Computer Security DD2395

http://www.csc.kth.se/utbildning/kth/kurser/DD2395/dasak10/

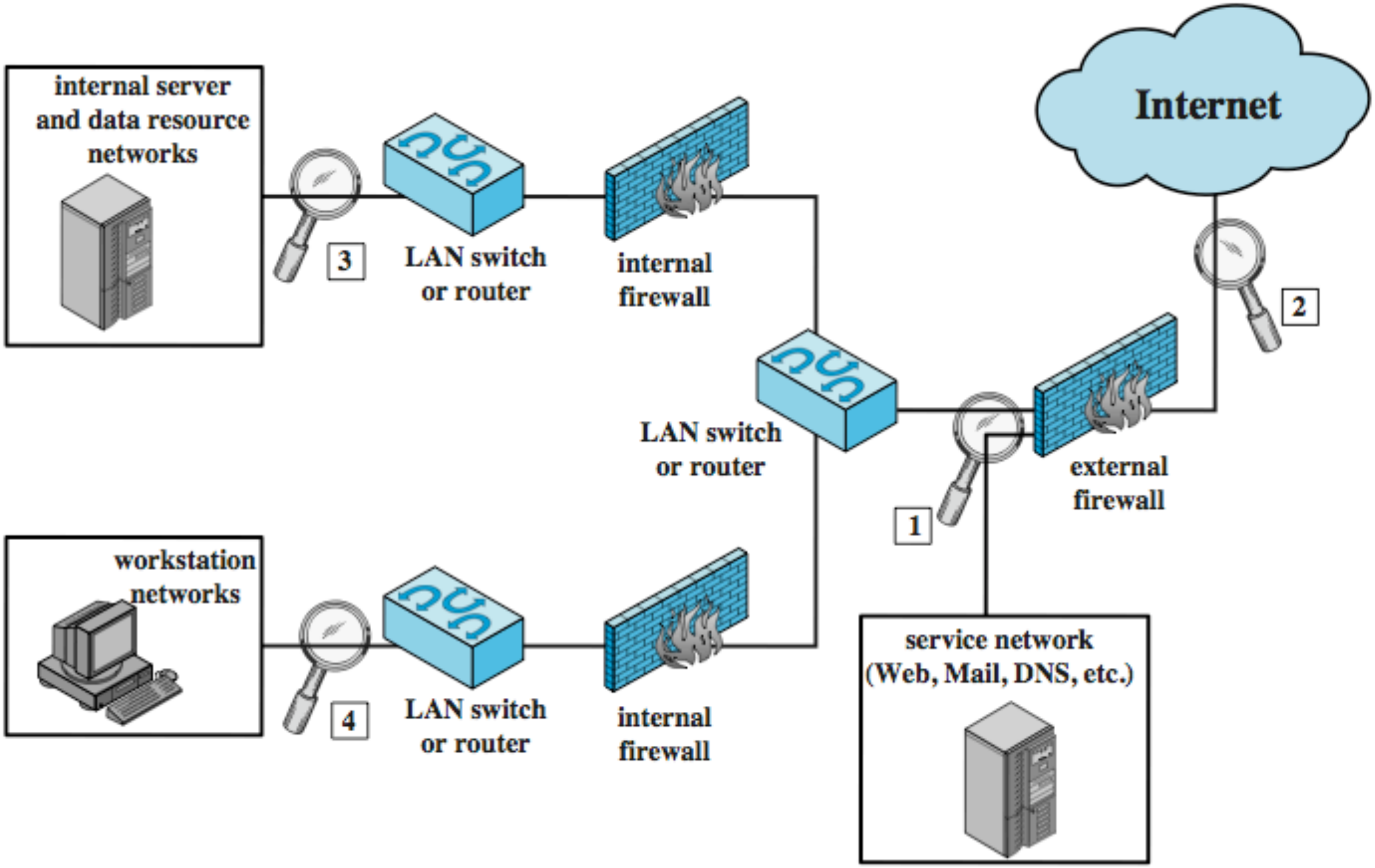
Spring 2010
Sonja Buchegger
buc@kth.se

Lecture 6, Feb. 3, 2010
Intrusion Detection, Prevention, Firewalls.

Network-Based IDS

- network-based IDS (NIDS)
  - monitor traffic at selected points on a network
  - in (near) real time to detect intrusion patterns
  - may examine network, transport and/or application level protocol activity directed toward systems
- comprises a number of sensors
  - inline (possibly as part of other net device)
  - passive (monitors copy of traffic)

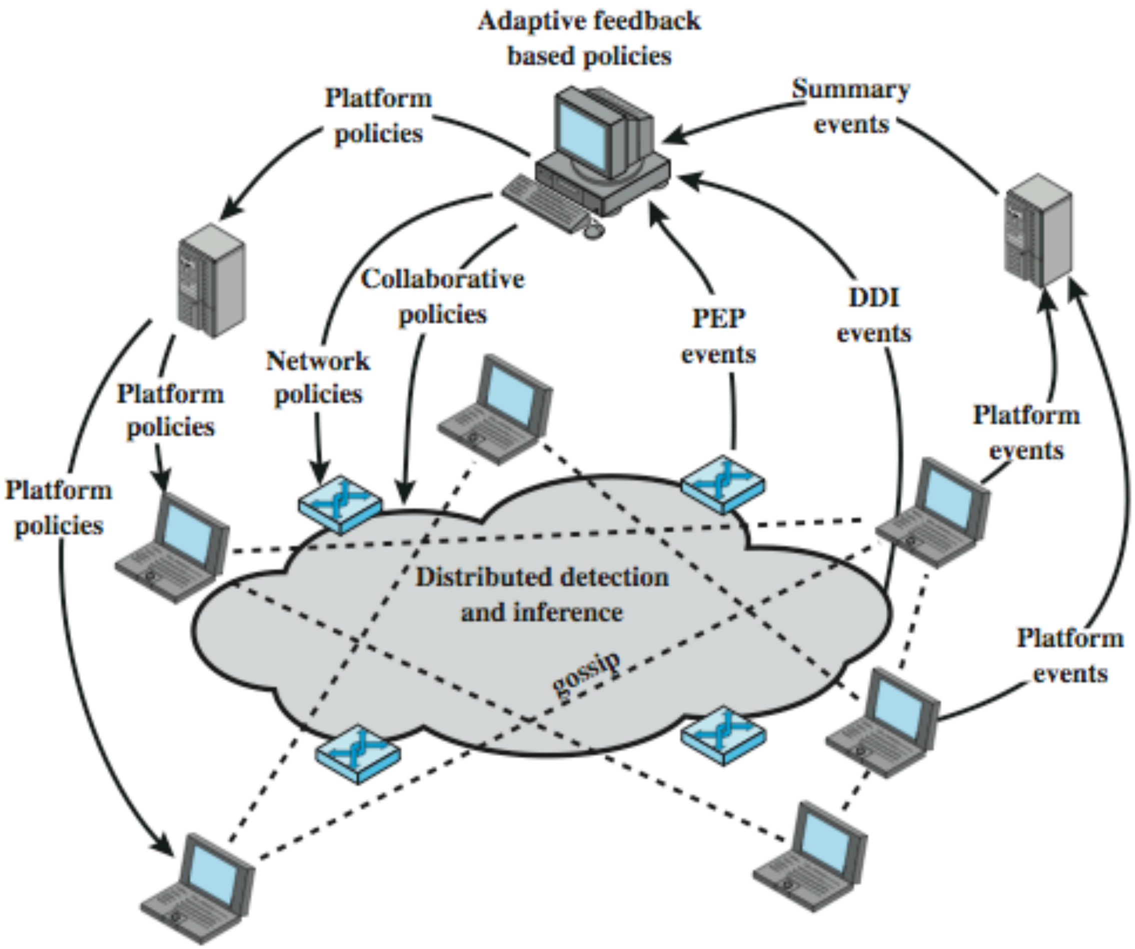
NIDS Sensor Deployment



Intrusion Detection Techniques

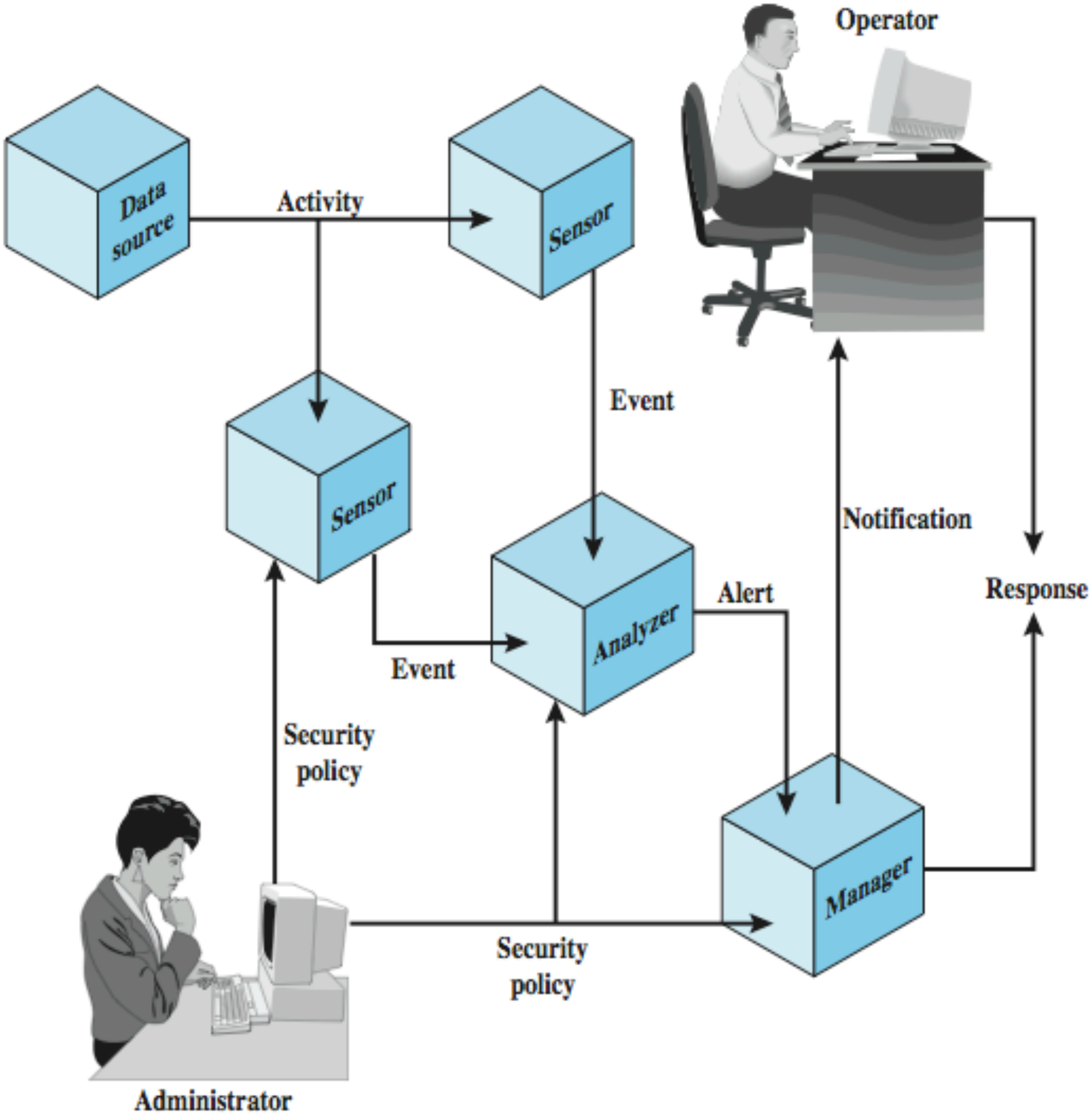
- signature detection
  - at application, transport, network layers; unexpected application services, policy violations
- anomaly detection
  - of denial of service attacks, scanning, worms
- when potential violation detected sensor sends an alert and logs information
  - used by analysis module to refine intrusion detection parameters and algorithms
  - by security admin to improve protection

Distributed Adaptive Intrusion Detection



PEP = policy enforcement point
DDI = distributed detection and inference

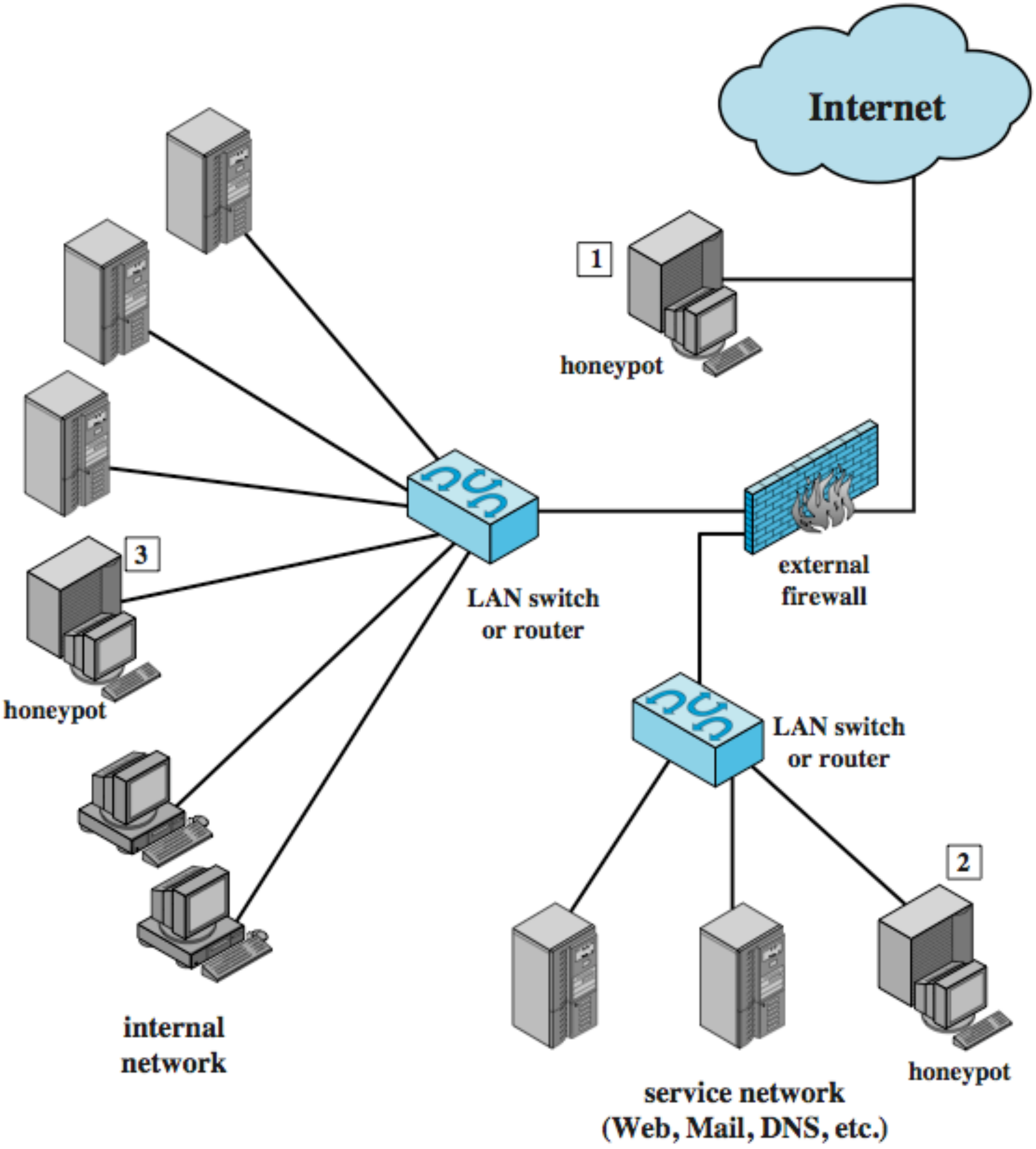
Intrusion Detection Exchange Format



Honeypots

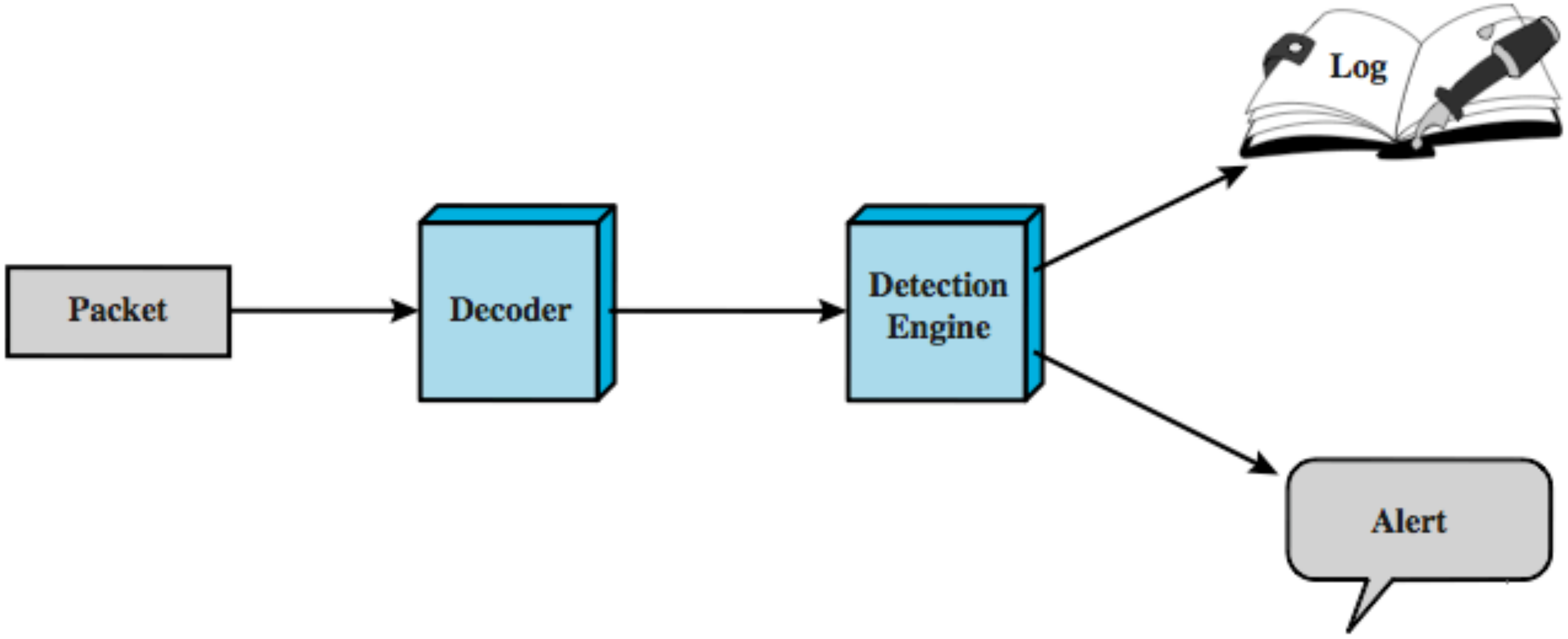
- are decoy systems
  - filled with fabricated info
  - instrumented with monitors / event loggers
  - divert and hold attacker to collect activity info
  - without exposing production systems
- initially were single systems
- more recently are/emulate entire networks

Honeypot Deployment



SNORT

- lightweight IDS
  - real-time packet capture and rule analysis
  - passive or inline



SNORT Rules

- use a simple, flexible rule definition language
- with fixed header and zero or more options
- header includes: action, protocol, source IP, source port, direction, dest IP, dest port
- many options
- example rule to detect TCP SYN-FIN attack:

```
Alert tcp $EXTERNAL_NET any -> $HOME_NET any \
(msg: "SCAN SYN FIN"; flags: SF, 12; \
reference: arachnids, 198; classtype: attempted-recon;)↰
```

Summary

- introduced intruders & intrusion detection
  - hackers, criminals, insiders
- intrusion detection approaches
  - host-based (single and distributed)
  - network
  - distributed adaptive
  - exchange format
- honeypots
- SNORT example

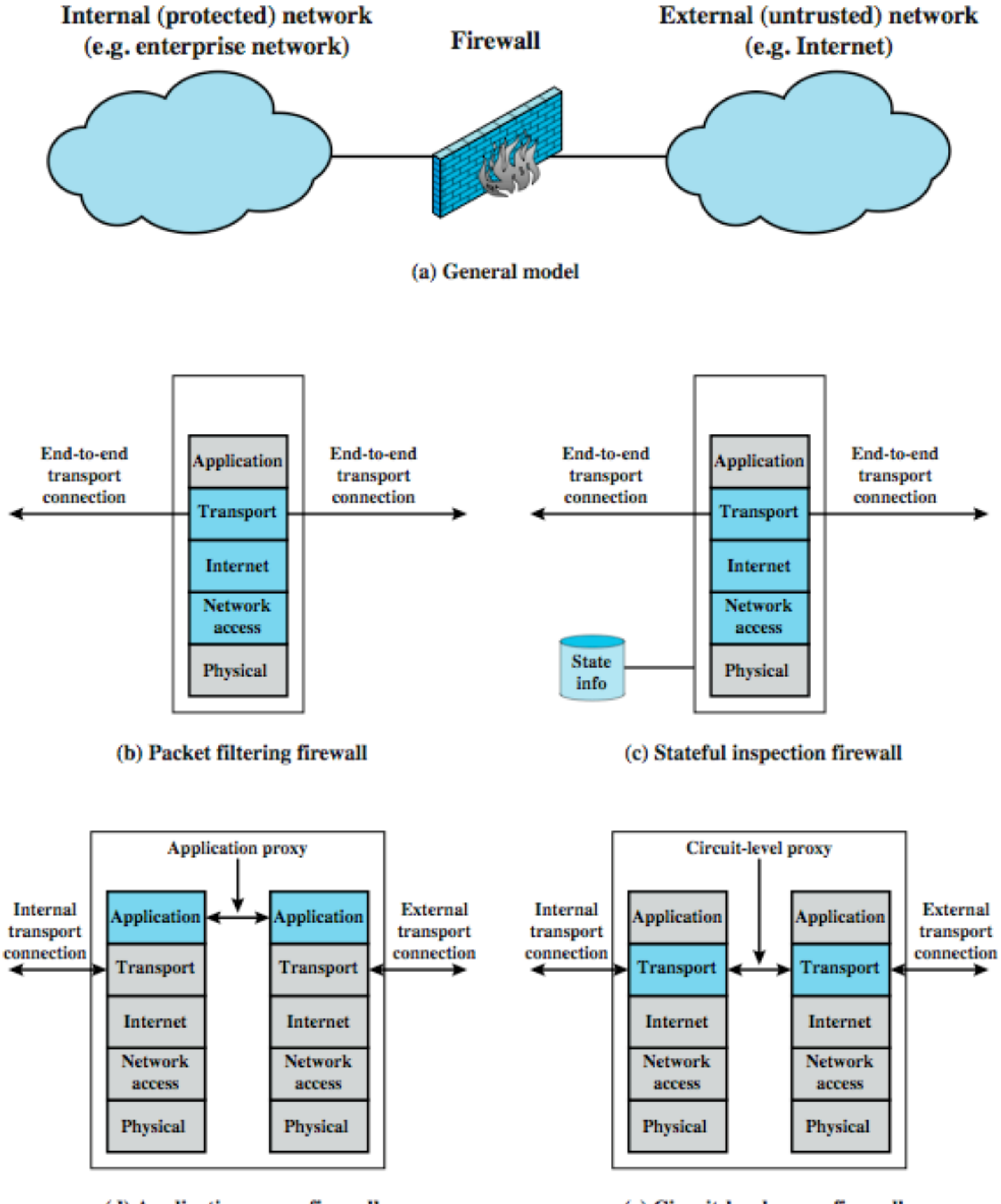
Firewalls and Intrusion Prevention Systems

- effective means of protecting LANs
- internet connectivity essential
  - for organization and individuals
  - but creates a threat
- could secure workstations and servers
- also 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
  - improperly secure wireless LAN
  - laptop, PDA, portable storage device infected outside then used inside

Types of Firewalls



(a) General model

(b) Packet filtering firewall

(c) Stateful inspection firewall

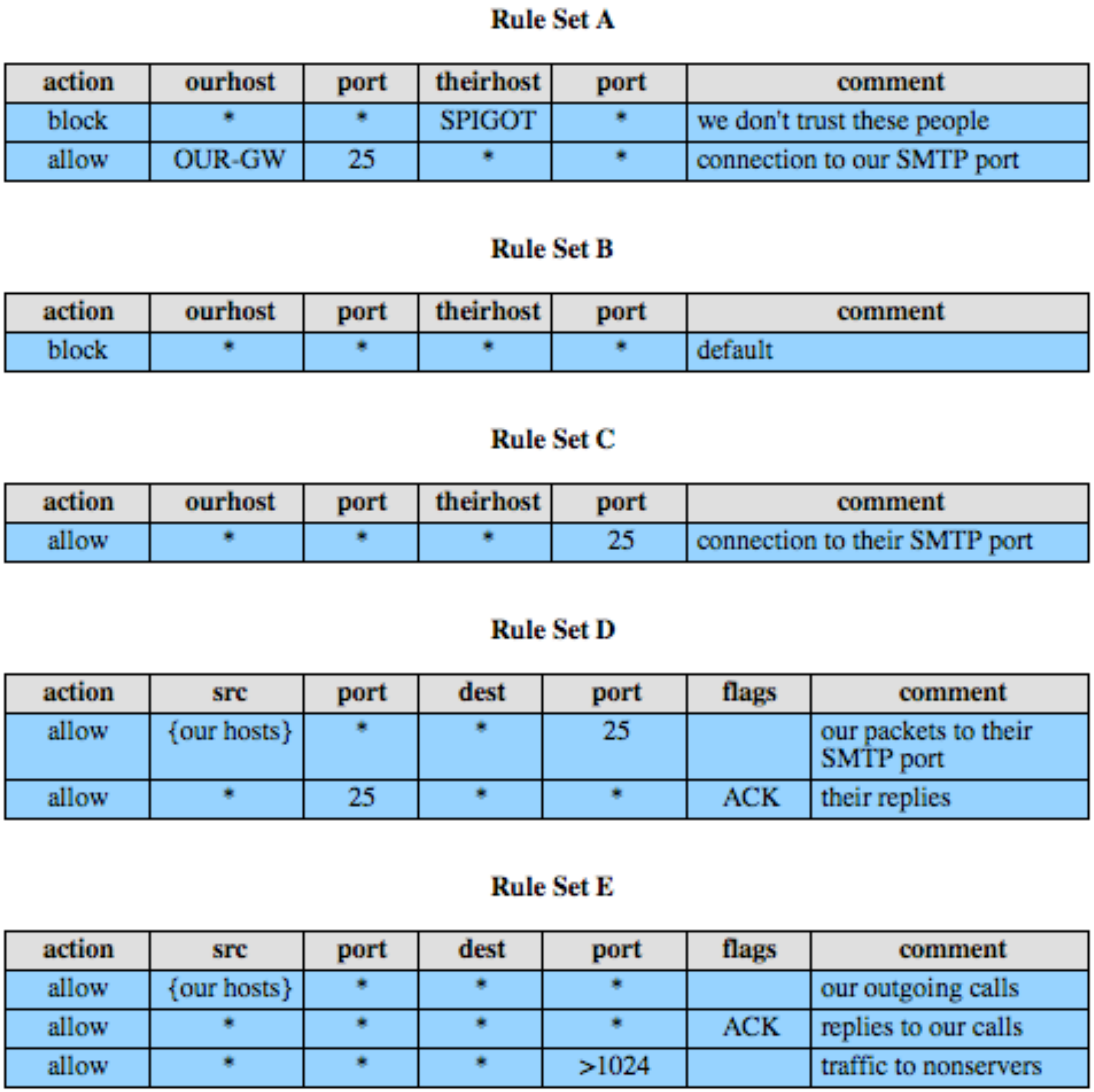
(d) Application proxy firewall

(e) Circuit-level proxy firewall

Packet Filtering Firewall

- applies rules to packets in/out of firewall
- based on information in packet header
  - src/dest IP addr & port, IP protocol, interface
- typically a list of rules of matches on fields
  - if match rule says if forward or discard packet
- two default policies:
  - discard - prohibit unless expressly permitted
    - more conservative, controlled, visible to users
  - forward - permit unless expressly prohibited
    - easier to manage/use but less secure

Packet Filter Rules



Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Packet Filter Weaknesses

- weaknesses
  - cannot prevent attack on application bugs
  - limited logging functionality
  - do no support advanced user authentication
  - vulnerable to attacks on TCP/IP protocol bugs
  - improper configuration can lead to breaches
- attacks
  - IP address spoofing, source route attacks, tiny fragment attacks

Stateful Inspection Firewall

- reviews packet header information but also keeps info on TCP connections
  - typically have low, “known” port no for server
  - and high, dynamically assigned client port no
  - simple packet filter must allow all return high port numbered packets back in
  - stateful inspection packet firewall tightens rules for TCP traffic using a directory of TCP connections
  - only allow incoming traffic to high-numbered ports for packets matching an entry in this directory
  - may also track TCP seq numbers as well

Application-Level Gateway

- acts as a relay of application-level traffic
  - user contacts gateway with remote host name
  - authenticates themselves
  - gateway contacts application on remote host and relays TCP segments between server and user
- must have proxy code for each application
  - may restrict application features supported
- more secure than packet filters
- but have higher overheads

Circuit-Level Gateway

- sets up two TCP connections, to an inside user and to an outside host
- relays TCP segments from one connection to the other without examining contents
  - hence independent of application logic
  - just determines whether relay is permitted
- typically used when inside users trusted
  - may use application-level gateway inbound and circuit-level gateway outbound
  - hence lower overheads

SOCKS Circuit-Level Gateway

- SOCKS v5 defined as RFC1928 to allow TCP/UDP applications to use firewall
- components:
  - SOCKS server on firewall
  - SOCKS client library on all internal hosts
  - SOCKS-ified client applications
- client app contacts SOCKS server, authenticates, sends relay request
- server evaluates & establishes relay connection
- UDP handled with parallel TCP control channel

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

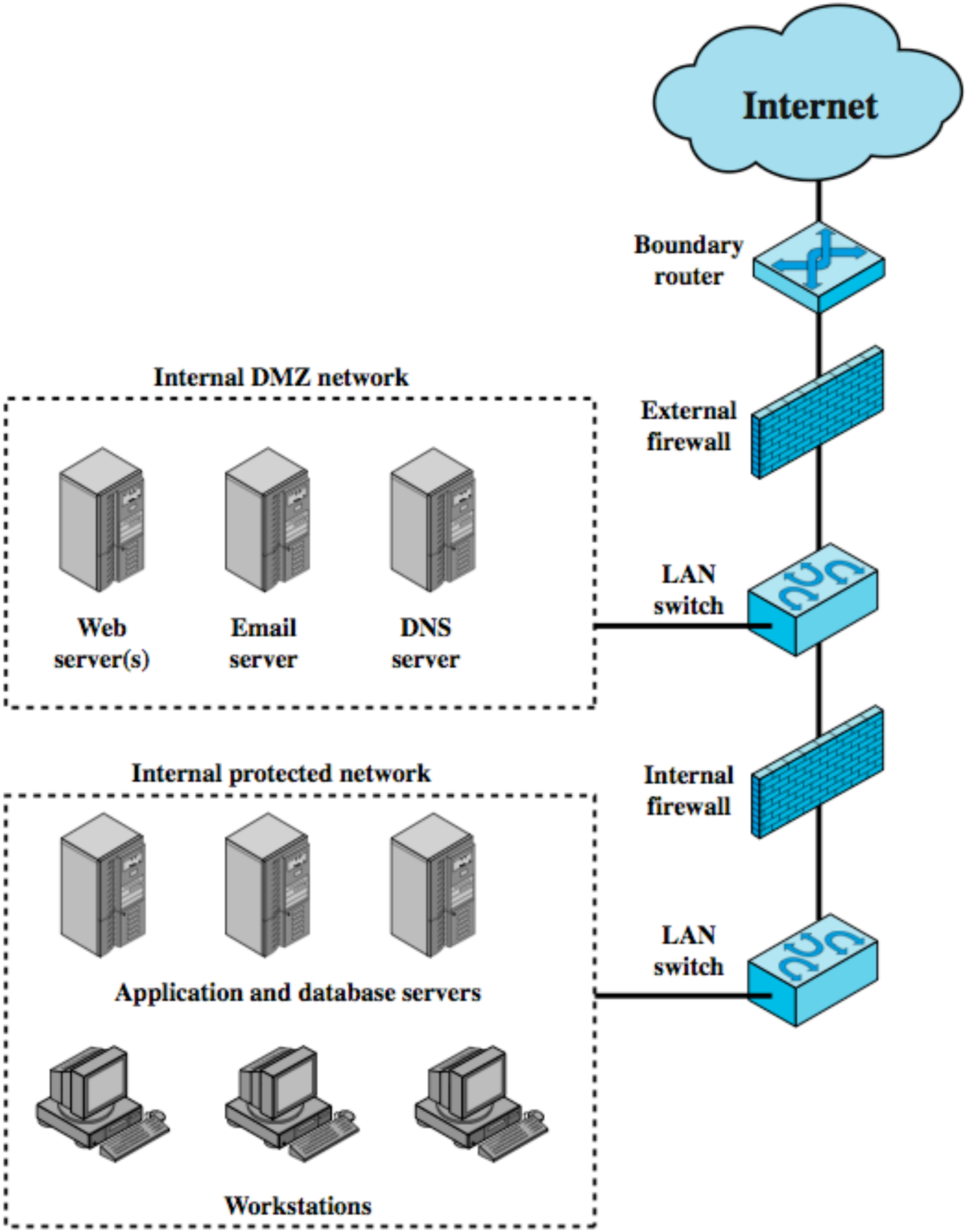
Host-Based Firewalls

- used to secure individual host
- available in/add-on for many O/S
- filter packet flows
- often used on servers
- advantages:
  - taylored filter rules for specific host needs
  - protection from both internal / external attacks
  - additional layer of protection to org firewall

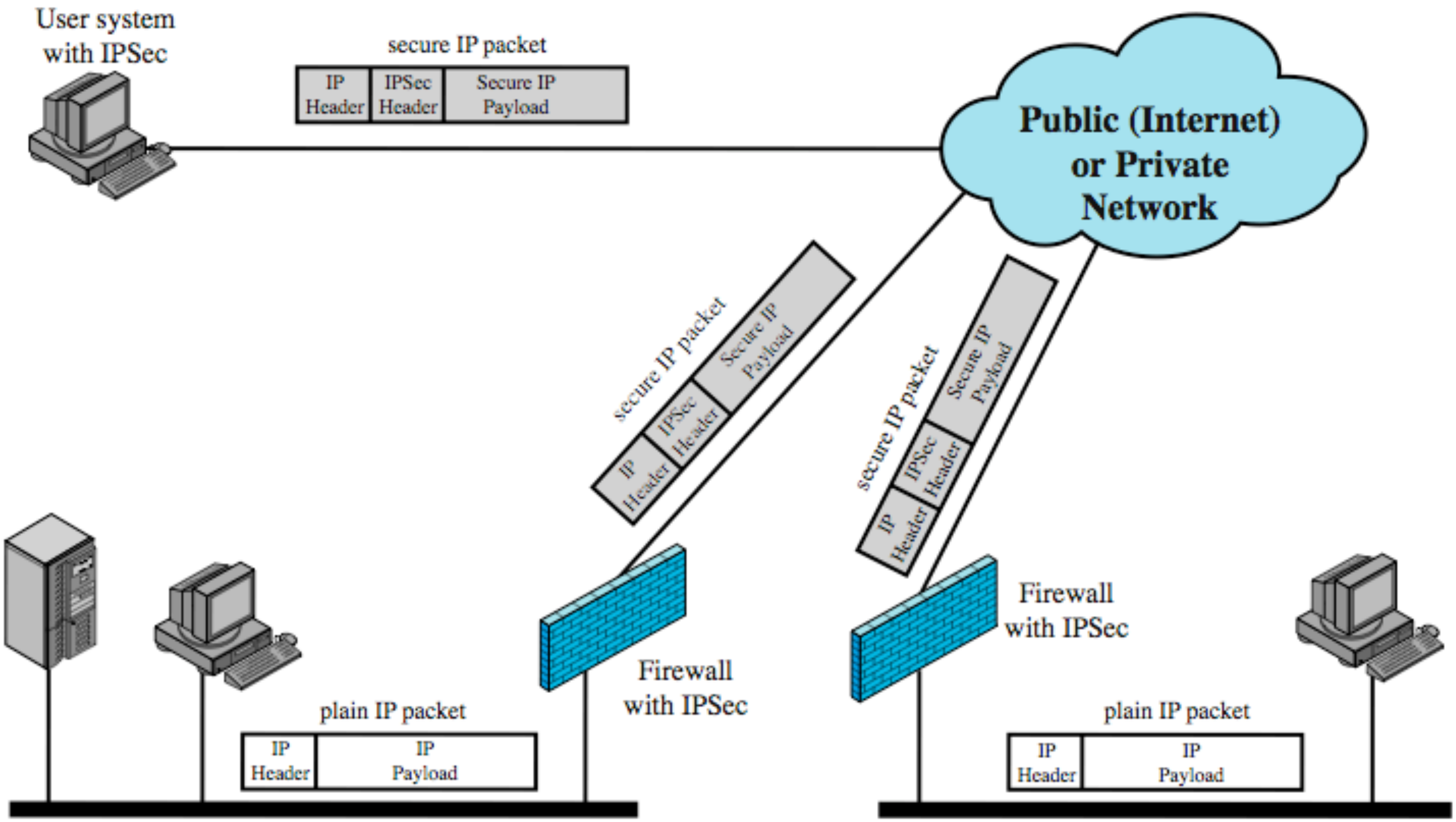
Personal Firewall

- controls traffic flow to/from PC/workstation
- for both home or corporate use
- 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

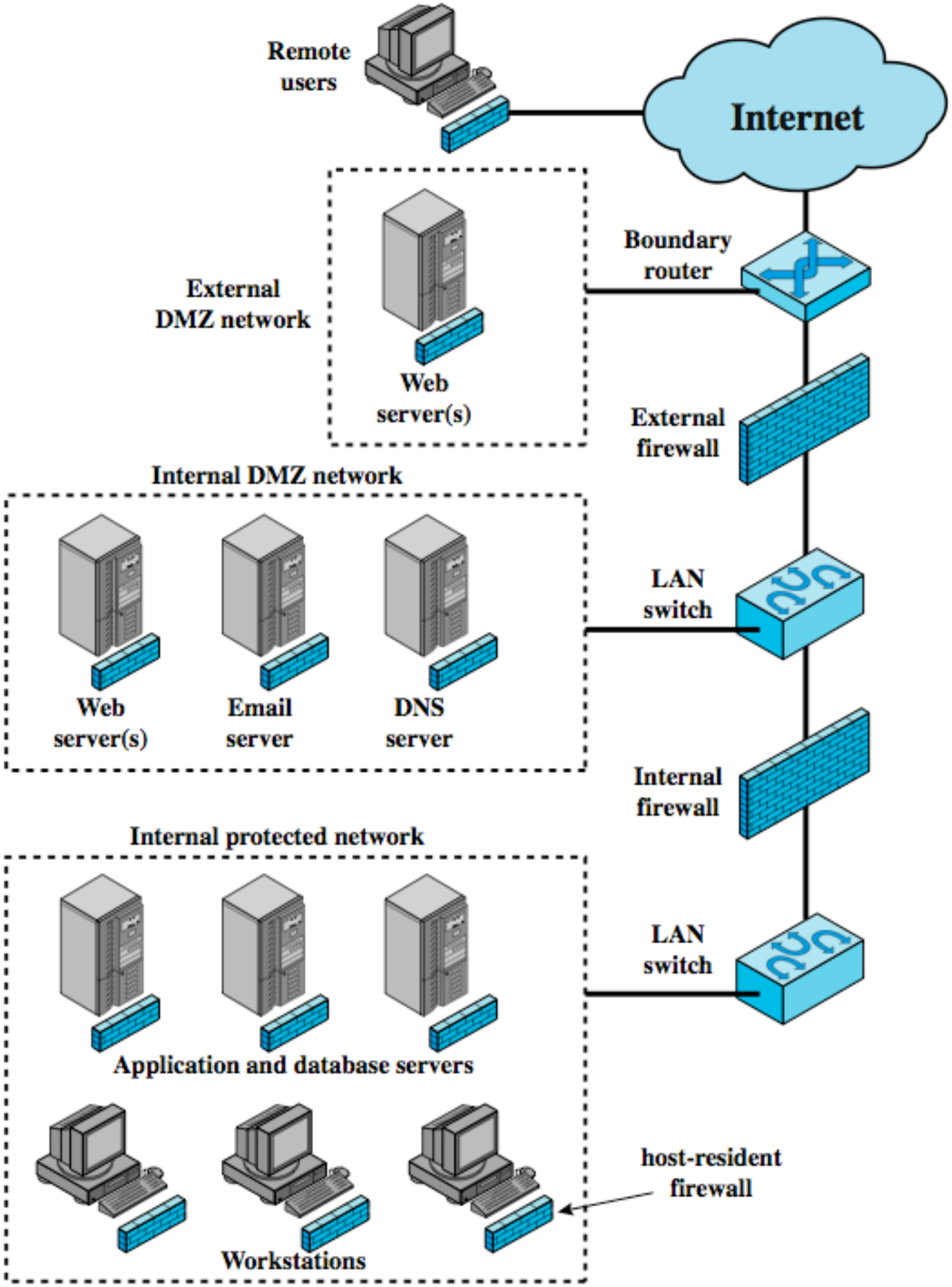
Firewall Locations



Virtual Private Networks



Distributed Firewalls



Firewall Topologies

- host-resident firewall
- screening router
- single bastion inline
- single bastion T
- double bastion inline
- double bastion T
- distributed firewall configuration

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

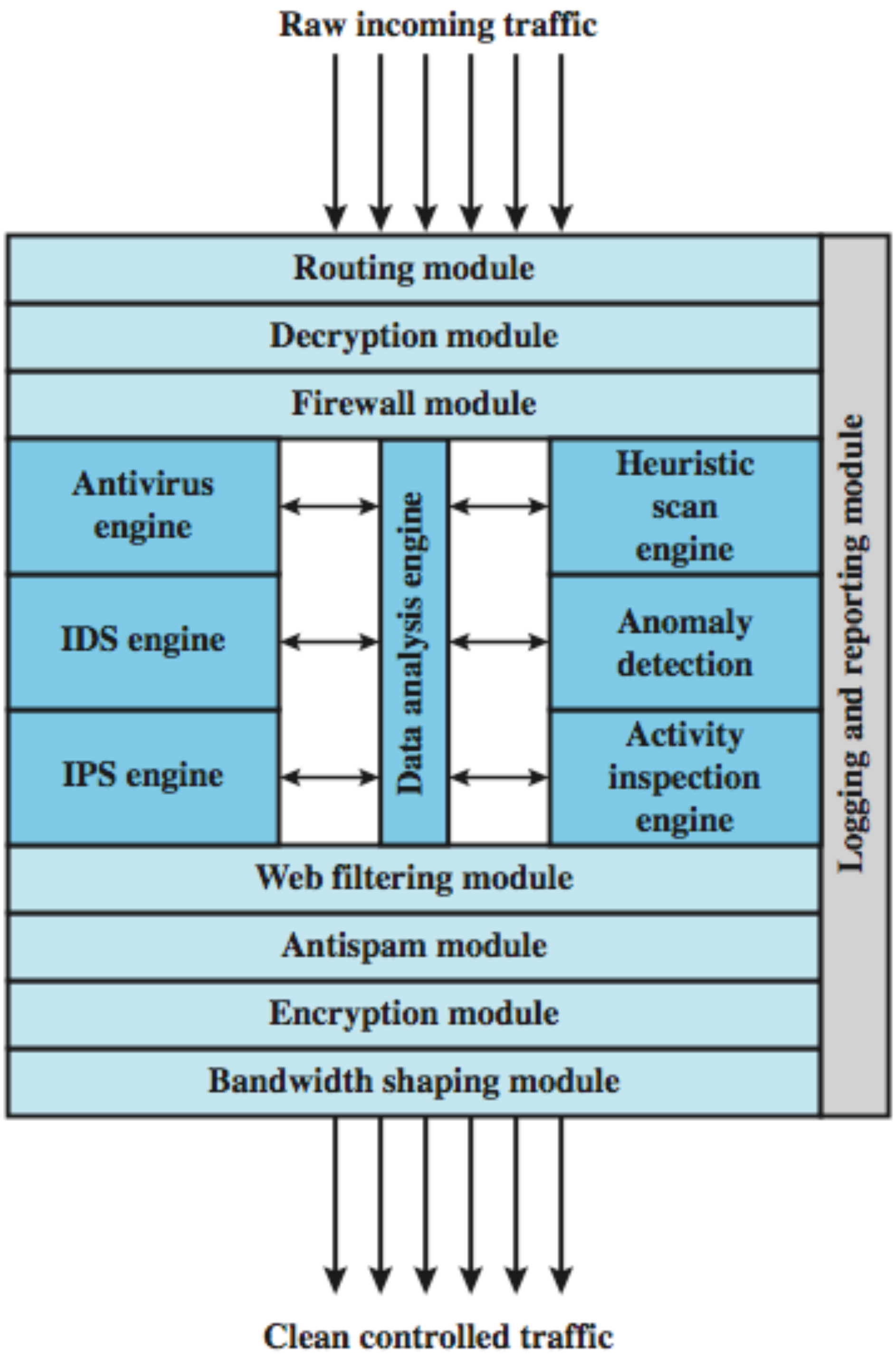
Host-Based IPS

- identifies attacks using both:
  - signature techniques
    - malicious application packets
  - anomaly detection techniques
    - behavior patterns that indicate malware
- can be tailored to the specific platform
  - e.g. general purpose, web/database server specific
- can also sandbox applets to monitor behavior
- may give desktop file, registry, I/O protection

Network-Based IPS

- inline NIDS that can discard packets or terminate TCP connections
- uses signature and anomaly detection
- may provide flow data protection
  - monitoring full application flow content
- can identify malicious packets using:
  - pattern matching, stateful matching, protocol anomaly, traffic anomaly, statistical anomaly
- cf. SNORT inline can drop/modify packets

Unified Threat Management Products



Raw incoming traffic

Routing module

Decryption module

Firewall module

Antivirus engine

IDS engine

IPS engine

Data analysis engine

Heuristic scan engine

Anomaly detection

Activity inspection engine

Web filtering module

Antispam module

Encryption module

Bandwidth shaping module

Logging and reporting module

Clean controlled traffic

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