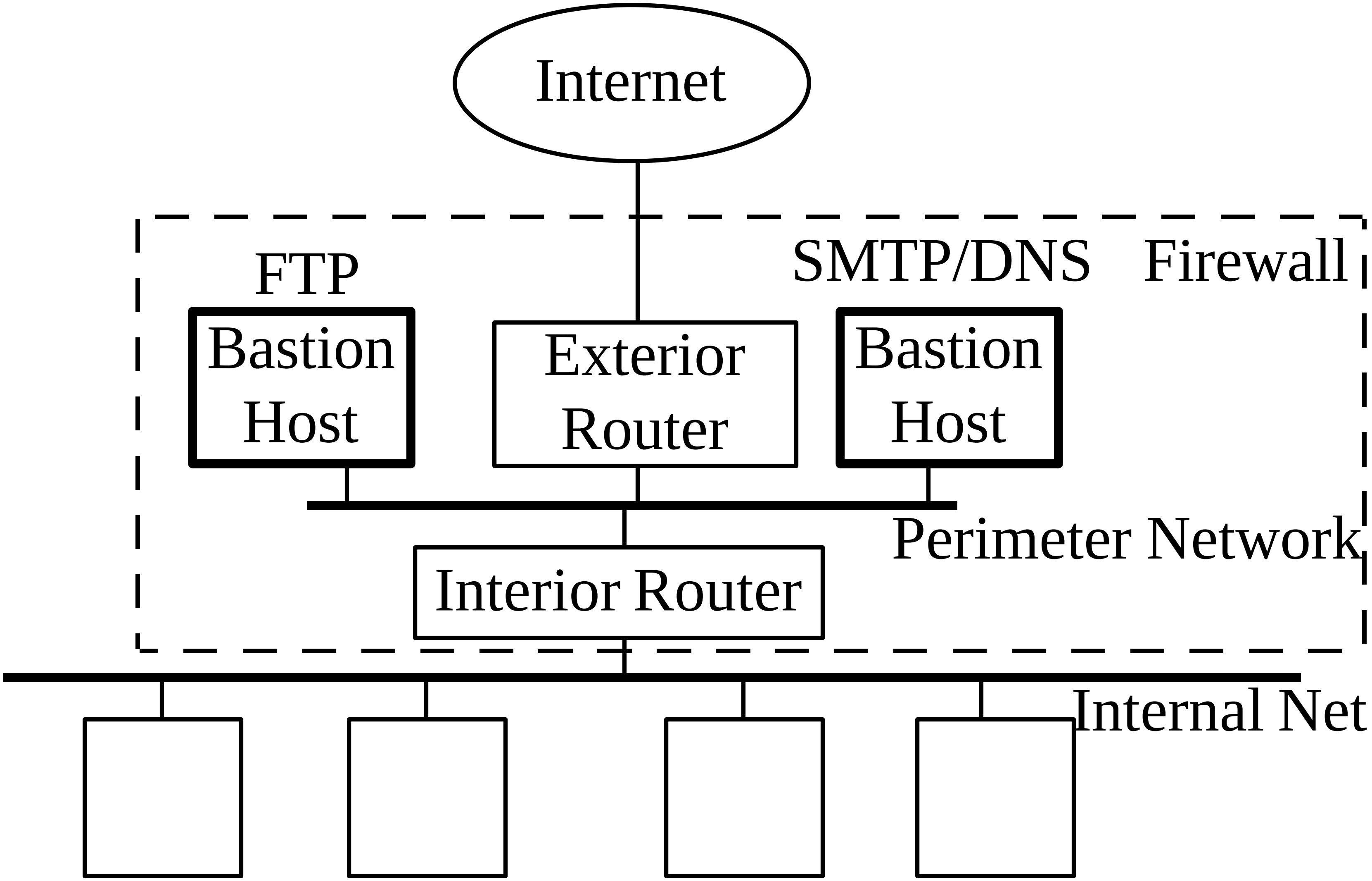
Screened Host Architecture



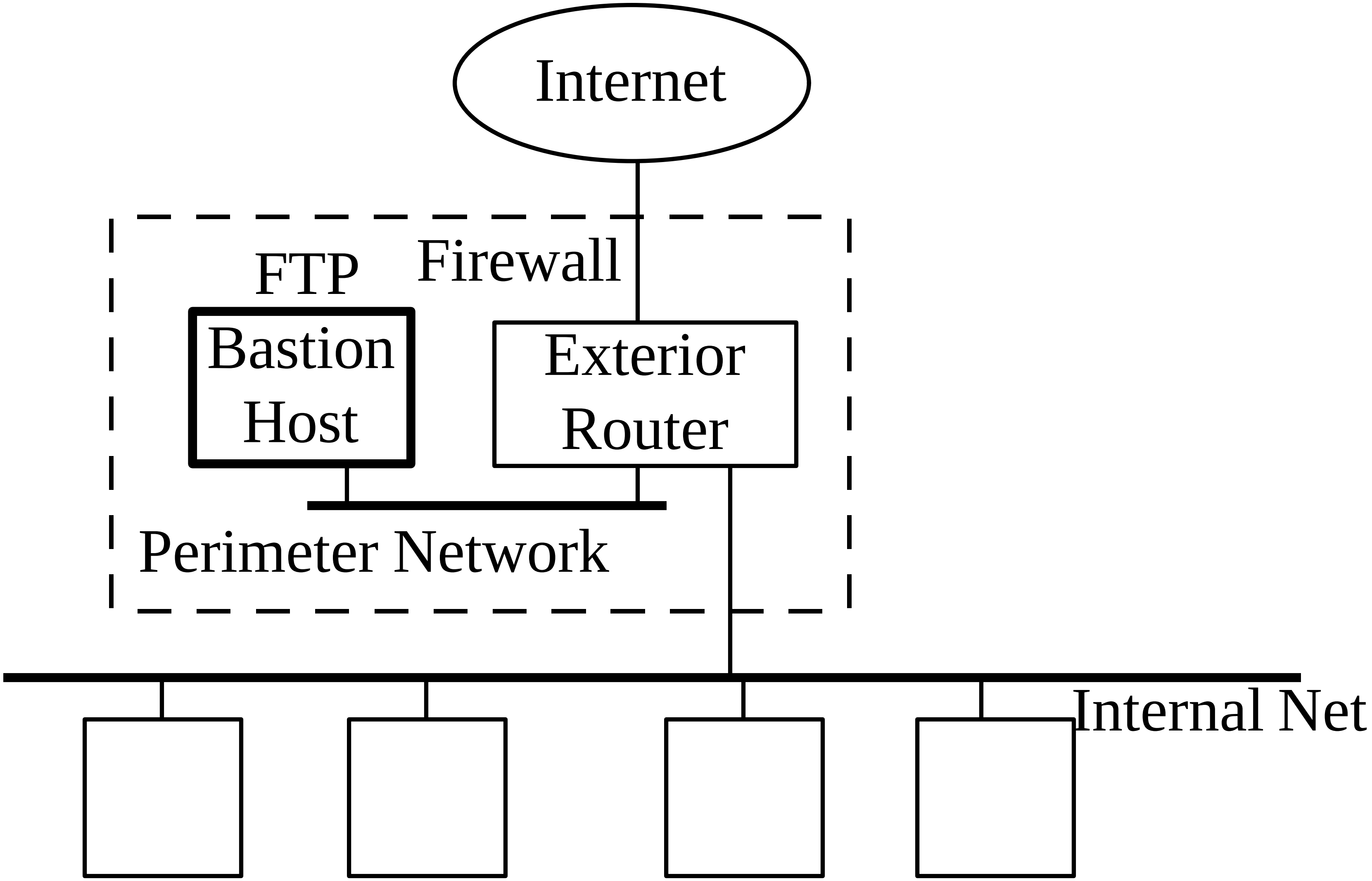
Screened subnet Architecture



Multiple Bastion Hosts

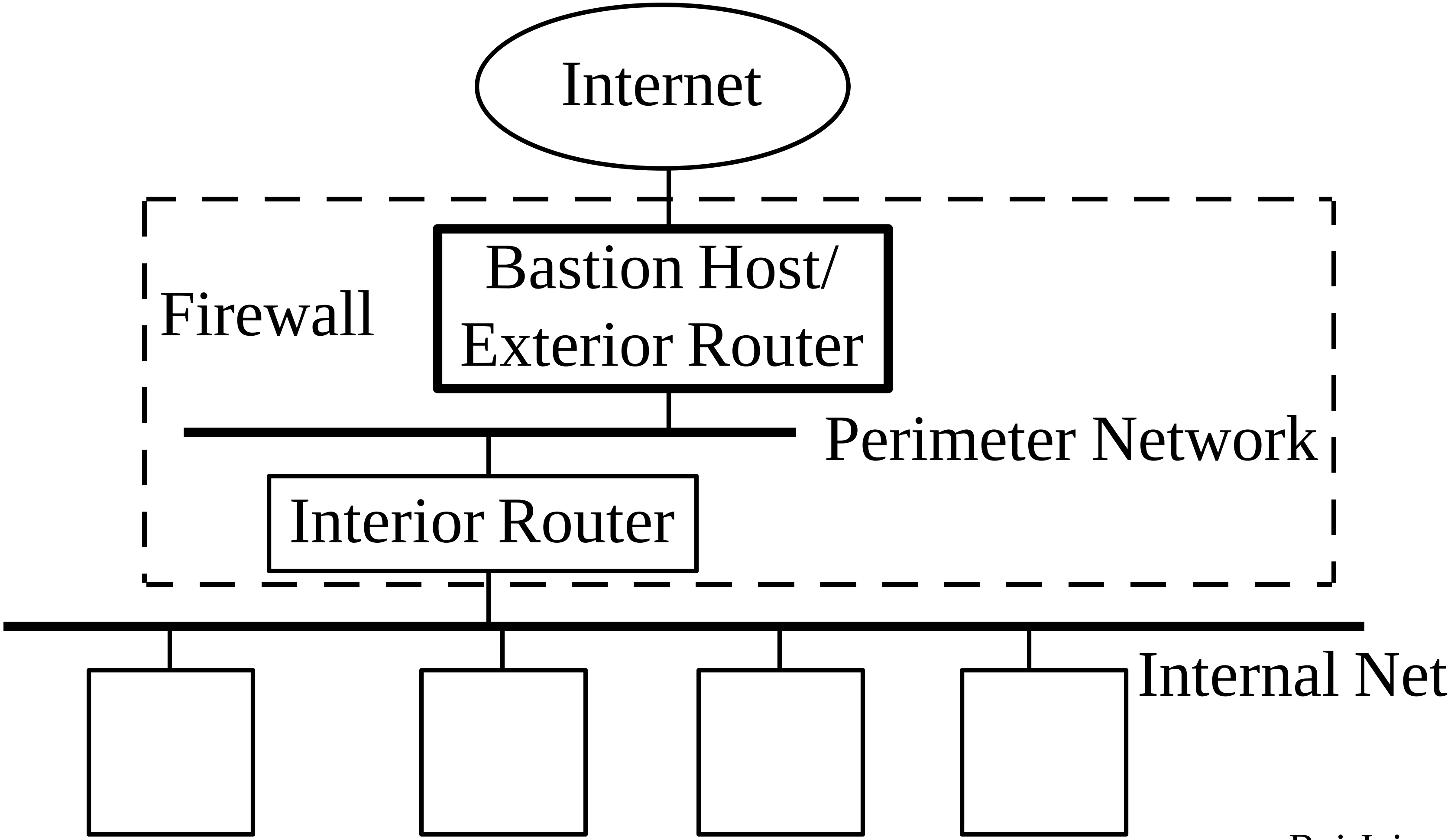


Merged Interior and Exterior Routers

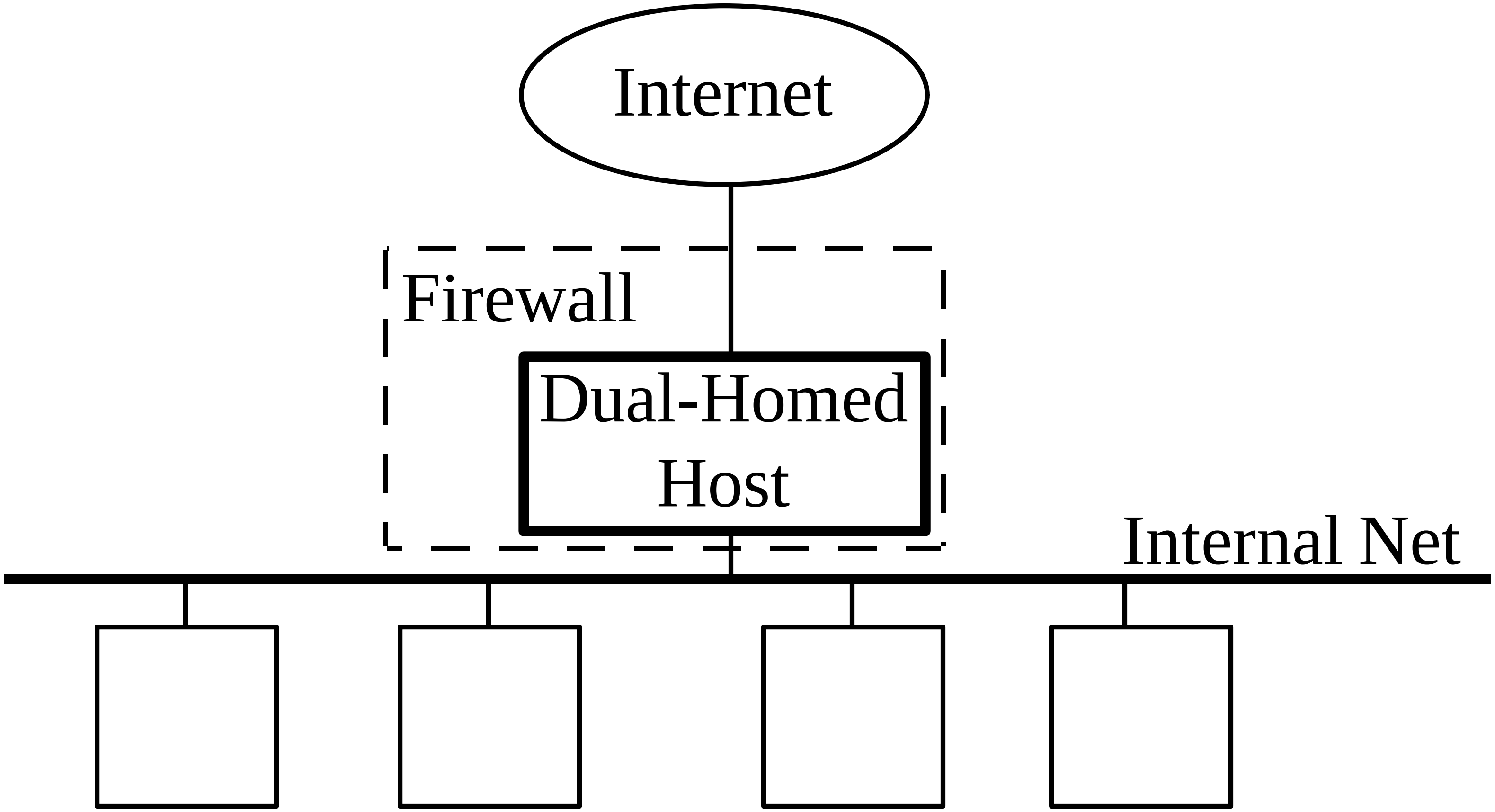


Merged Bastion Host and Exterior Router

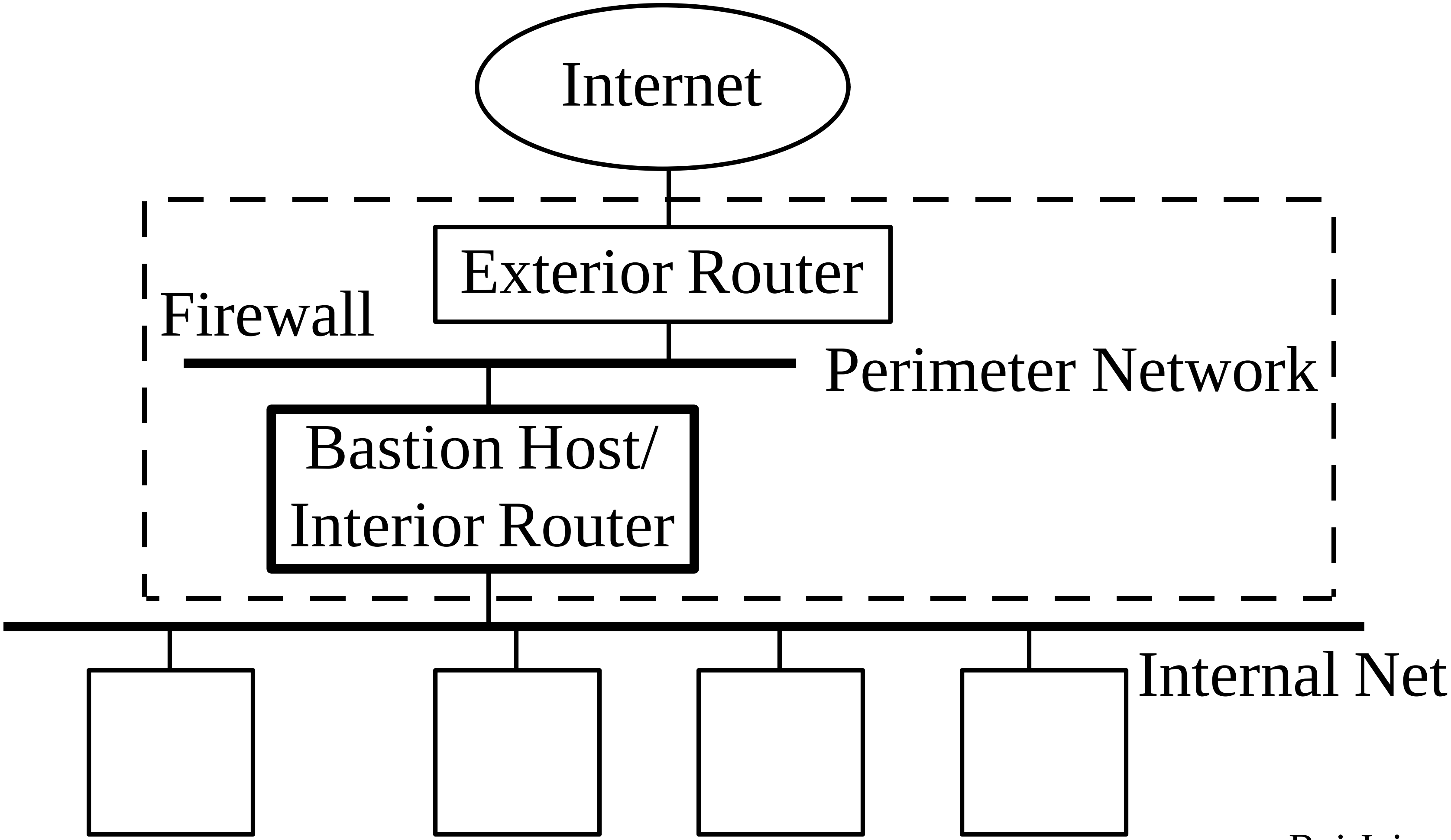
- Also known as a dual-homed gateway



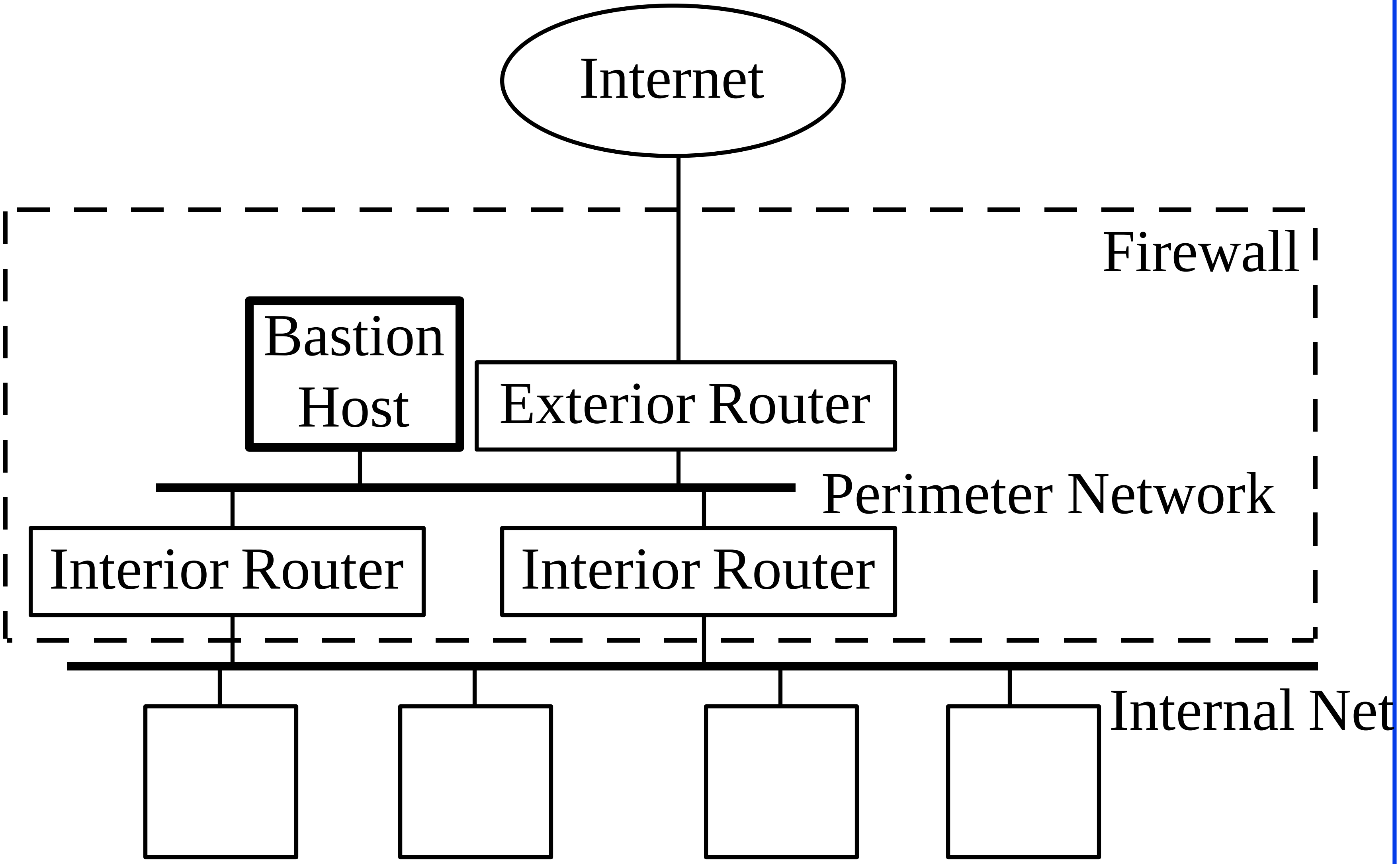
Dual-Homed Host Architecture



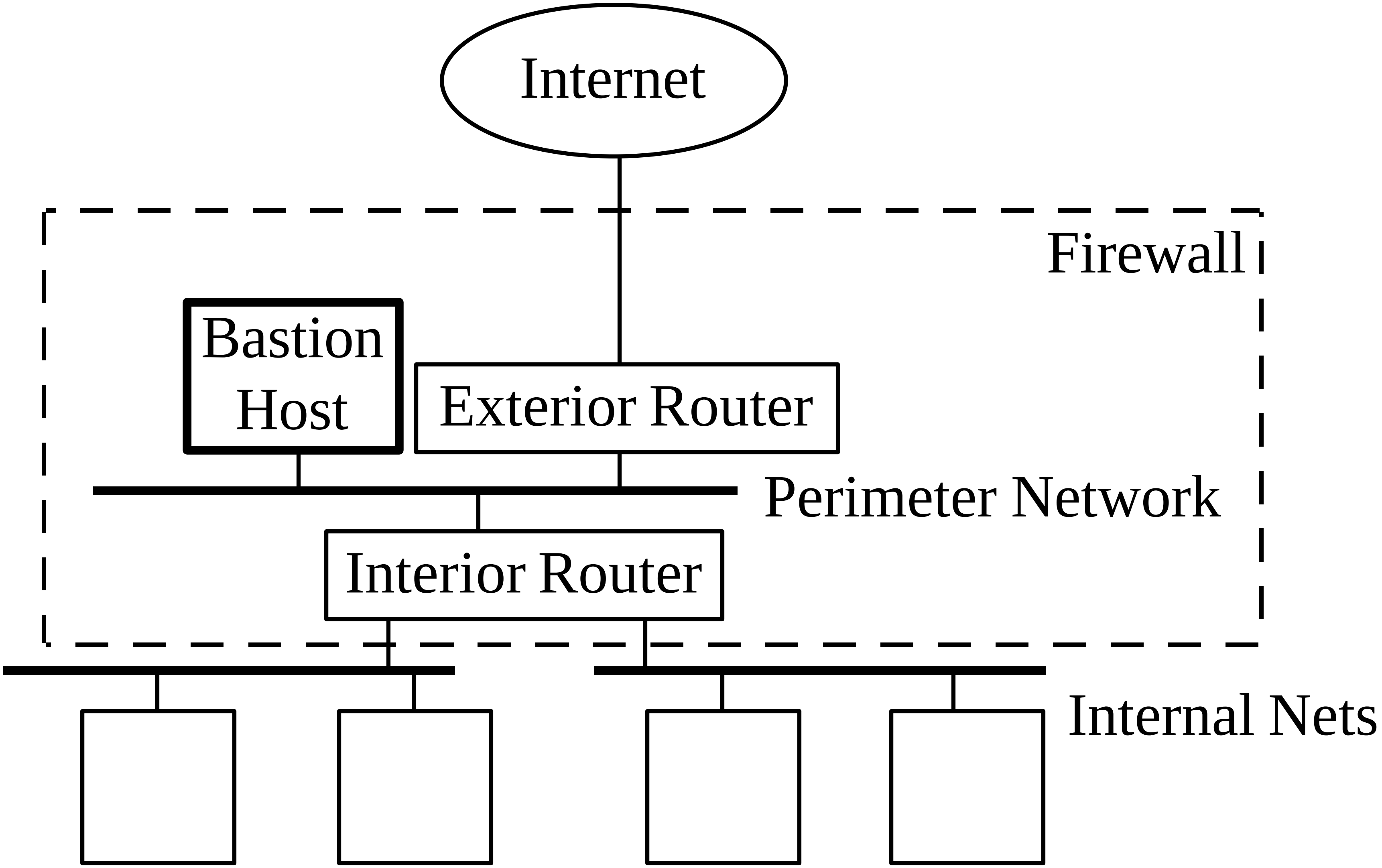
Merged Bastion Host and Interior Router (Not Recommended)



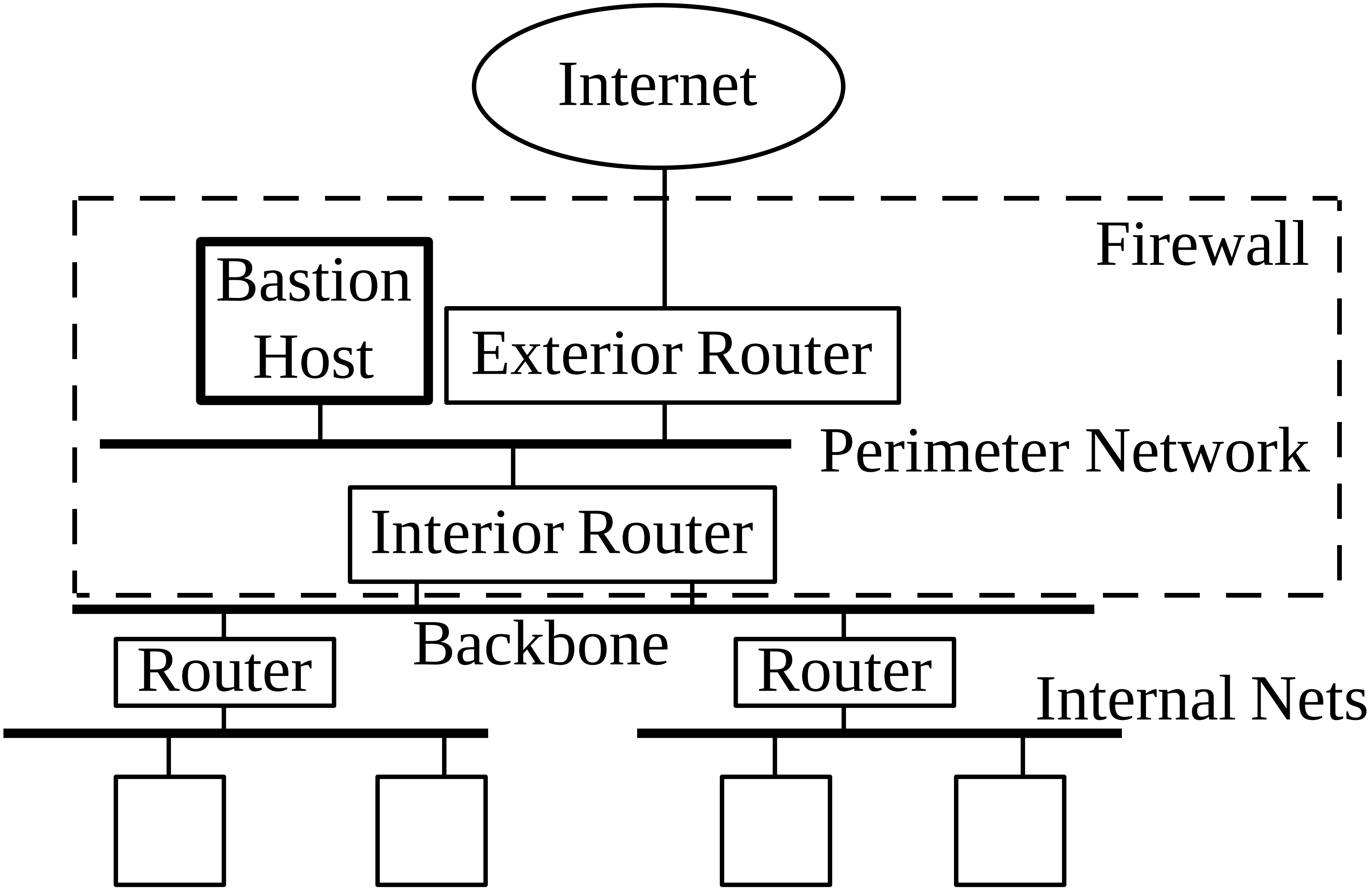
Multiple Interior Routers



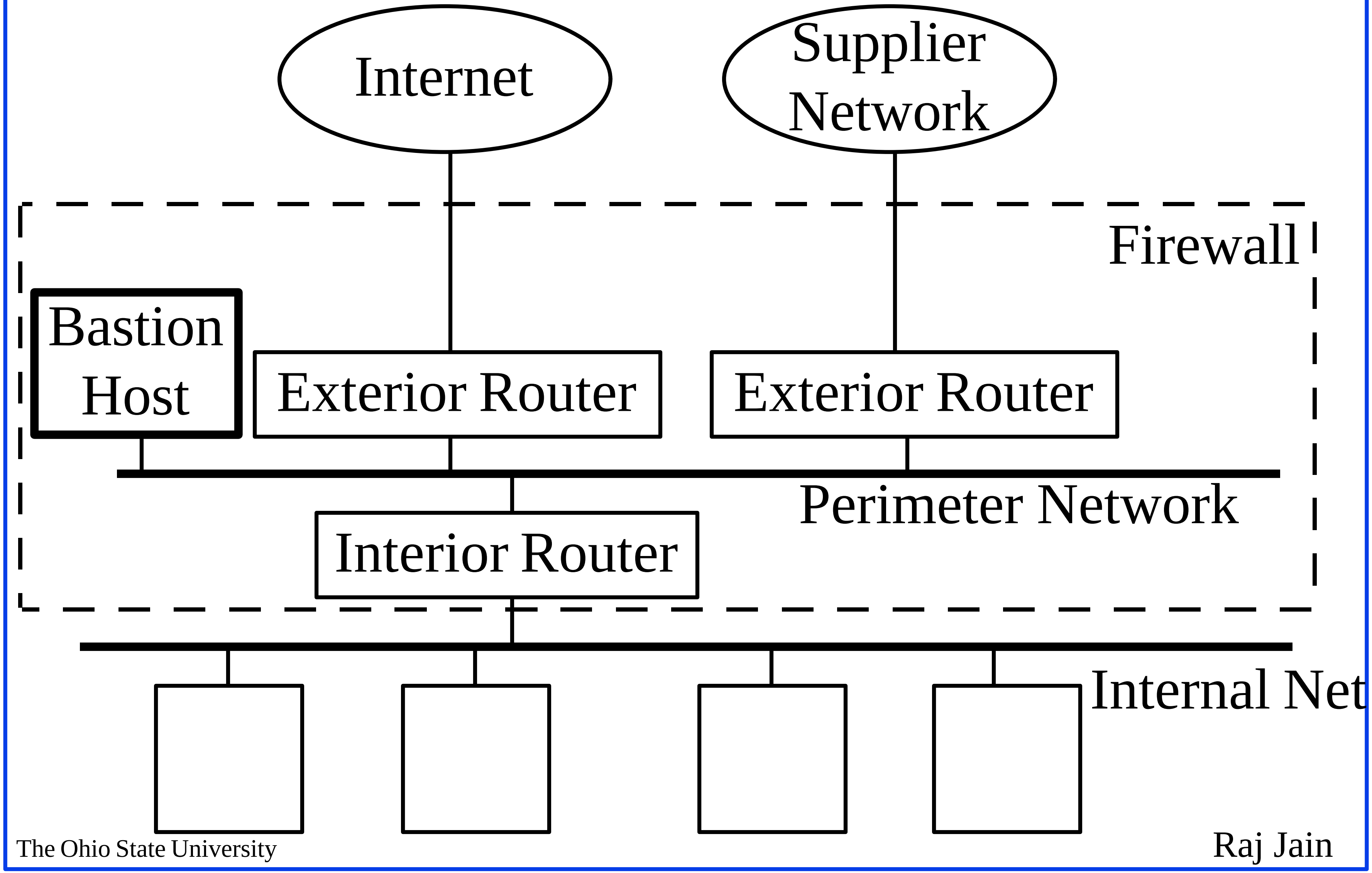
Multiple Internal Networks



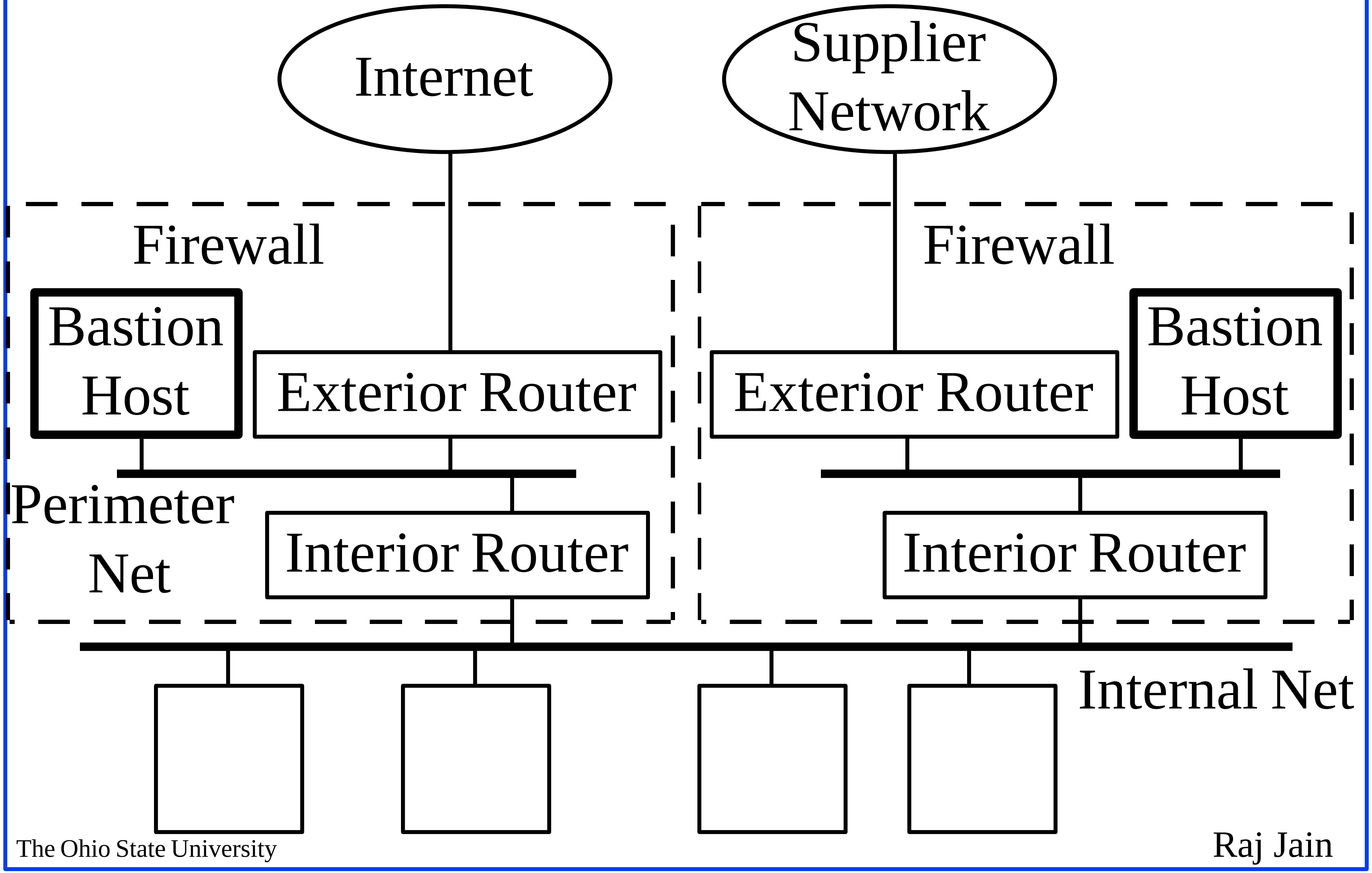
Multiple Internal Networks with a Backbone



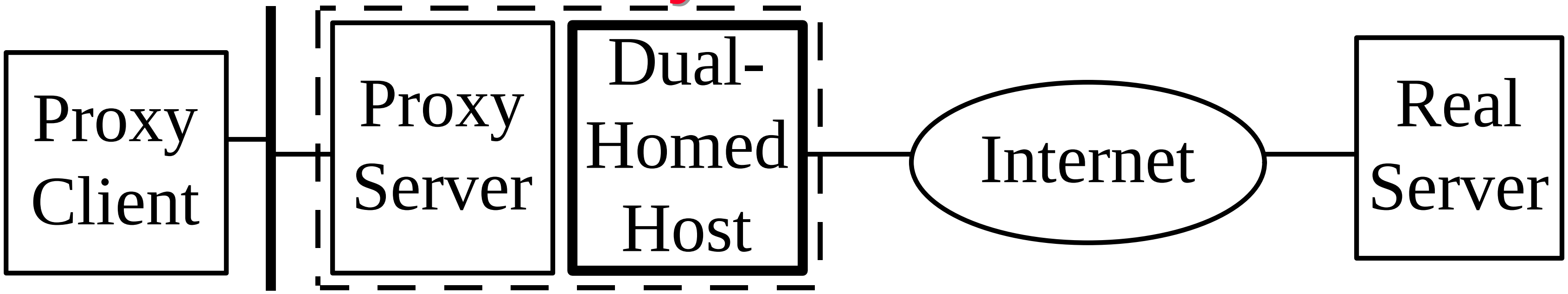
Multiple Exterior Routers



Multiple Perimeter Networks



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

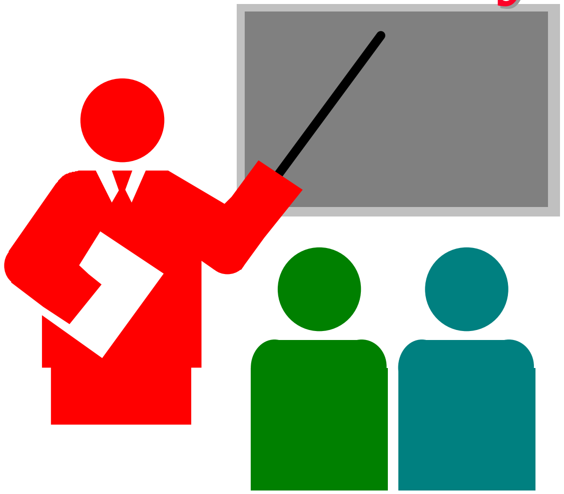
What Firewalls Can't Do

- 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

Summary



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

Homework

❑ Read Chapter 31

❑ Submit answer to Exercise 31.3

References

- D. B. Chapman and E. D. Zwicky, “Building Internet Firewalls,” O’Reilly & Associates, 1995
- D. E. Comer, “Internetworking with TCP/IP,” Vol. 1, 3rd Ed, Prentice Hall, 1995, Chapter 28.
- C. Kaufman, R. Perlman, M. Speciner, “Network Security,” Prentice-Hall, 1995.
- Coast Security Project at Purdue University http://www.cs.purdue.edu/coast/coast.html

Security: RFCs

- [RFC1848] S. Crocker, N. Freed, J. Galvin, S. Murphy, "MIME Object Security Services", 10/03/1995, 48 pages.
- [RFC1847] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", 10/03/1995, 11 pages.
- [RFC1108] S. Kent, "U.S. Department of Defense Security Options for the Internet Protocol", 11/27/1991, 17 pages.
- [RFC1244] P. Holbrook, J. Reynolds, "Site Security Handbook", 07/23/1991, 101 pages. (FYI 8)
- [RFC1352] J. Davin, J. Galvin, K. McCloghrie, "SNMP Security Protocols", 07/06/1992, 41 pages.
- [RFC1446] J. Galvin, K. McCloghrie, "Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)", 05/03/1993, 51 pages.

- [RFC1455] D. Eastlake, III, "Physical Link Security Type of Service", 05/26/1993, 6 pages.
- [RFC1457] R. Housley, "Security Label Framework for the Internet", 05/26/1993, 14 pages.
- [RFC1472] F. Kastenholz, "The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol", 06/08/1993, 11 pages.
- [RFC1507] C. Kaufman, "DASS - Distributed Authentication Security Service", 09/10/1993, 119 pages.
- [RFC1509] J. Wray, "Generic Security Service API : C-bindings", 09/10/1993, 48 pages.
- [RFC1535] E. Gavron, "A Security Problem and Proposed Correction With Widely Deployed DNS Software", 10/06/1993, 5 pages.
- [RFC1636] I. Architecture Board, R. Braden, D. Clark, S. Crocker, C. Huitema, "Report of IAB Workshop on Security in the Internet Architecture - February 8-10, 1994", 06/09/1994, 52 pages.
- [RFC1675] S. Bellovin, "Security Concerns for IPng", 08/08/1994, 4 pages.
- [RFC1750] D. Eastlake, S. Crocker, J. Schiller, "Randomness Recommendations for Security", 12/29/1994, 25 pages.

- [RFC1824] H. Danisch, "The Exponential Security System TESS: An Identity-Based Cryptographic Protocol for Authenticated Key-Exchange (E.I.S.S.-Report 1995/4)", 08/11/1995, 21 pages.
- [RFC1825] R. Atkinson, "Security Architecture for the Internet Protocol", 08/09/1995, 22 pages.
- [RFC1827] R. Atkinson, "IP Encapsulating Security Payload (ESP)", 08/09/1995, 12 pages.
- [RFC1858] P. Ziemba, D. Reed, P. Traina, "Security Considerations for IP Fragment Filtering", 10/25/1995, 10 pages.
- [RFC1910] G. Waters, "User-based Security Model for SNMPv2", 02/28/1996, 44 pages.
- [RFC2015] M. Elkins, "MIME Security with Pretty Good Privacy (PGP)", 10/14/1996, 8 pages.
- [RFC2065] D. Eastlake, C. Kaufman, "Domain Name System Security Extensions", 01/03/1997, 41 pages. (Updates RFC1034)
- [RFC2078] J. Linn, "Generic Security Service Application Program Interface, Version 2", 01/10/1997, 85 pages.

- [RFC2084] G. Bossert, S. Cooper, W. Drummond, "Considerations for Web Transaction Security", 01/22/1997, 6 pages.