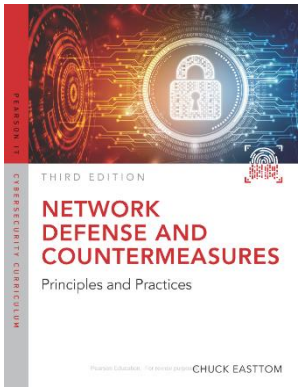
Implementing Firewalls



Based on slides accompanying the book
Network Defense and Countermeasures
by Chuck Easttom (2018)

Objectives

- Understand how firewalls are deployed in different networks
  - host-based firewalls vs router-based firewalls
  - Other configurations

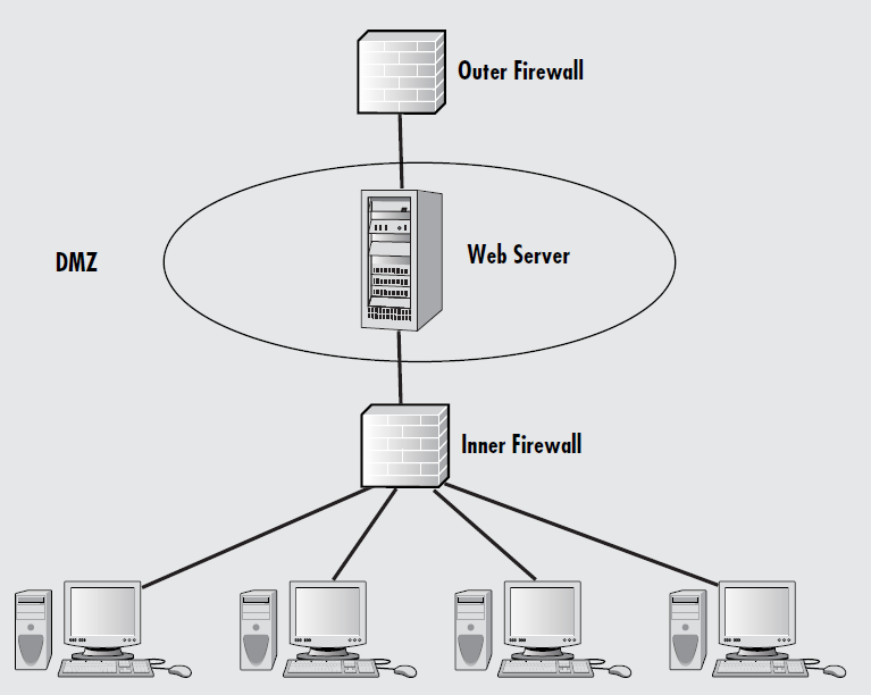
Implementing Firewalls

- Need to understand the firewall's relationship to the network it is protecting
- Most common solutions
  - Network host-based
  - Dual-homed host
  - Router-based firewall
  - Screened host

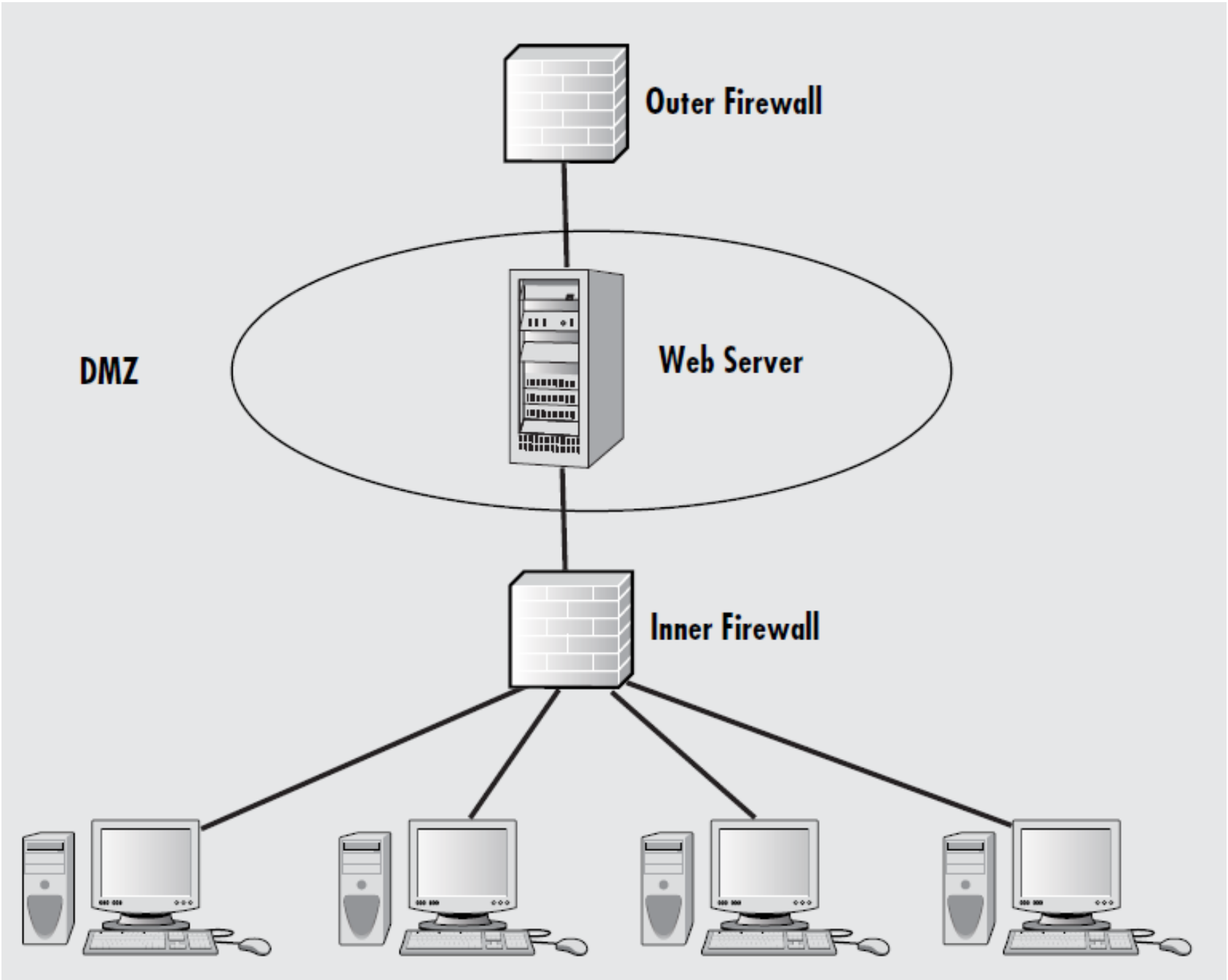
Network Host-Based Firewalls

- c.f., Host-Based Firewalls
  - https://www.howtogeek.com/122065/htg-explains-i-have-a-router-do-i-need-a-firewall/ (Windows Firewall)
- Software-based solution runs on top of an operating system
- Must **harden** the operating system:
  - Ensure all patches are updated
  - Uninstall unneeded applications or utilities
  - Close unused ports
  - Turn off all unused services
- Cheap solution **Q:** What are the trade-offs (vs commercial-grade firewalls)?

In Practice: Demilitarized Zone (DMZ)

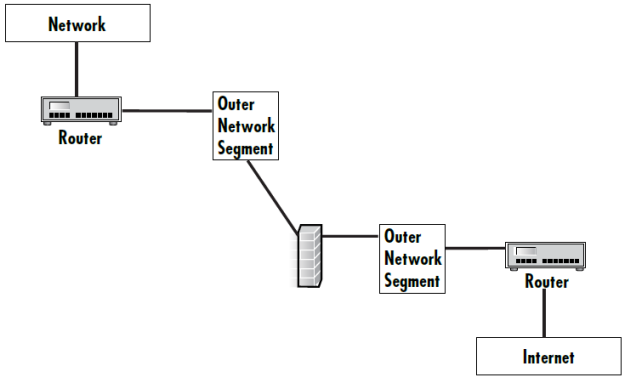


- Two separate firewalls
- One faces the outside world
- One faces the inside
- Web, email, and FTP servers are located in the area in-between them


Outer Firewall
DMZ
Web Server
Inner Firewall

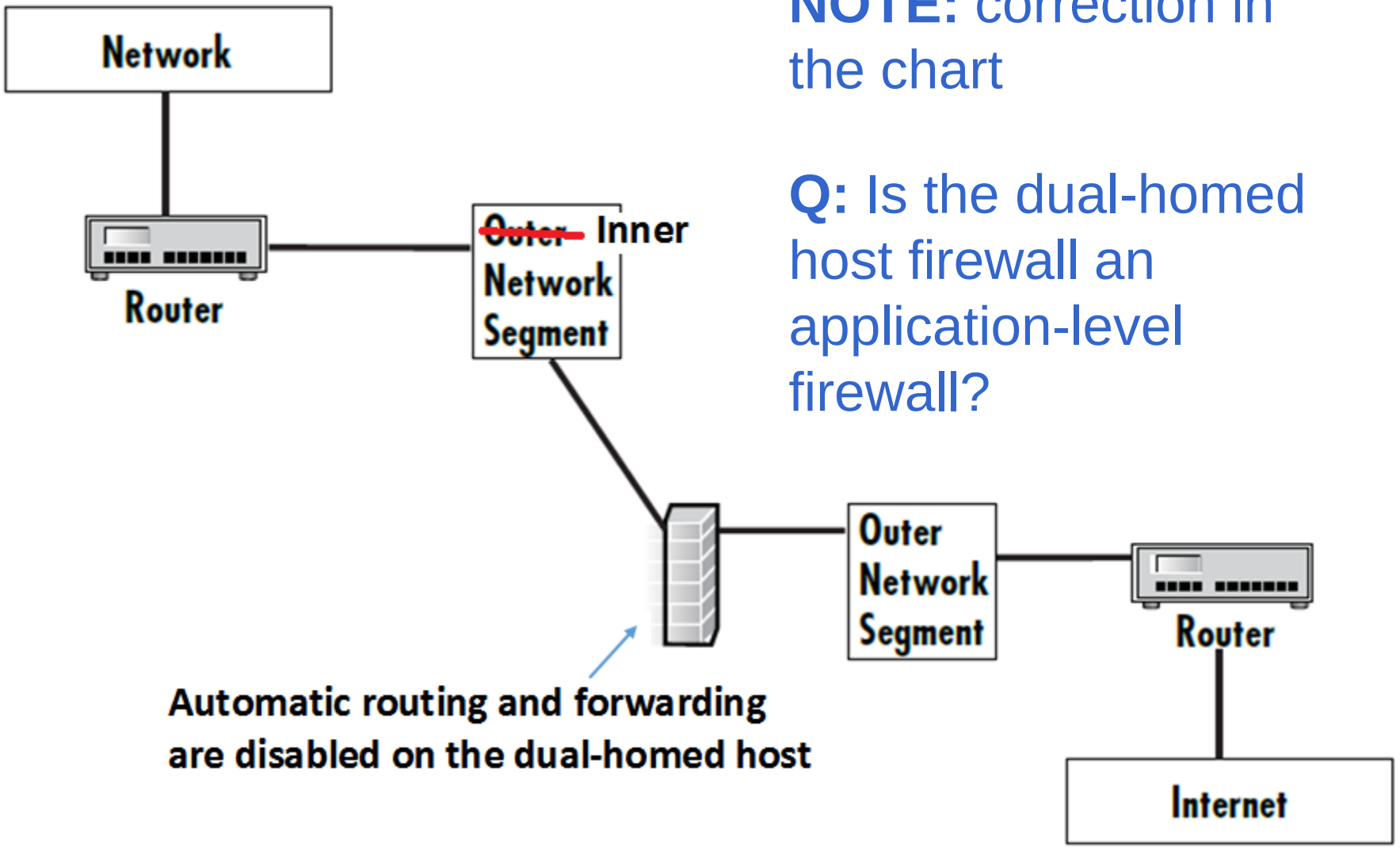
Dual-Homed Hosts

- Expanded version of the Network Host-based Firewall
- Also runs on top of the OS of a server
- An older technology
- Automatic routing is disabled on the host
- The **outer** and the **inner** networks cannot see each other; both talk to the dual-homed host



- Disadvantage, as with Network host firewalls, is its reliance on the security of the OS

Dual-Homed Hosts



NOTE: correction in the chart

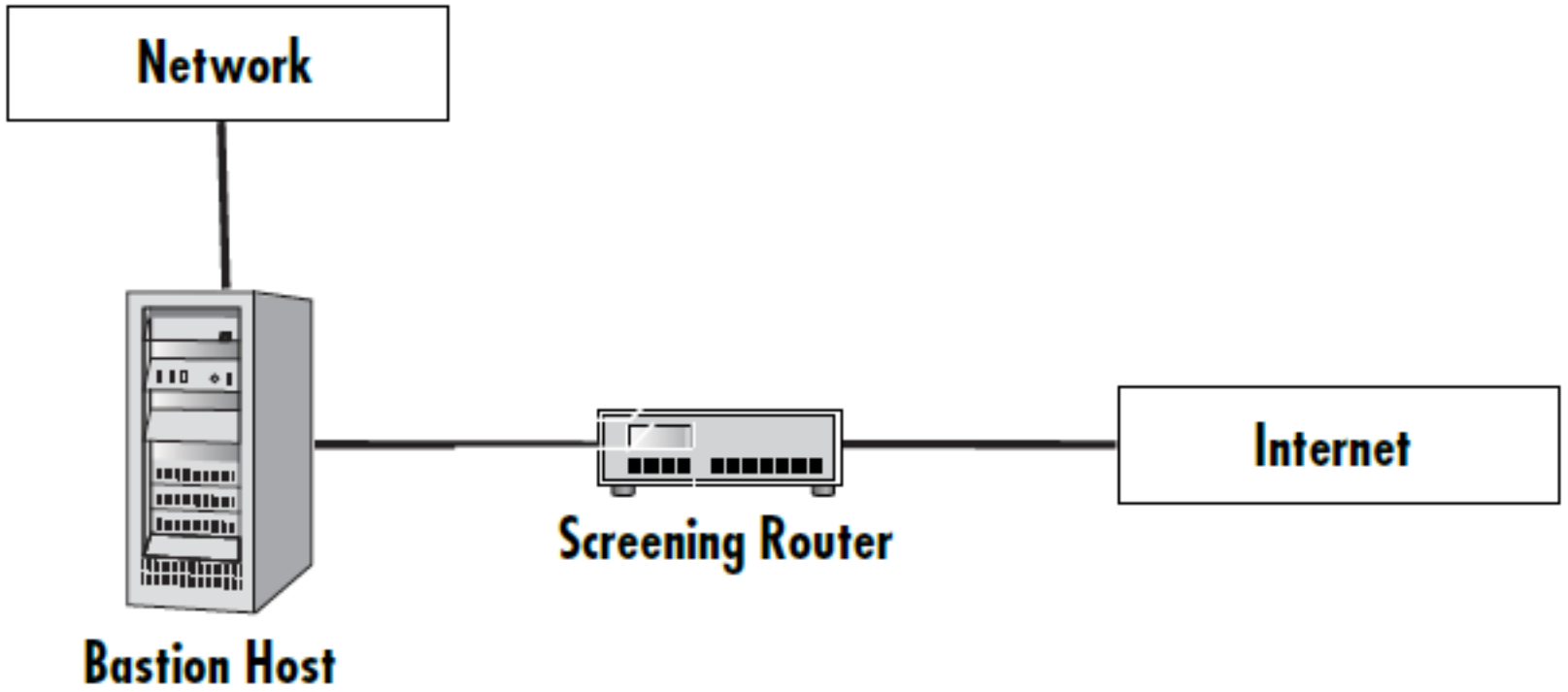
Q: Is the dual-homed host firewall an application-level firewall?

Router-Based Firewall

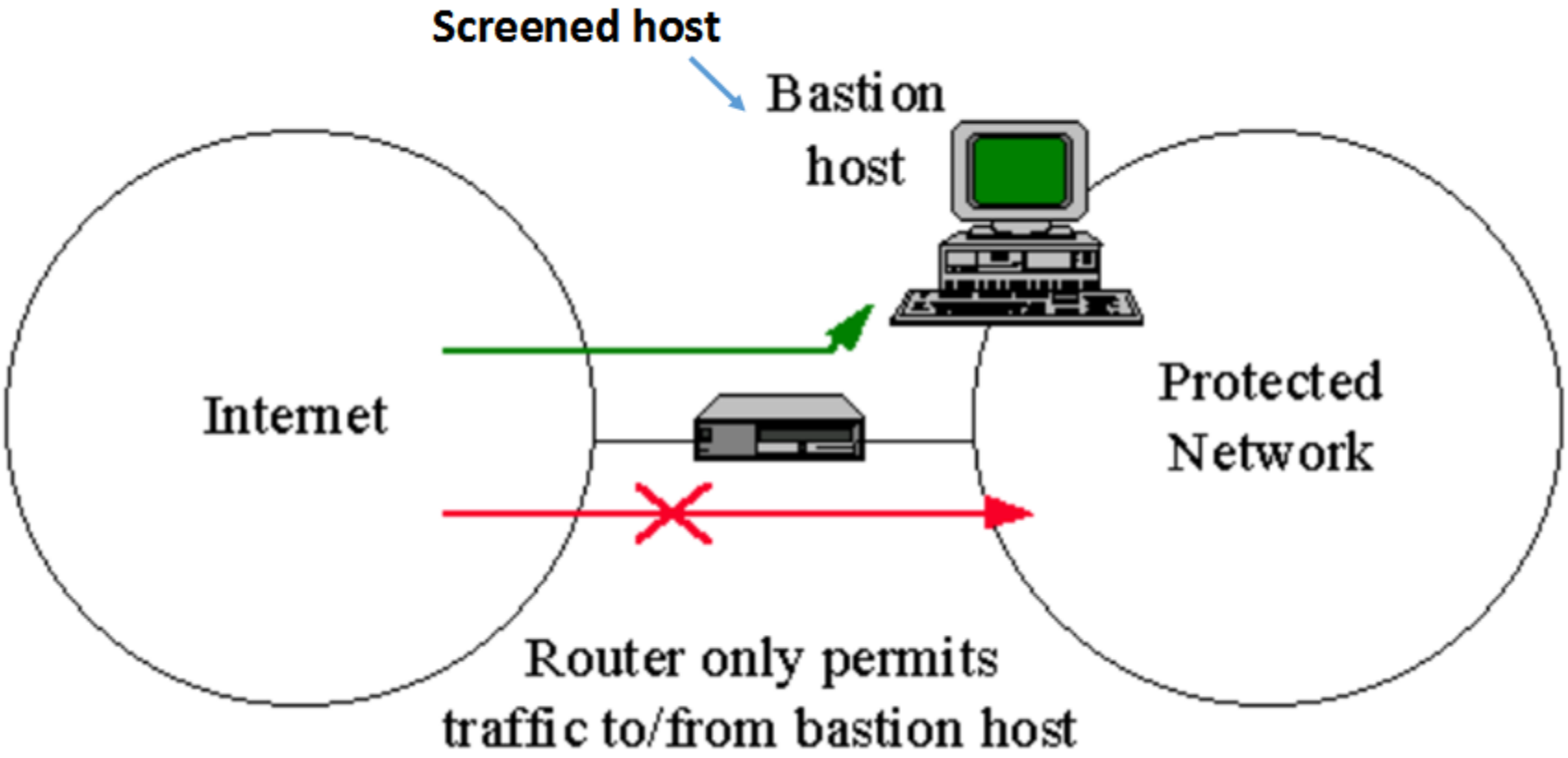
- Usually the first line of defense
- Uses simple packet filtering
- Ideal for novice administrators
- Can be preconfigured by vendor for specific needs of user
- Can be placed between segments of a network

Screened Host

- A combination of firewalls
- Bastion host and screening router is used
- Similar in concept to the dual-homed host (except for the use of a screening router)



screened host firewall



- The packet-filtering router allows only traffic destined to the bastion host.
- A network-level firewall

screened host firewall

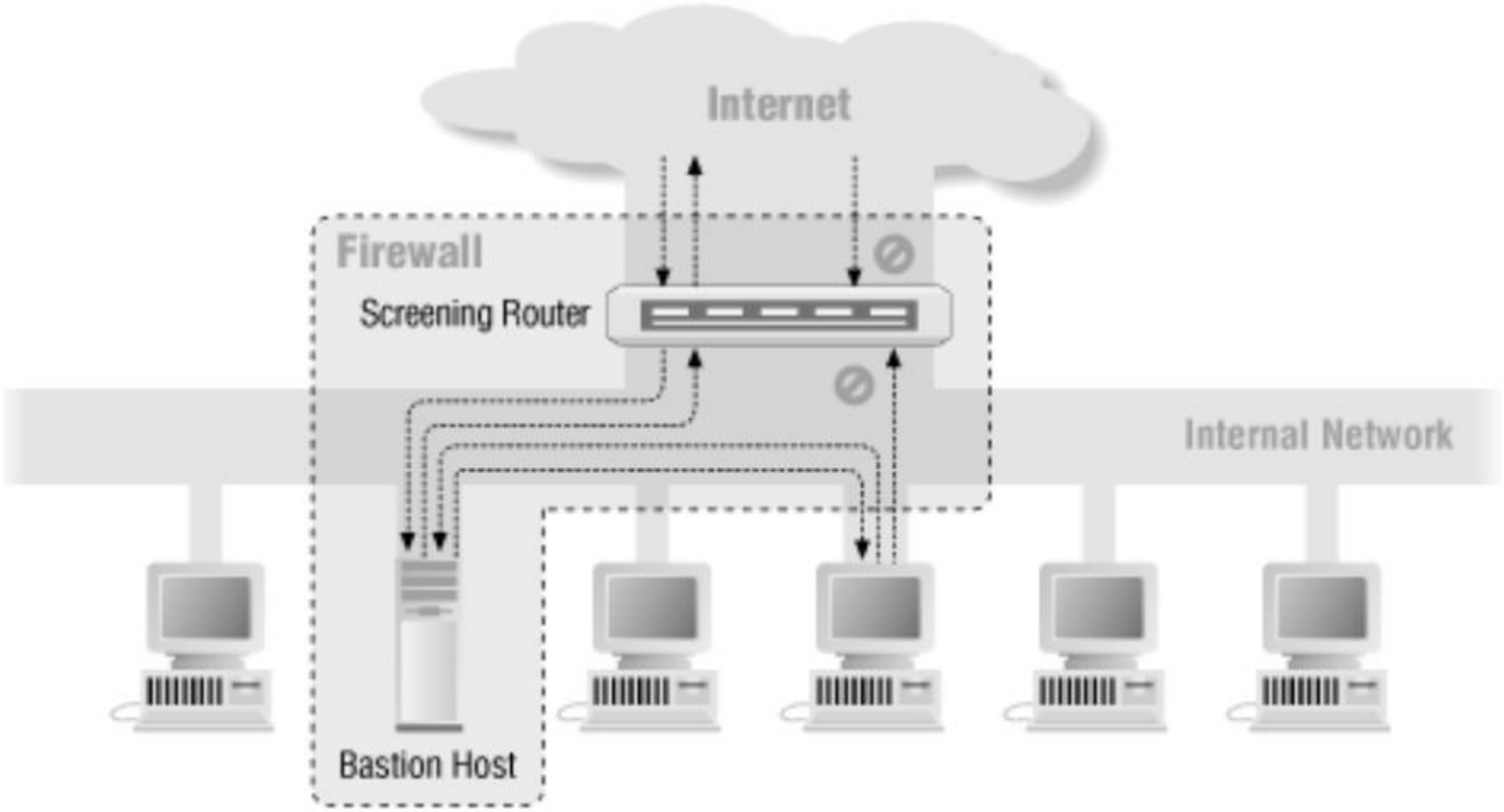


Figure 6-3. Screened host architecture

screened subnet firewall

- The single bastion host in the *screened host firewall* is expanded into a subnet of bastion hosts.
- The subnet is called *perimeter network, in which public servers (HTTP, FTP, etc) are hosted.*
- *If one of the hosts in the perimeter network is compromised, the hacker can only snoop on traffic transmitted over the subnet (but not traffic between hosts in the protected network).*
- *Communication within the protected network is therefore protected from* snooping.

Q: Is the *perimeter network* a DMZ?

screened subnet firewall

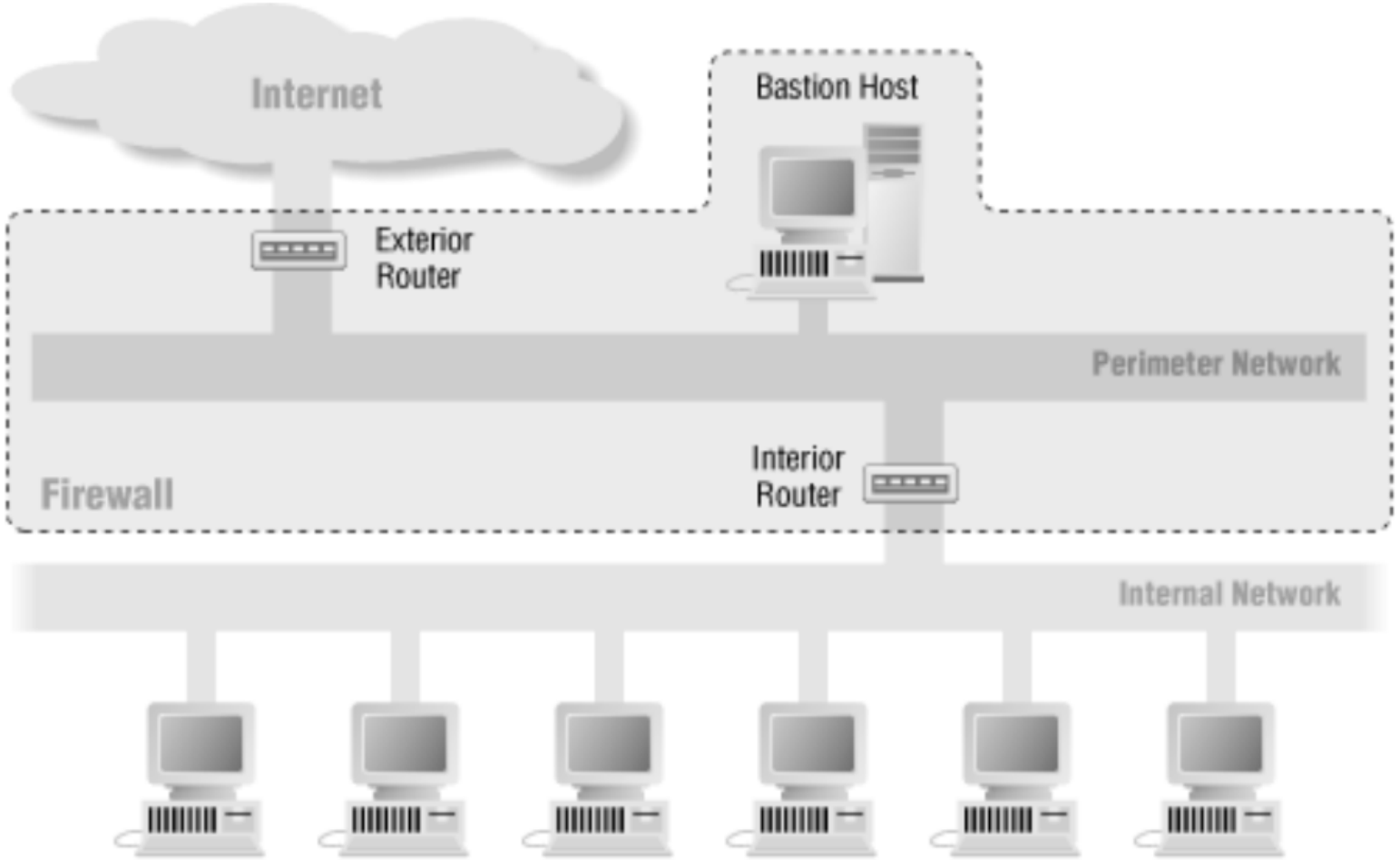
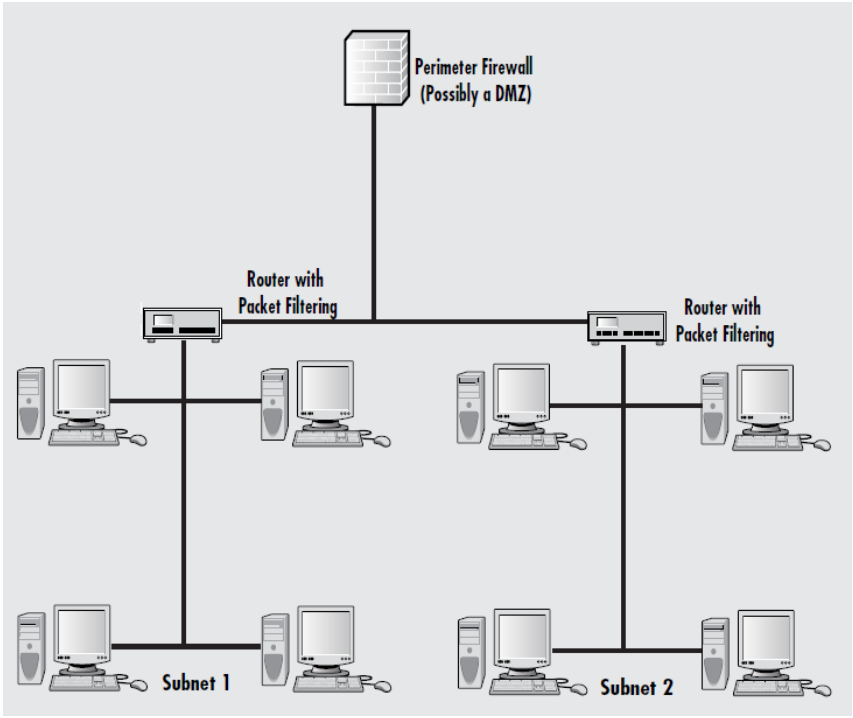


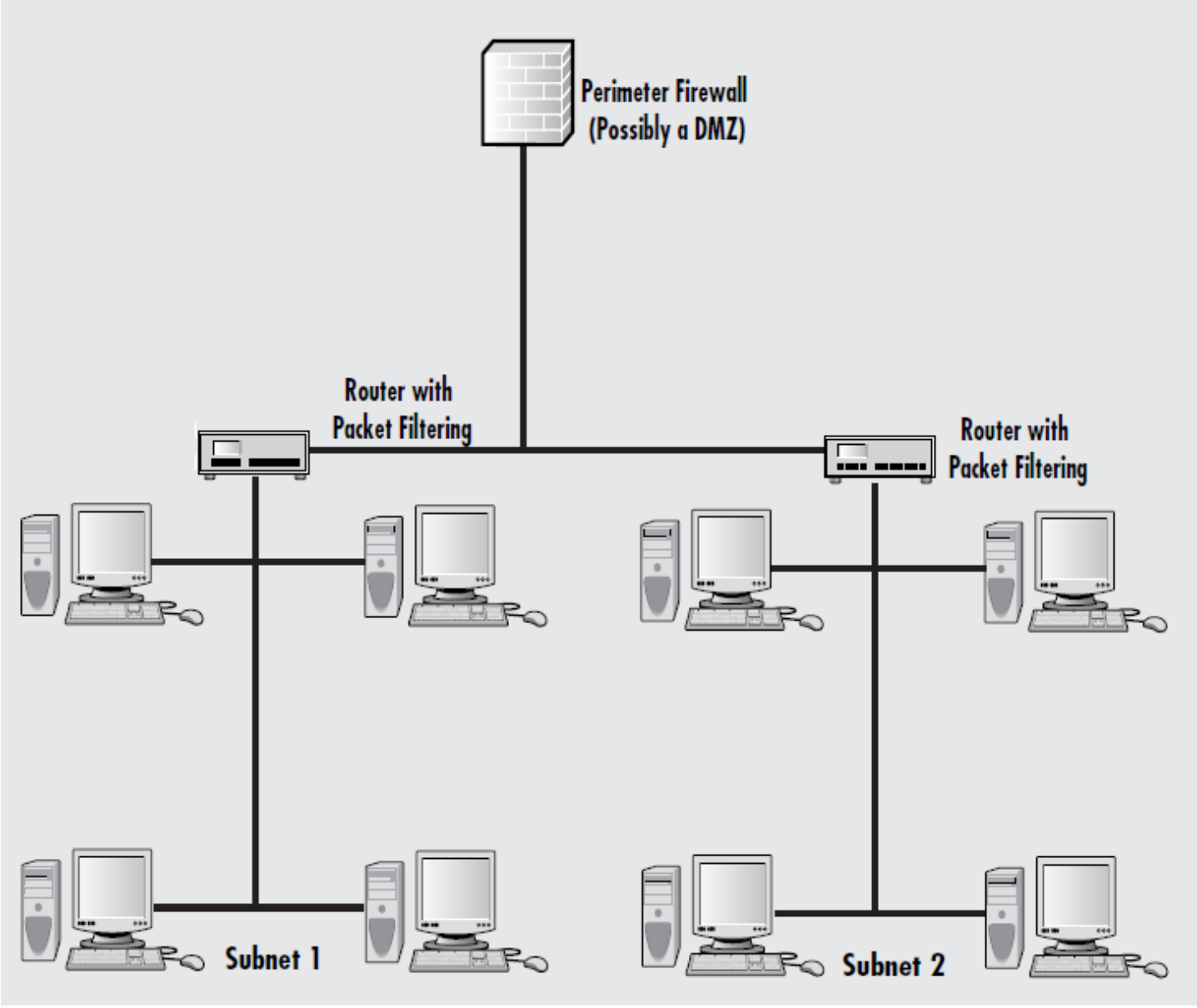
Figure 6-4. Screened subnet architecture (using two routers)

In Practice: Utmost Security

- Multiple firewalls
  - Stateful packet inspecting firewall
  - Application gateway
- Screened firewall routers separating each network segment
- Dual-perimeter firewall, packet screening on all routers, individual packet filtering firewalls on every server



In Practice: Utmost Security



Selecting and Using a Firewall

- Configure it properly
- Consider a consultant for initial setup
- Review logs periodically for anomalies
- Utilize statistics for baseline performance

Using Proxy Servers

- Prevent the outside world from gathering information about your internal network
- Provide valuable log information
- Can redirect certain traffic, based on configuration
- Typically runs on the firewall machine
- Protects against spoofing

Network Address Translation (NAT)

- Supersedes proxy servers
- Translates internal IP addresses to public addresses
- Can explicitly map ports to internal addresses for web servers

Summary

- Firewalls and proxy servers are critical for network security solutions
- Many solutions are available, which vary in price and features
- Choose the most secure solution that the budget allows

Summary

- Types of Firewalls
  - Packet filter
  - Stateful packet inspection
  - Circuit level gateway
  - Application gateway
- Types of Implementations
  - Host-based
  - Network host-based
  - Router-based
  - Dual-homed, screened host, screened subnet