CAN 304
Computer Systems Security

Lecture 10-11. Defenses: Intrusion Detection, Firewalls & Intrusion Prevention

Week 11: 2022-05-06, 14:00-16:00, Friday

Jie Zhang
Department of Communications and Networking
Email: jie.zhang01@xjtlu.edu.cn
Office: EE522

Review

- Cryptographic tools
- User authentication
- Access control

- Malware
- DoS attacks

Learning objectives

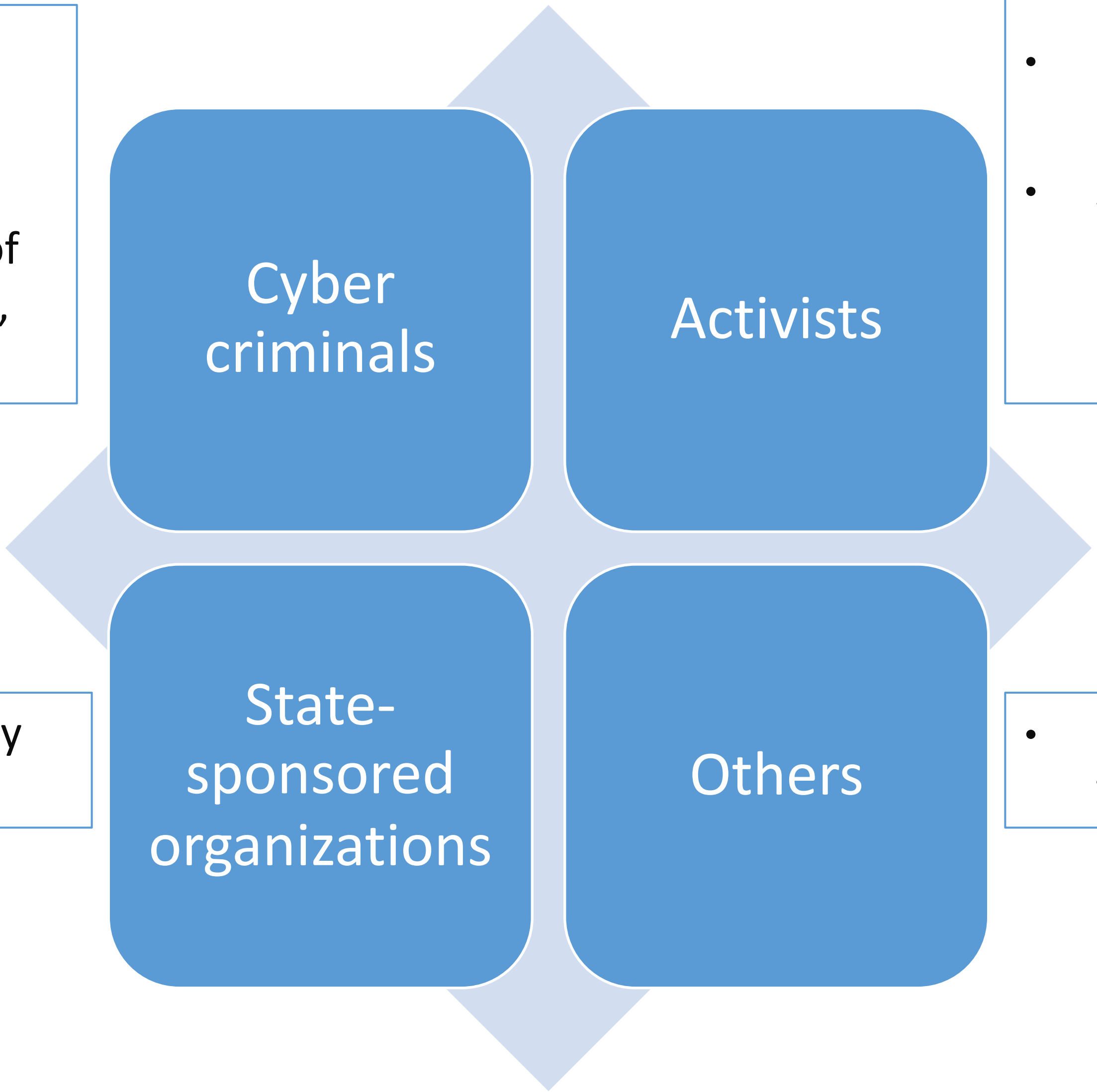
- Understand the basic principles of and requirements for intrusion detection.
- Understand anomaly and signature/heuristic approaches for intrusion detection.
- Discuss various types of firewall.

Outline

- Intrusion detection
- Firewalls & intrusion prevention

Part 1. Intrusion Detection

Classes of Intruders



Cyber criminals

- Individuals or members of an organized crime group
- Goal: financial reward
- Activities: identity theft, theft of financial credentials, data theft, or data ransoming

Activists

- Individuals (normally insiders), or members of a larger group of outsider attackers
- Motivated by social or political causes
- Activities: website defacement, Dos attacks, or the theft and distribution of data that results in negative publicity

State-sponsored organizations

- groups of hackers sponsored by governments

Others

- hackers with motivations other than those listed above

Intrusion Detection

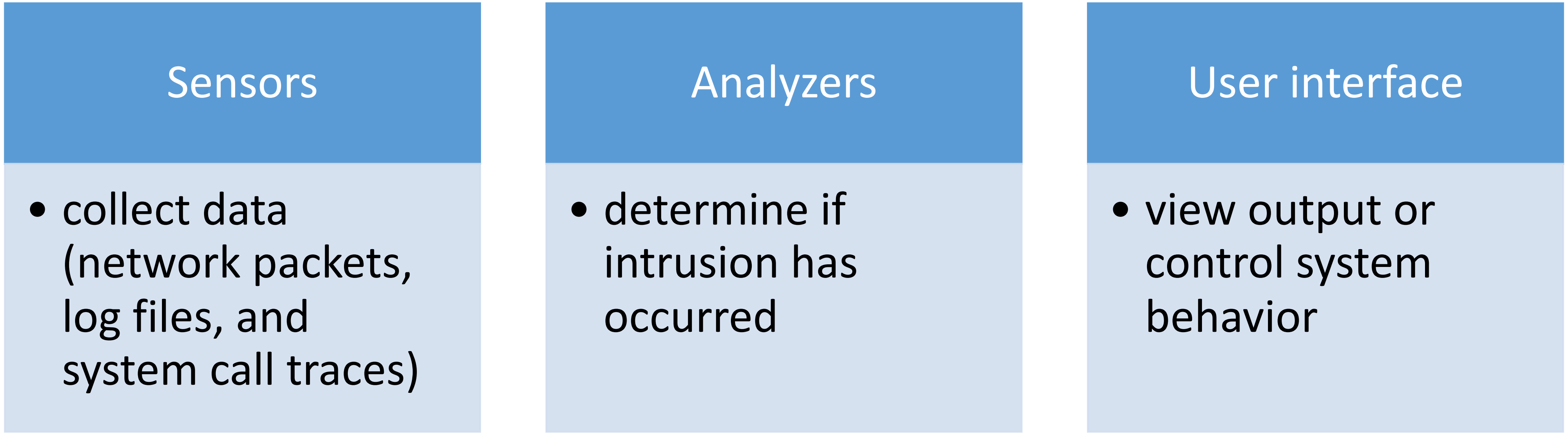
- Definitions from RFC 2828 (Internet Security Glossary)

- **Security Intrusion**: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

- **Intrusion Detection**: A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intrusion Detection System (IDS)

- An IDS comprises three logical components:



Sensors

- collect data (network packets, log files, and system call traces)

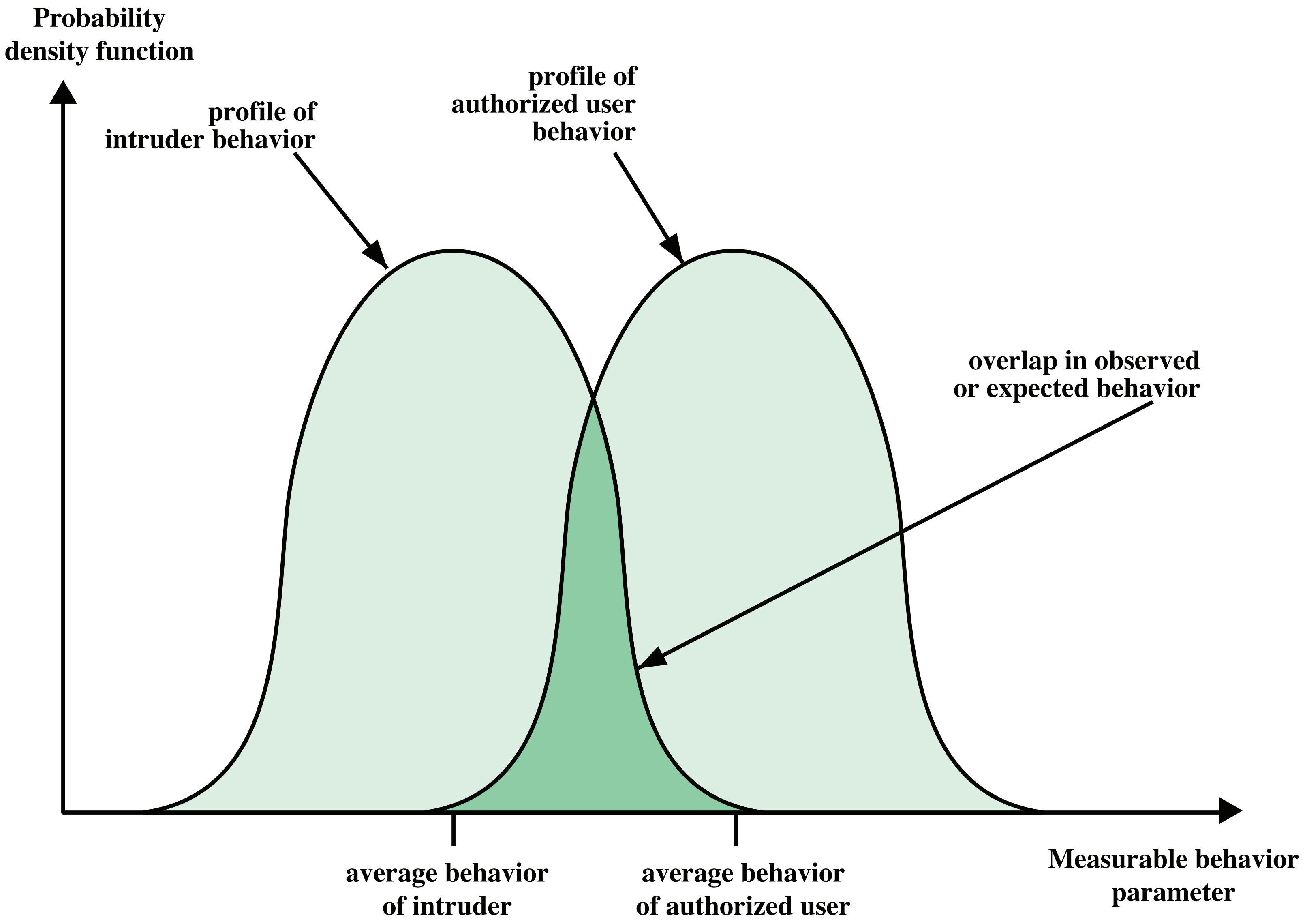
Analyzers

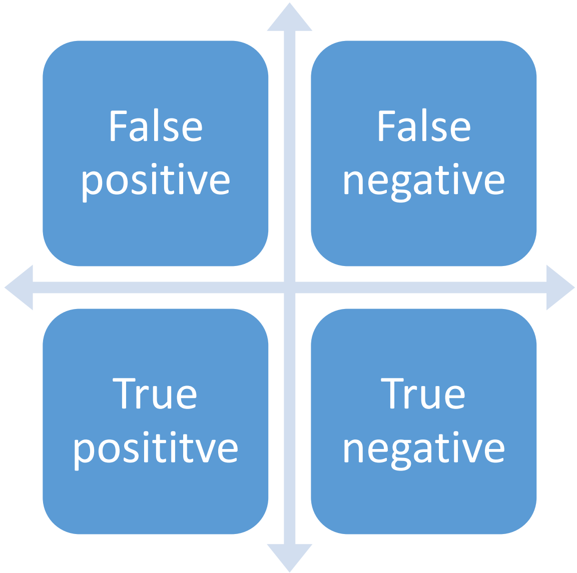
- determine if intrusion has occurred

User interface

- view output or control system behavior

Profiles of Behavior of Intruders and Authorized Users


Probability density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter



False positive	False negative
True posititve	True negative

IDS Requirements

- Run continually
- Be fault tolerant
- Resist subversion
- Impose a minimal overhead on a system
- Configured according to system security policies
- Adapt to changes in systems and users
- Scale to monitor large number of systems
- Provide graceful degradation of services
- Allow dynamic reconfiguration

Analysis Approaches

Anomaly detection

Model normal behavior

- Involves the collection of data relating to the behavior of legitimate users over a period of time
- Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

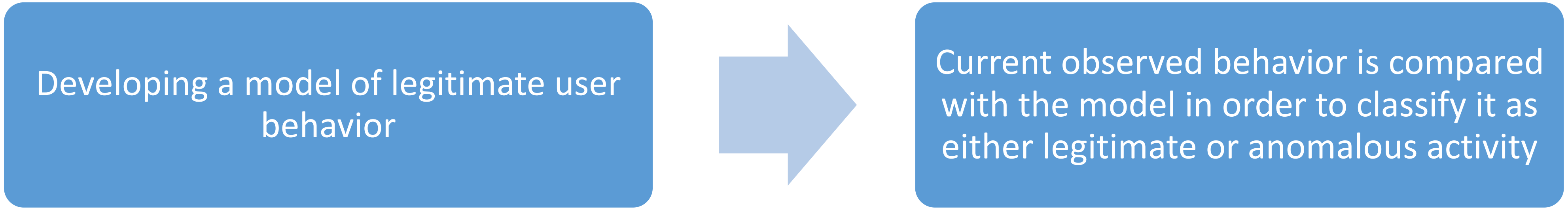
Signature/Heuristic detection

Model malicious pattern or behavior

- Uses a set of known malicious data patterns (signature) or attack rules (heuristics)
- Compares current behavior with the signatures or rules to decide if is that of an intruder
- Also known as misuse detection
- Can only identify known attacks for which it has patterns or rules

Anomaly Detection

- Two steps:



Developing a model of legitimate user behavior

Current observed behavior is compared with the model in order to classify it as either legitimate or anomalous activity

- A variety of classification approaches are used:

Statistical

- Analyze the observed behavior using univariate, multivariate, or time-series models of observed metrics

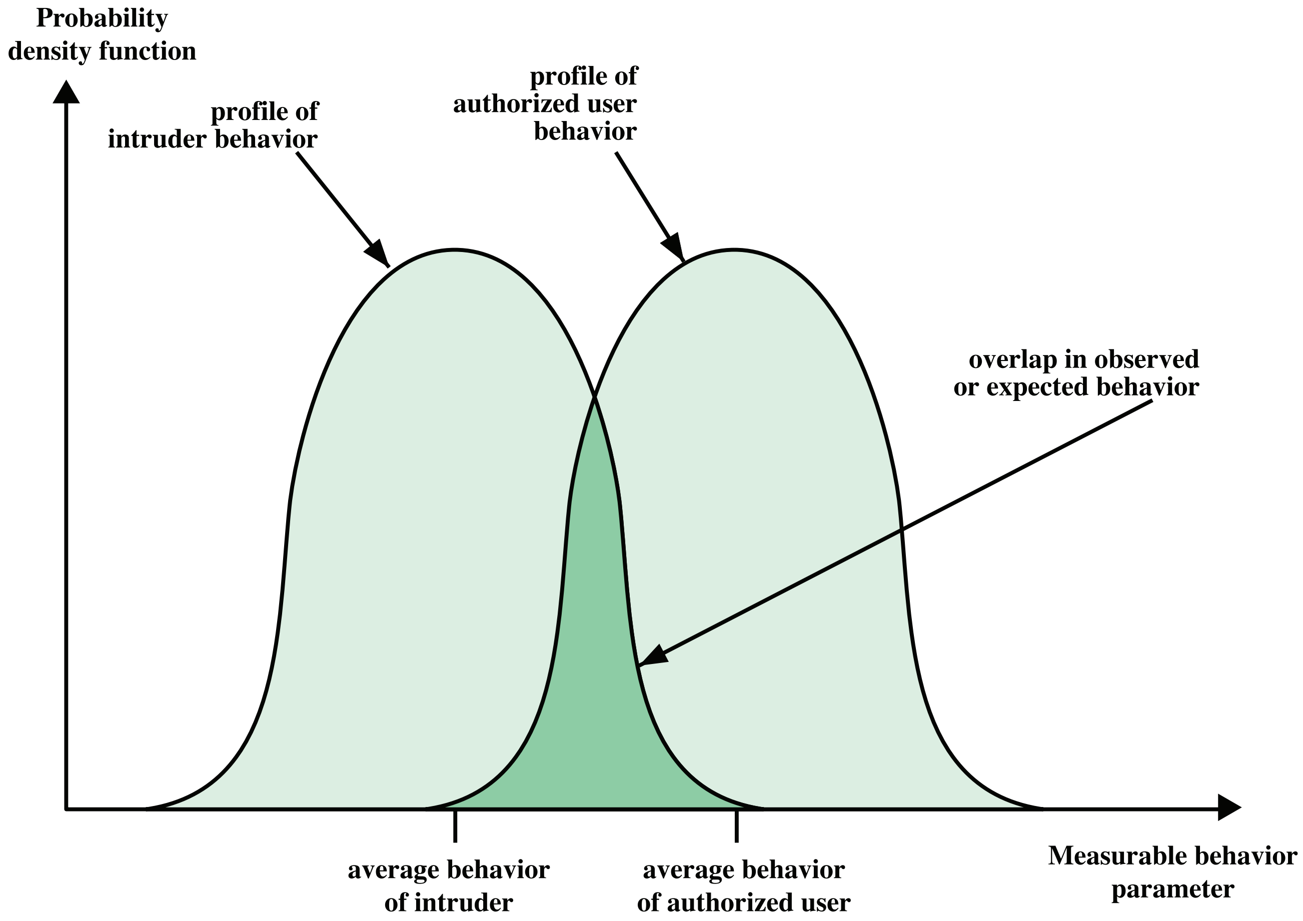
Knowledge based

- Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior

Machine-learning

- Approaches automatically determine a suitable classification model from the training data using data mining techniques

Anomaly Detection: False Positive


Probability density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter

Signature or Heuristic Detection

- Detects intrusion by observing events in the system and applying a set of signature patterns to the data, or a set of rules that characterize the data, leading to a decision regarding whether the observed data indicates normal or anomalous behavior.

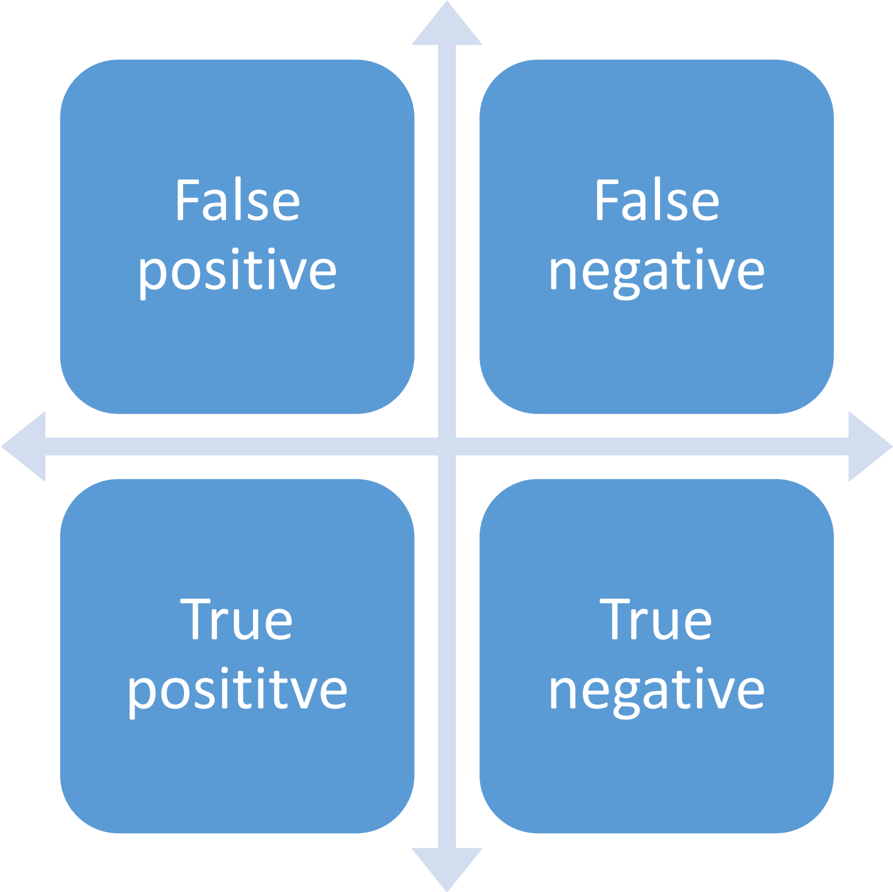
Signature approaches

- Match a large collection of known patterns of malicious data against data stored on a system or in transit over a network
- Widely used in anti-virus products, network traffic scanning proxies, and in NIDS

Rule-based heuristic identification

- Involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses

Signature or Heuristic Detection: False Negative



False positive

False negative

True posititve

True negative

Intrusion Detection System (IDS)

- Based on the source and type of data analyzed, IDSs are classified as:

Host-based IDS (HIDS)

- Monitors the characteristics of a single host for suspicious activity

Network-based IDS (NIDS)

- Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity

Distributed or hybrid IDS

- Combines information from a number of sensors, often both host and network based, in a central analyzer that is able to better identify and respond to intrusion activity

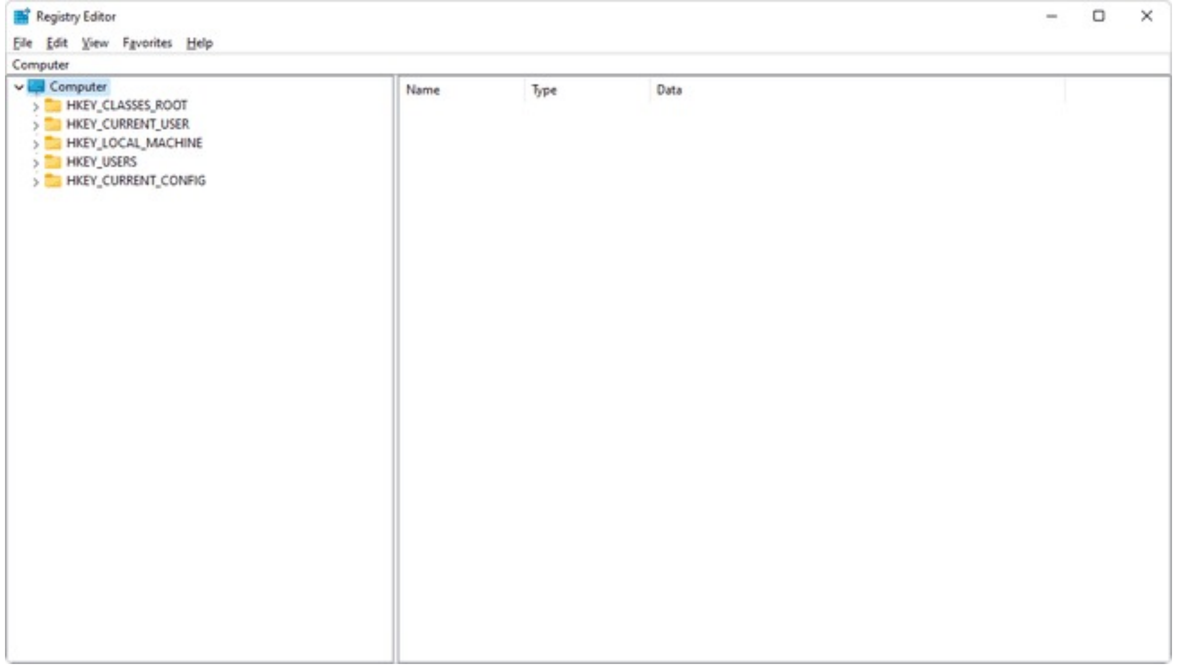
Host-Based Intrusion Detection (HIDS)

- Adds a specialized layer of security software to vulnerable or sensitive systems
  - e.g., database servers and administrative systems
- Can use either anomaly or signature/heuristic approaches
- Monitors activity to detect suspicious behavior
  - Primary purpose is to detect intrusions, log suspicious events, and send alerts
  - Can detect both external and internal intrusions

HIDS: Data Sources and Sensors

- A fundamental component of intrusion detection is the sensor that collects data

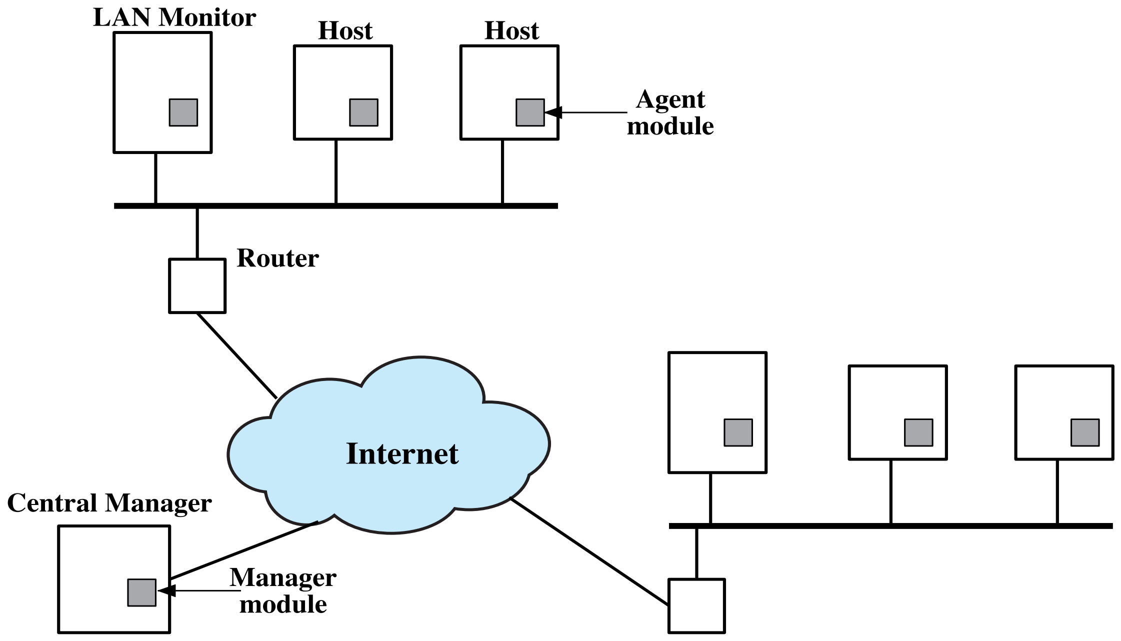
- Common data sources include:
  - System call traces
  - Audit (log file) records
  - File integrity checksums
  - Registry access



E.g., Windows Registry stores much of the information and settings for software programs, hardware devices, user preferences, and operating-system configurations.

HIDS

- Anomaly HIDS
- Signature or Heuristic HIDS
- Distributed HIDS



Architecture for Distributed Intrusion Detection

Host agent module:

- Collect data on security-related events on the host
- Transmit these to the central manager.

LAN monitor agent module:

- A host agent module
- + Analyzes LAN traffic and reports the results to the central manager

Central manager module:

- Receives reports from LAN monitor and host agents
- Processes and correlates these reports to detect intrusion.

Network-Based IDS (NIDS)

- Monitors traffic at a selected points on the network
- Examines traffic packet by packet in real (or close to real) time
- May examine network, transport, and/or application-level protocol activity

- Includes a number of sensors, one or more servers for NIDS management, and one or more management consoles for the human interface
- Analysis of traffic can be done at sensor, the management server, or the combination of the two.

Types of Network Sensors

- Sensors can be deployed in one of two modes: inline and passive.

Inline sensor

- is inserted into a network segment so that the traffic that it is monitoring must pass through the sensor.

Passive sensor

- monitors a copy of network traffic; the actual traffic does not pass through the device.

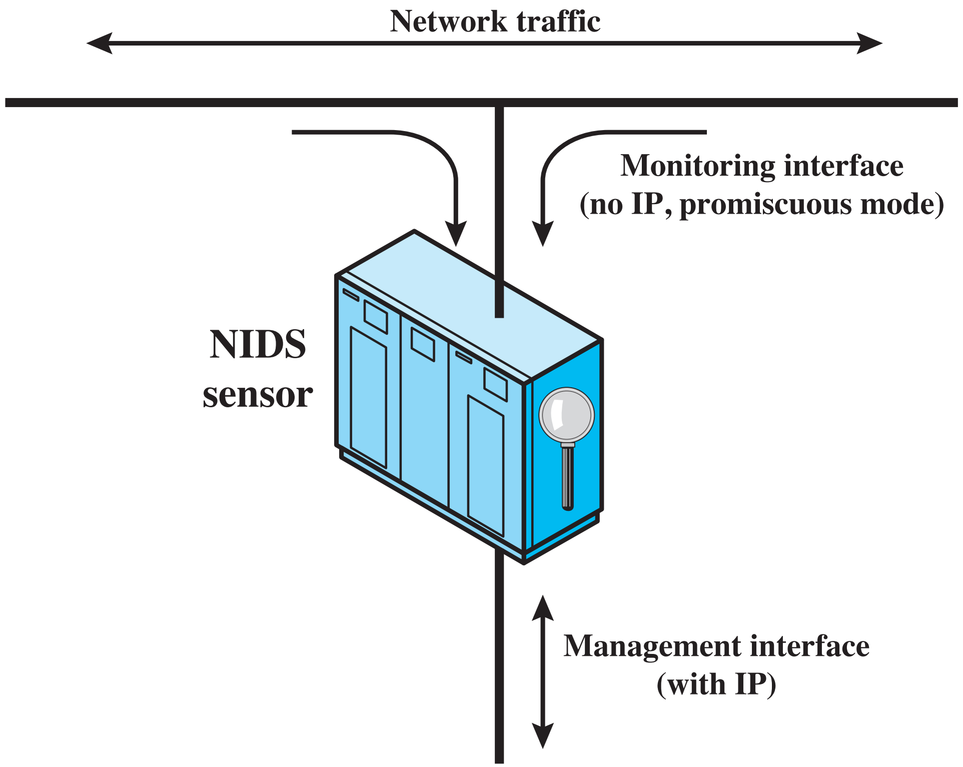


Figure 8.4 Passive NIDS Sensor

NIDS Sensor Deployment

- Example of NIDS Sensor Deployment

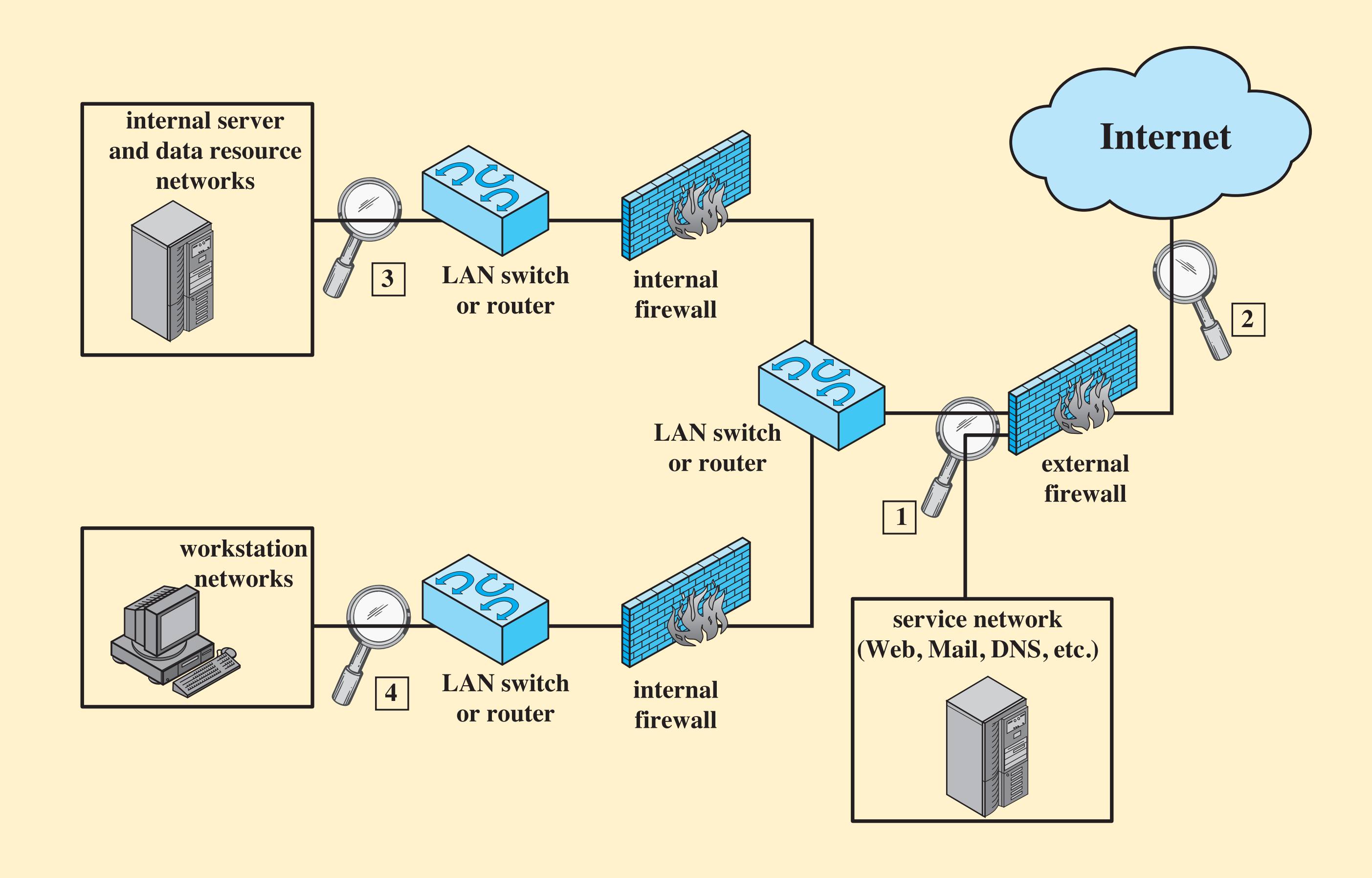
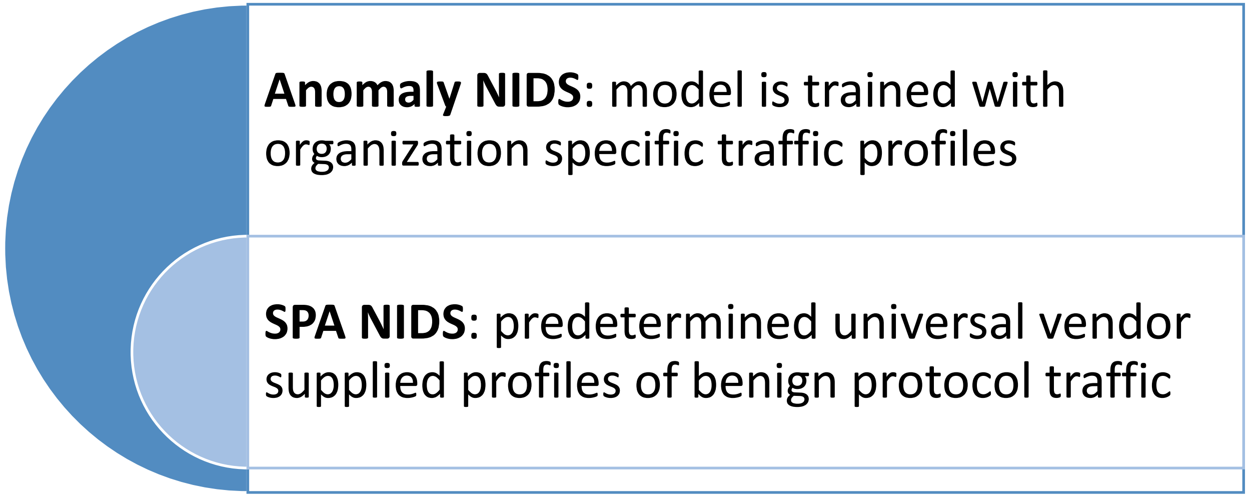


Figure 8.5 Example of NIDS Sensor Deployment

Intrusion Detection Techniques for NIDS

- Signature Detection
- Anomaly Detection Techniques
- Stateful Protocol analysis (SPA)



Anomaly NIDS: model is trained with organization specific traffic profiles

SPA NIDS: predetermined universal vendor supplied profiles of benign protocol traffic

Logging of Alerts

- Typical information logged by a NIDS sensor includes:
  - Timestamp
  - Connection or session ID
  - Event or alert type
  - Rating (e.g., priority, severity, impact, confidence)
  - Network, transport, and application layer protocols
  - Source and destination IP addresses
  - Source and destination TCP or UDP ports, or ICMP types and codes
  - Number of bytes transmitted over the connection
  - …

Honeypots

- Decoy systems designed to:
  - Divert an attacker from accessing critical systems
  - Collect information about the attacker’s activity
  - Encourage the attacker to stay on the system long enough for administrators to respond

- These systems are filled with fabricated information that a legitimate user of the system wouldn’t access

- Resources that have no production value
  - Therefore, incoming communication is most likely a probe, scan, or attack
  - Initiated outbound communication suggests that the system has probably been compromised

Honeypot Classifications

Low interaction honeypot

- Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems
- Provides a less realistic target
- Often sufficient for use as a component of a distributed IDS to warn of imminent attack

High interaction honeypot

- A real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers
- Is a more realistic target that may occupy an attacker for an extended period
- However, it requires significantly more resources
- If compromised could be used to initiate attacks on other systems.

Example of Honeypot Deployment

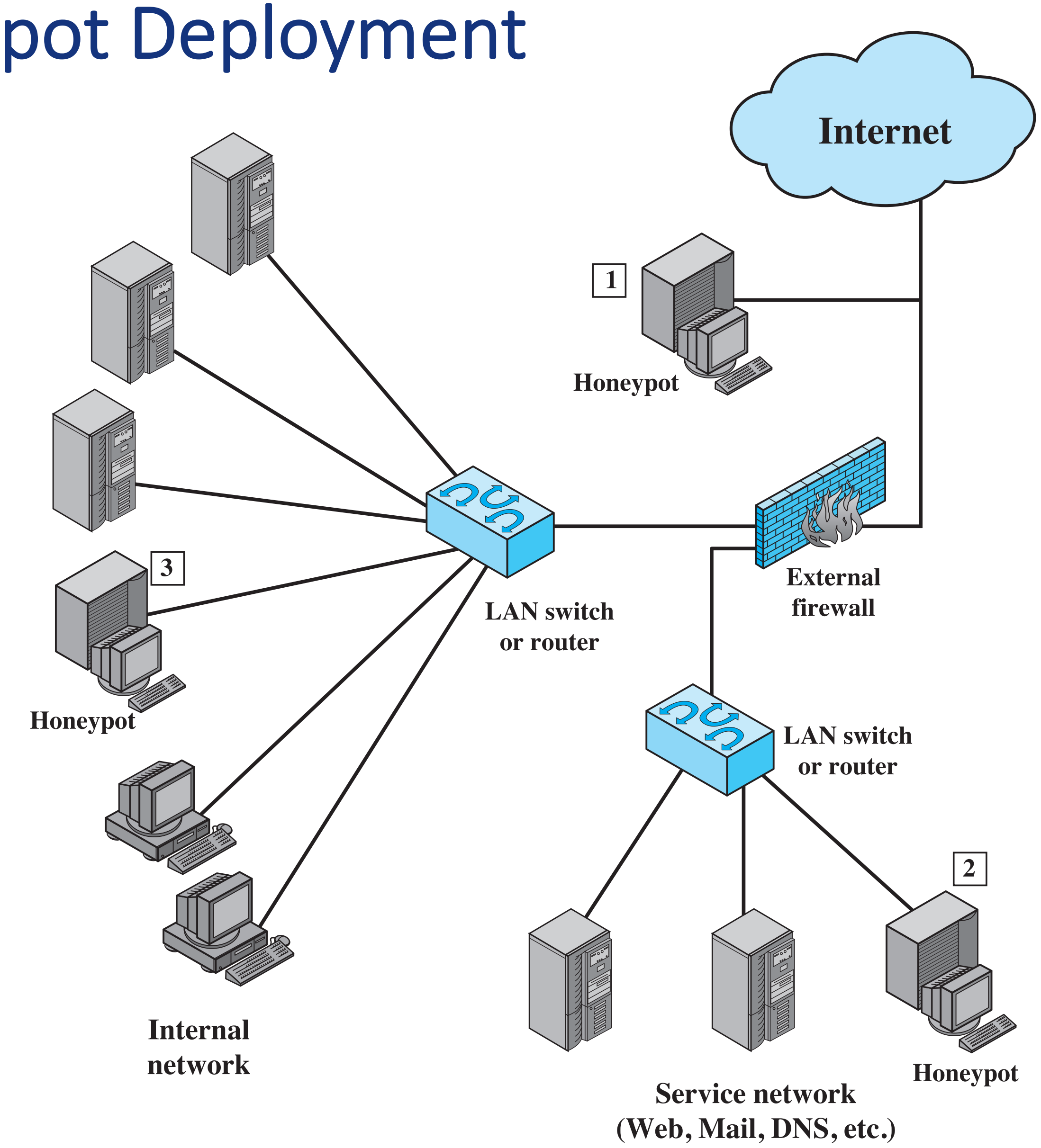


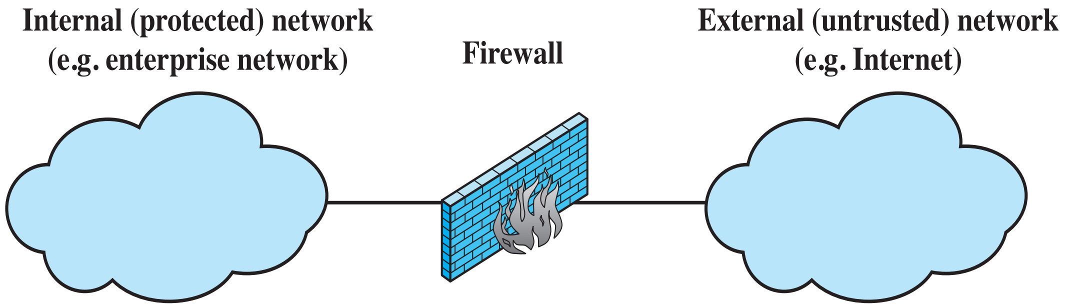
Figure 8.8 Example of Honeypot Deployment

Part 2. Firewall & Intrusion Prevention

Firewalls

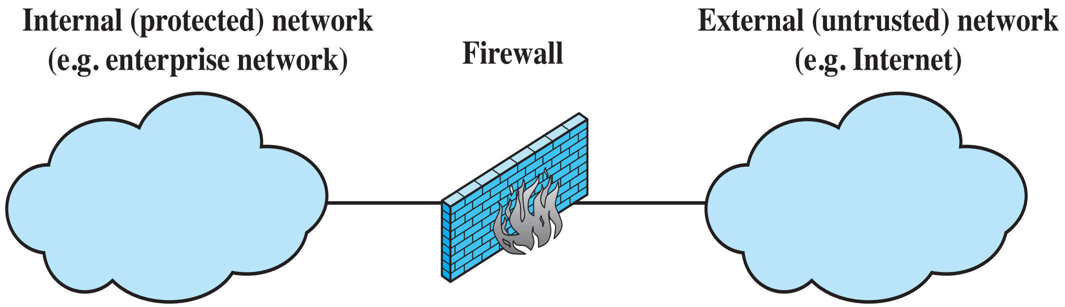
- What is a firewall

- A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- Typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)

Firewall Design Goals

- All traffic from inside to outside, and vice versa, must pass through the firewall
- Only authorized traffic as defined by the local security policy will be allowed to pass
- The firewall itself is immune to penetration


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)

Firewall Filter Characteristics

- Characteristics that a firewall access policy could use to filter traffic include:

IP address and protocol values

- Based on the source or destination addresses and port numbers, direction of flow (inbound or outbound), and other network and transport layer characteristics
- Used by **packet filter** and **stateful inspection firewalls**
- Typically used to limit access to specific services

Application protocol

- Controls access on the basis of authorized application protocol data.
- Used by **application-level gateways** that relay and monitor the exchange of information for specific application protocols

User identity

- Based on the identity of inside users

Network activity

- Controls access based on considerations such as the time or request, rate of requests, or other activity patterns

Firewall Capabilities and Limits

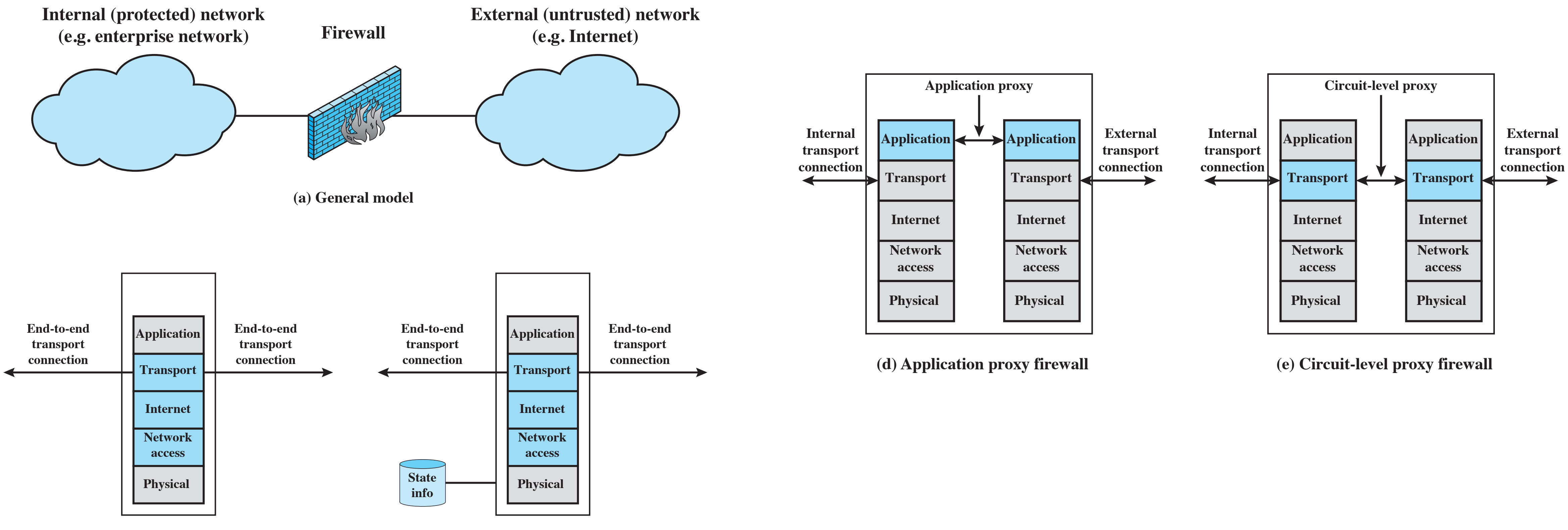
Capabilities:

- Defines a single choke point
- Provides a location for monitoring security events (e.g., audits, alarms)
- Convenient platform for several Internet functions that are not security related, e.g., network address translator

Limitations:

- Cannot protect against attacks bypassing firewall
- May not protect fully against internal threats
- Laptop or portable storage device may be infected outside the corporate network then used internally

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
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

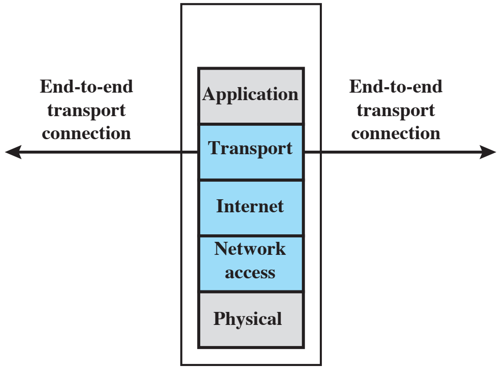
Packet Filtering Firewall

- Applies rules to each incoming and outgoing IP packet
  - Is typically set up as a list of rules based on matches in the IP or TCP header
  - Forwards or discards the packet based on rules match

- Two default policies:
  - Discard - prohibit unless expressly permitted
    - More secure but can reduce availablity
  - Forward - permit unless expressly prohibited
    - Easier to manage and use but less secure

Filtering rules are based on information contained in a network packet

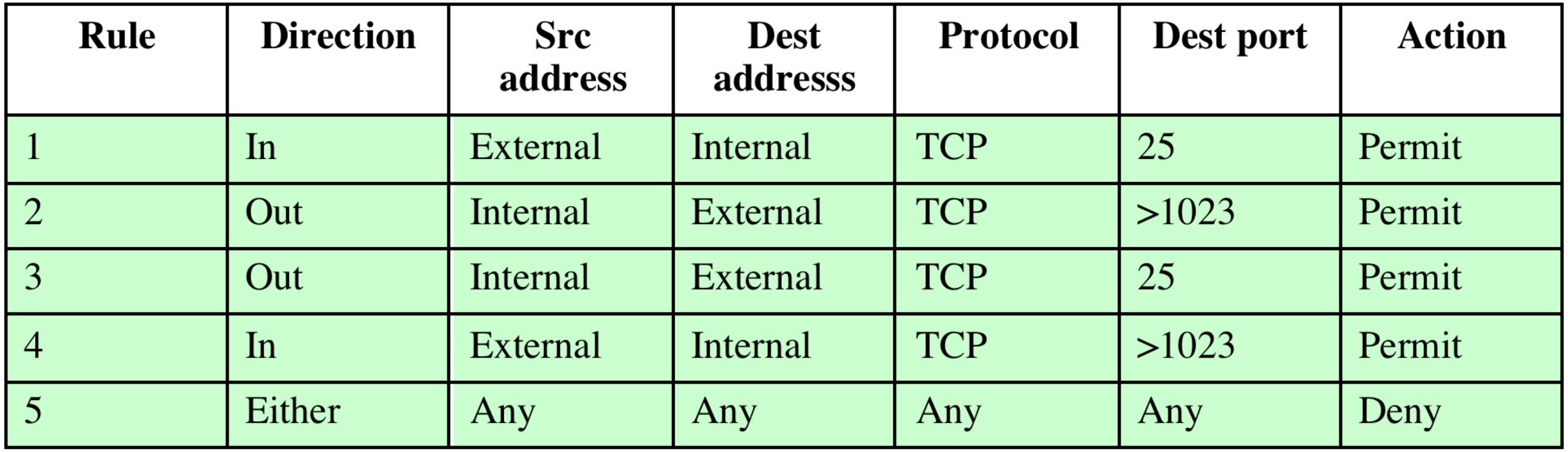
- Source IP address
- Destination IP address
- Source and destination transport-level address
- IP protocol field
- Interface


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection

(b) Packet filtering firewall

Packet-Filtering Firewall Example

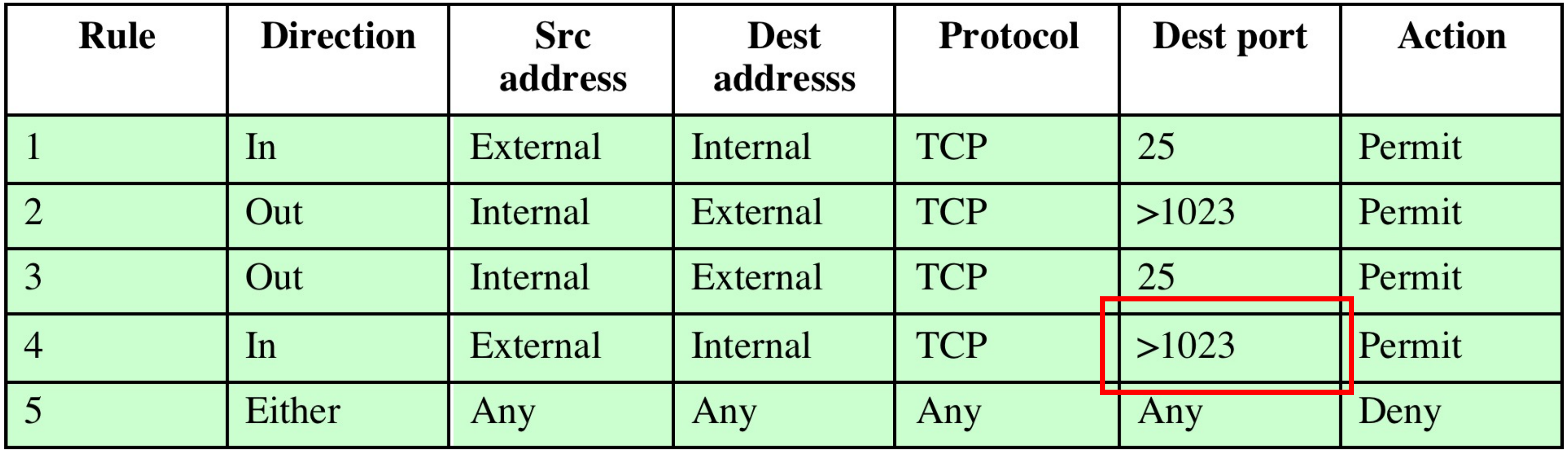
- Simplified rule set for SMTP traffic.
- The goal is to allow inbound and outbound email traffic but to block all other traffic.



Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Packet-Filtering Firewall Example

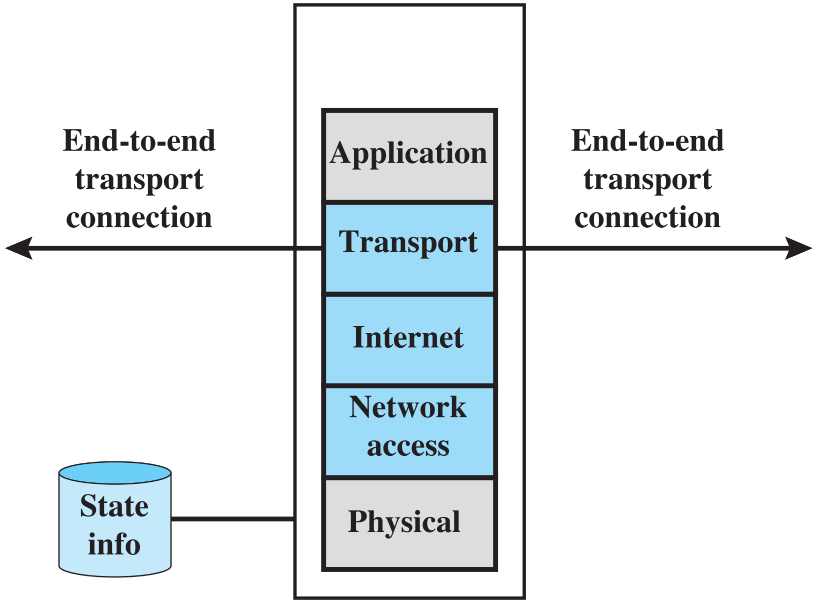
- Any vulnerabilities?



Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Stateful Inspection Firewall

- Tightens rules for TCP traffic by creating a directory of outbound TCP connections
  - There is an entry for each currently established connection
  - Packet filter allows incoming traffic to high numbered ports only for those packets that fit the profile of one of the entries in this directory


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info

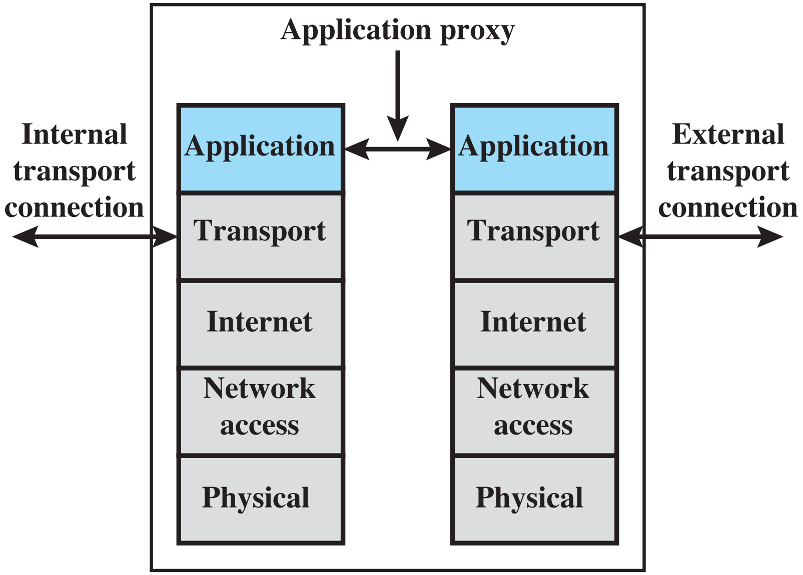
(c) Stateful inspection firewall

Example Stateful Firewall Connection State Table

3Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Application-Level Gateway

- Also called an application proxy
- Acts as a relay of application-level traffic

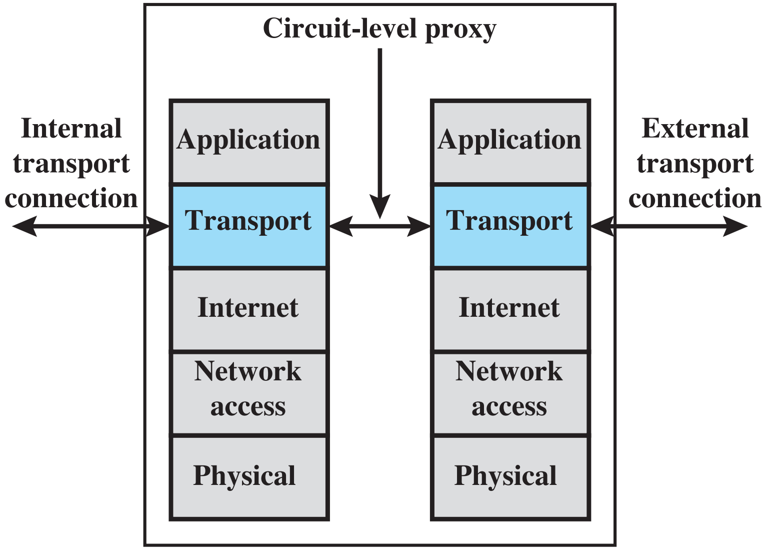


(d) Application proxy firewall

User contacts gateway using a TCP/IP application → User is authenticated → Gateway contacts application on remote host and relays TCP segments between server and user

Circuit-Level Gateway

- Circuit level proxy



(e) Circuit-level proxy firewall

- Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host
- Relays TCP segments from one connection to the other without examining contents

- Typically used when inside users are trusted
  - May use application-level gateway inbound and circuit-level gateway outbound

Firewall Basing

- Bastion Hosts
  - Serves as a platform for an application-level or circuit-level gateway
- Host-Based Firewalls
  - A software module used to secure an individual host.
  - A common location for such firewalls is a server.
- Personal Firewall
  - A software module on the personal computer, e.g., in home environment

Firewall Location and Configurations

DMZ: demilitarized zone

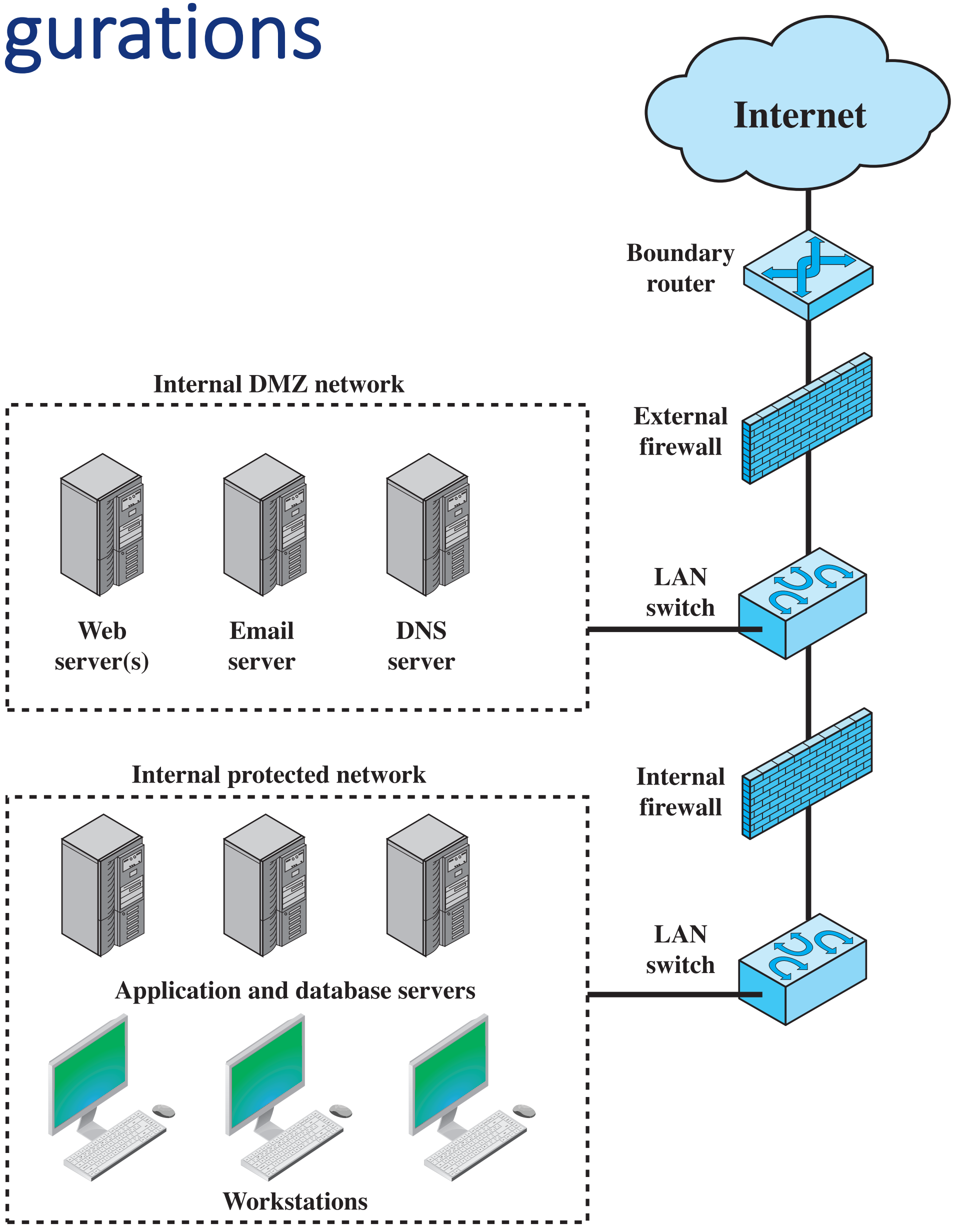


Figure 9.2 Example Firewall Configuration

Distributed Firewalls

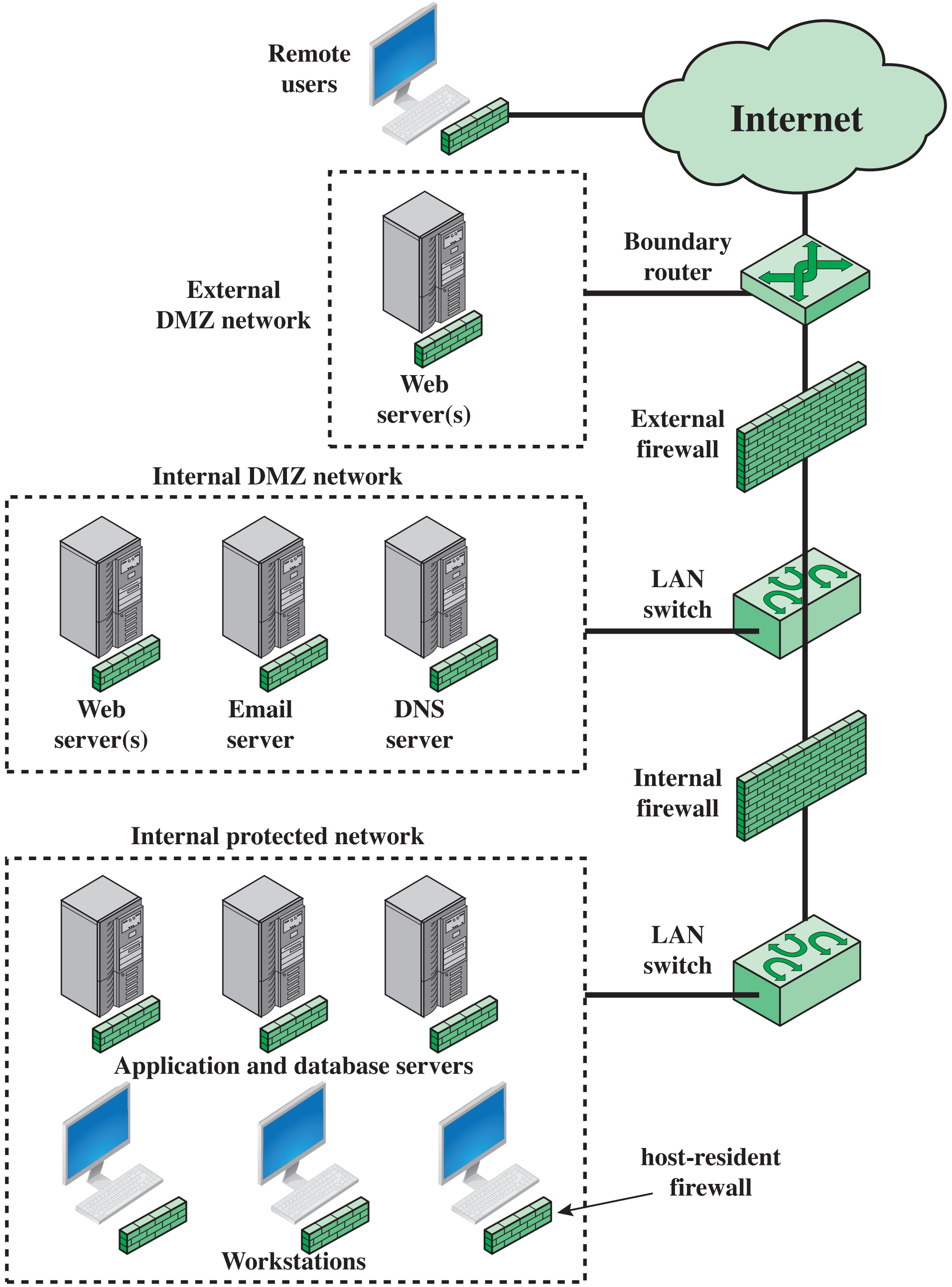


Figure 9.4 Example Distributed Firewall Configuration

Intrusion Prevention Systems (IPS)

- Also known as Intrusion Detection and Prevention System (IDPS)
- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid

- Can use anomaly detection to identify behavior that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior.
- Can block traffic as a firewall does but make use of the types of algorithms developed for IDSs to determine **when** to do so.

Summary

- Intrusion detection
- Firewalls and intrusion prevention