# Computer Security: Principles and Practice

## Chapter 9 – Firewalls and Intrusion Prevention Systems

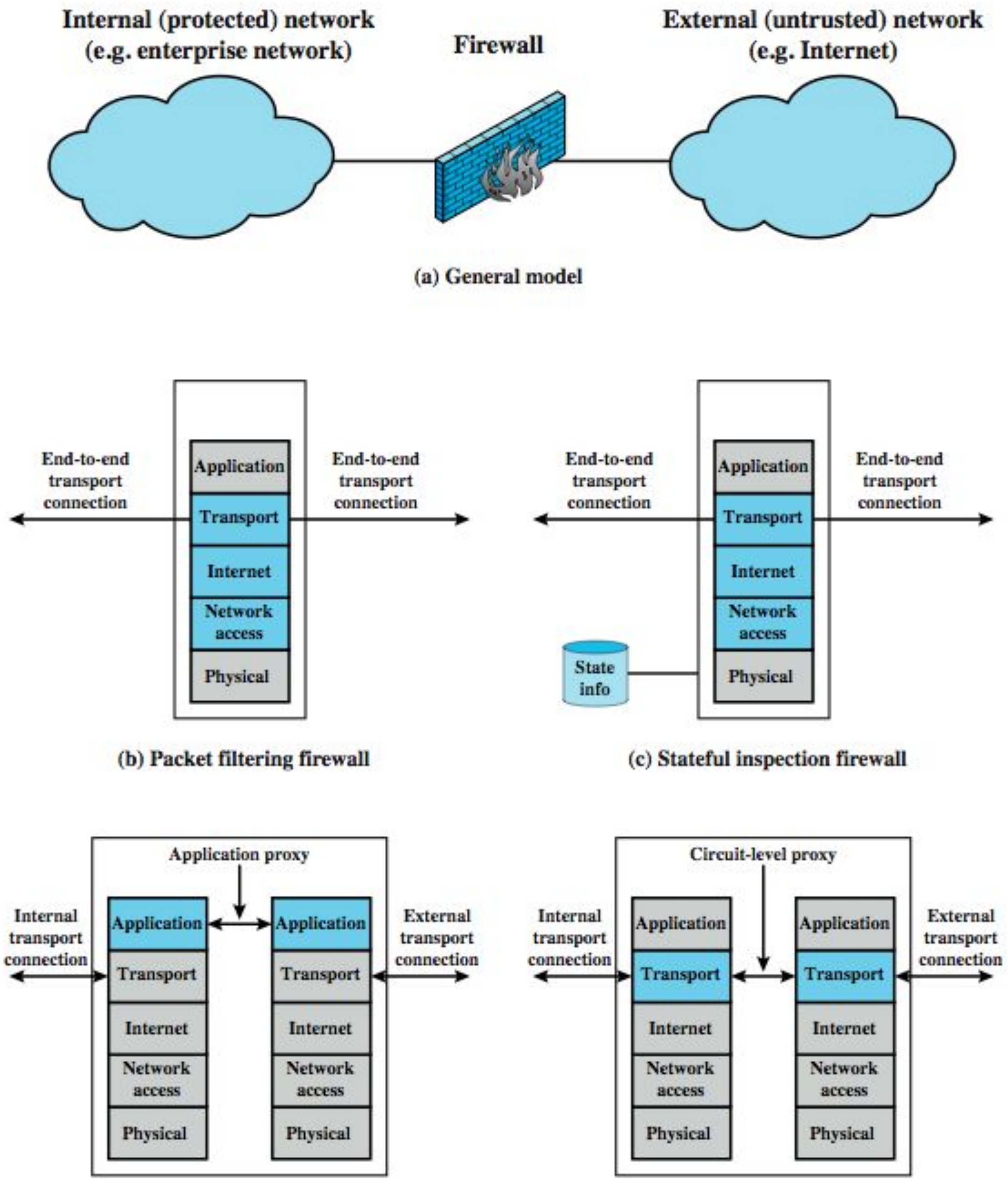
# Firewalls and Intrusion Prevention Systems

- effective means of protecting LANs
  - **Protects** from outside
  - **Allows** connection with outside
- internet connectivity essential
  - for organization and individuals
  - but creates a threat
- use firewall as perimeter defence
  - single choke point to impose security

# Firewall Capabilities & Limits

- capabilities:
  - defines a single choke point
  - provides a location for monitoring security events
  - convenient platform for some Internet functions such as NAT, usage monitoring, IPSEC VPNs
- limitations:
  - cannot protect against attacks bypassing firewall
  - may not protect fully against internal threats
  - laptop, PDA, portable storage device infected outside then used inside

# Types of Firewalls


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)
End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info
Application proxy
Internal transport connection
External transport connection
Circuit-level proxy

(a) General model

(b) Packet filtering firewall

(c) Stateful inspection firewall

(d) Application proxy firewall

(e) Circuit-level proxy firewall

# Firewall Basing

- several options for locating firewall:
- bastion host
- individual host-based firewall
- personal firewall

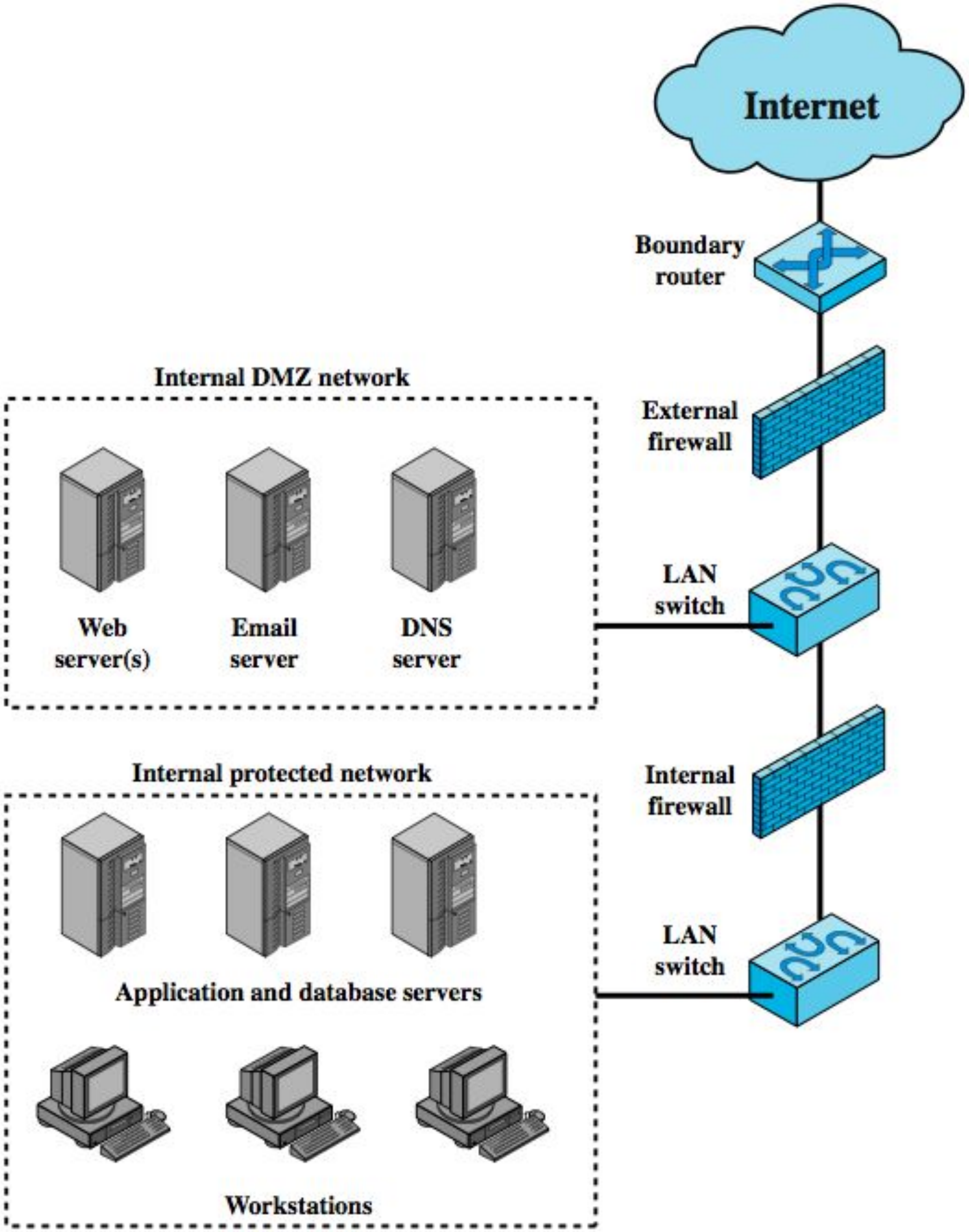
# Bastion Hosts

- critical strongpoint in network
- hosts application/circuit-level gateways
- common characteristics:
  - runs secure O/S, only essential services
  - may require user auth to access proxy or host
  - each proxy can restrict features, hosts accessed
  - each proxy small, simple, checked for security
  - each proxy is independent, non-privileged
  - limited disk use, hence read-only code

# Personal Firewall

- controls traffic flow to/from PC/workstation
- may be software module on PC
- or in home cable/DSL router/gateway
- typically much less complex
- primary role to deny unauthorized access
- may also monitor outgoing traffic to detect/block worm/malware activity

# Firewall Locations



# Intrusion Prevention Systems (IPS)

- recent addition to security products which
  - inline net/host-based IDS that can block traffic
  - functional addition to firewall that adds IDS capabilities
- can block traffic like a firewall
- using IDS algorithms
- may be network or host based

# Summary

- introduced need for & purpose of firewalls
- types of firewalls
  - packet filter, stateful inspection, application and circuit gateways
- firewall hosting, locations, topologies
- intrusion prevention systems