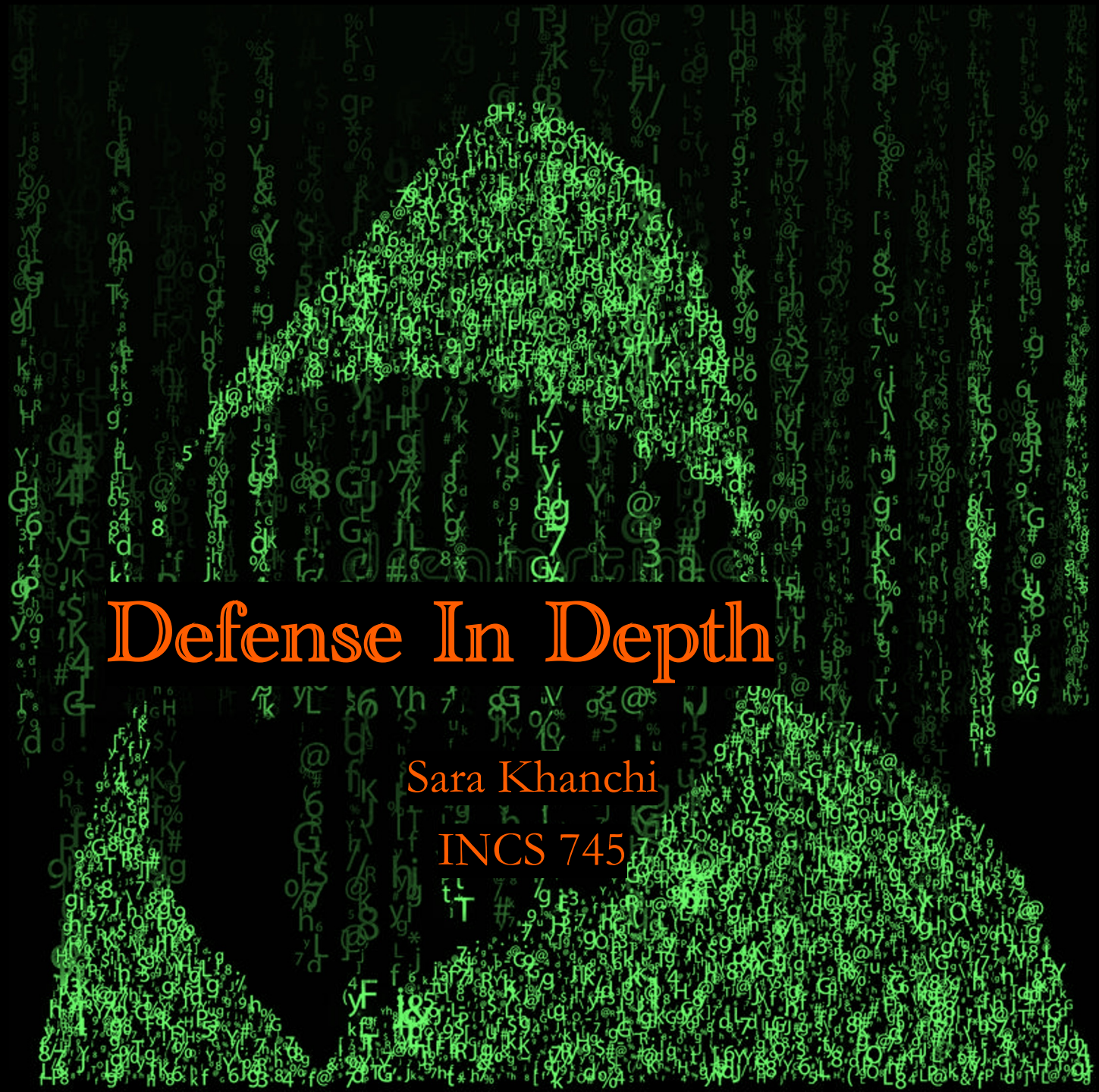


Defense In Depth

Sara Khanchi

INCS 745

Outline

- Defense in depth
- Firewall
- Logging
- Intrusion detection and prevention
- Honeypot

Defense In Depth

- No single control or countermeasure can eliminate risk
- Defense in depth
  - Relates to process of layering defenses
  - Known as
    - protection in depth
    - security in depth

Defense In Depth

Figure 3.6—Types of Defense in Depth Implementations

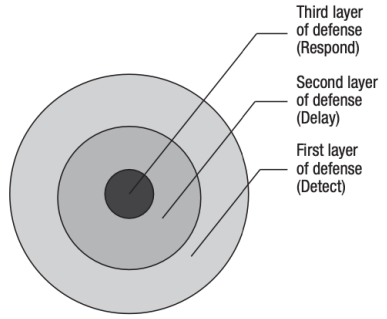
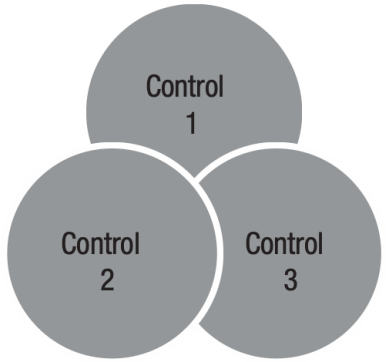
Type of Defense	Graphical Representation	Description
Concentric Rings (or nested layering)		Creates a series of nested layers that must be bypassed in order to complete an attack. Each layer delays the attacker and provides opportunities to detect the attack.
Overlapping redundancy		Two or more controls that work in parallel to protect an asset. Provides multiple, overlapping points of detection. This is most effective when each control is different.

Figure 3.6—Types of Defense in Depth Implementations *(cont.)*

Type of Defense	Graphical Representation	Description
Segregation or compartmentalization		Compartmentalizes access to an asset, requiring two or more processes, controls or individuals to access or use the asset. This is effective in protecting very high value assets or in environments where trust is an issue.

Source: Encurve, LLC.

Information Flow Control

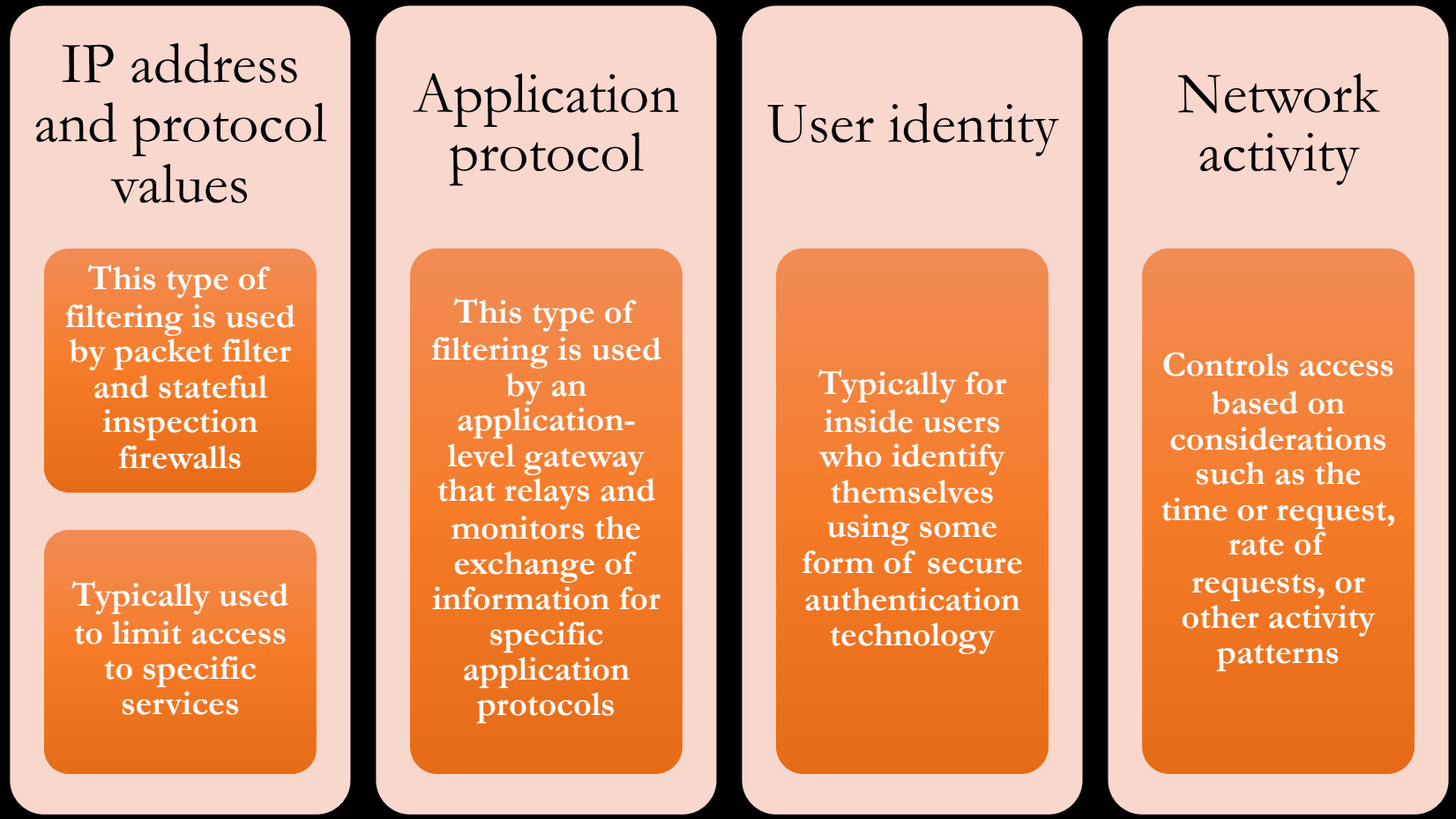
- Corporate network is vulnerable
  - Internet's openness makes every corporate network connected to it vulnerable to attack.
- Hackers on the Internet could break into a corporate network and do harm in a number of ways
- Firewalls are built as one means of perimeter security for these networks.

Firewall

- Firewall
  - A system or combination of systems
  - Enforces a boundary between two or more networks
  - Typically forming a barrier between a secure and an open environment such as the Internet
- Enable organizations to
  - Block access to particular sites on the Internet
  - Limit traffic on an organization's public services segment to relevant addresses and ports
  - Prevent certain users from accessing certain servers or services
  - Monitor and record communications
  - Encrypt packets that are sent between different physical locations within an organization

Firewall Filter Characteristics

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



Firewall Filter Characteristics

- **IP Address and Protocol Values**: Controls access based on the source or destination addresses and port numbers, direction of flow being inbound or outbound, and other network and transport layer characteristics. This type of filtering is used by packet filter and stateful inspection firewalls. It is typically used to limit access to specific services.

- **Application Protocol**: Controls access on the basis of authorized application protocol data. This type of filtering is used by an application-level gateway that relays and monitors the exchange of information for specific application protocols, for example, checking Simple Mail Transfer Protocol (SMTP) e-mail for spam, or HTPP Web requests to authorized sites only.

- **User Identity**: Controls access based on the users identity, typically for inside users who identify themselves using some form of secure authentication technology, such as IPSec.

- **Network Activity**: Controls access based on considerations such as the time or request, for example, only in business hours; rate of requests, for example, to detect scanning attempts; or other activity patterns.

Firewall Capabilities And Limitations

- **Capabilities:**
  - Defines a single choke point
  - Provides a location for monitoring security events
  - Convenient platform for several Internet functions that are not security related such as Network Address Translator
  - Can serve as the platform for IPSec
- **Limitations:**
  - Cannot protect against attacks bypassing firewall
  - May not protect fully against internal threats
  - Improperly secured wireless LAN can be accessed from outside the organization
  - Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

Firewall Access Policy

- A critical component in the planning and implementation of a firewall is specifying a suitable access policy
  - This lists the types of traffic authorized to pass through the firewall
  - Includes address ranges, protocols, applications and content types
- This policy should be developed from the organization's information security risk assessment and policy
- Should be developed from a broad specification of which traffic types the organization needs to support
  - Then refined to detail the filter elements which can then be implemented within an appropriate firewall topology

Firewall Access Policy

- User control: Controls access to the data based on the role of the user who is attempting to access it. Applied to users inside the firewall perimeter.

- Service control: Controls access by the type of service offered by the host. Applied on the basis of network address, protocol of connection and port numbers.

- Direction control: Determines the direction in which requests may be initiated and are allowed to flow through the firewall. It tells whether the traffic is "inbound" (From the network to firewall) or vice-versa "outbound"

Firewall Actions

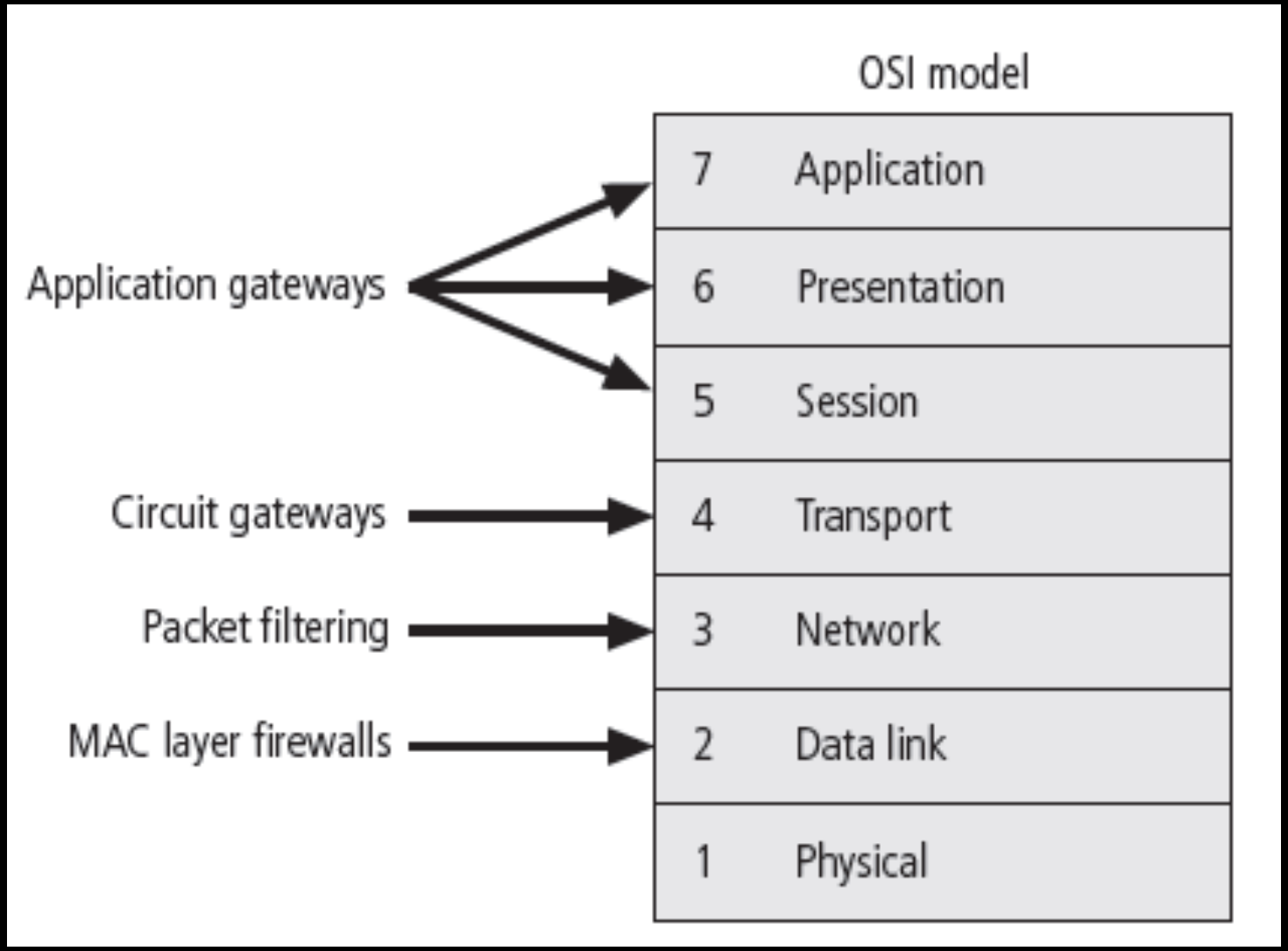
- Accept: Allowed to enter the connected network/host through the firewall.
- Deny: Not permitted to enter the other side of firewall.
- Reject: Similar to “Denied”, but tells the source about this decision through ICMP packet.

Network Firewall Types

- Packet filtering
- Application firewall systems
- Stateful inspection
- Next generation firewall (NGFW)

Figure 3.8—Firewall Types	
First Generation	A simple packet-filtering router that examines individual packets and enforces rules based on addresses, protocols and ports.
Second Generation	Keeps track of all connections in a state table. This allows it to enforce rules based on packets in the context of the communications session.
Third Generation	Operates at layer seven (the application layer) and is able to examine the actual protocol being used for communications, such as Hypertext Transfer Protocol (HTTP). These firewalls are much more sensitive to suspicious activity related to the content of the message itself, not just the address information.
Next Generation	Sometimes called deep packet inspection—is an enhancement to third generation firewalls and brings in the functionality of an intrusion prevention system (IPS) and will often inspect Secure Sockets Layer (SSL) or Secure Shell (SSH) connections.
Source: ISACA, *CRISC Review Manual 6th Edition*, USA, 2015	

Network Firewall Types



Network Firewall Types

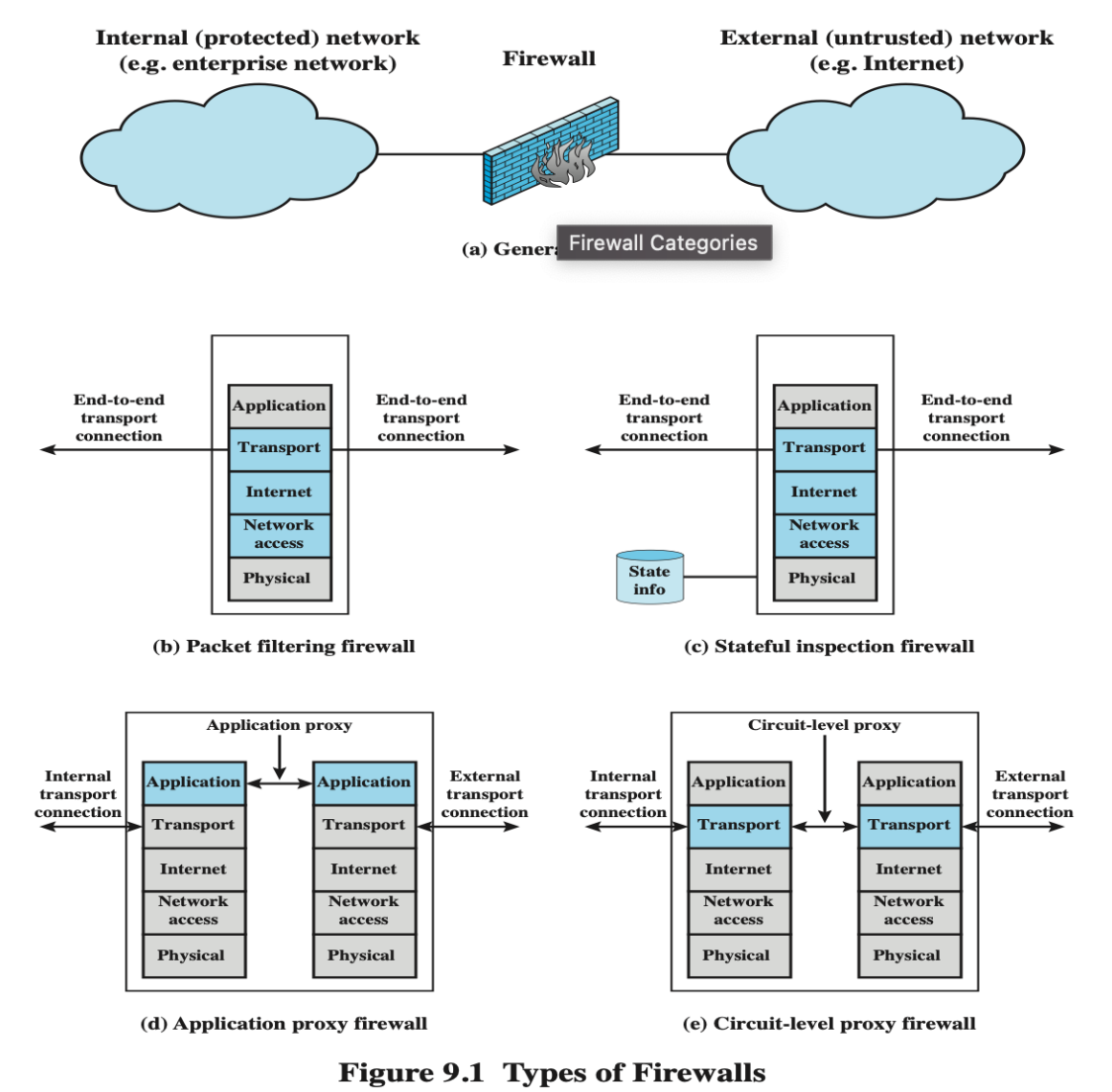
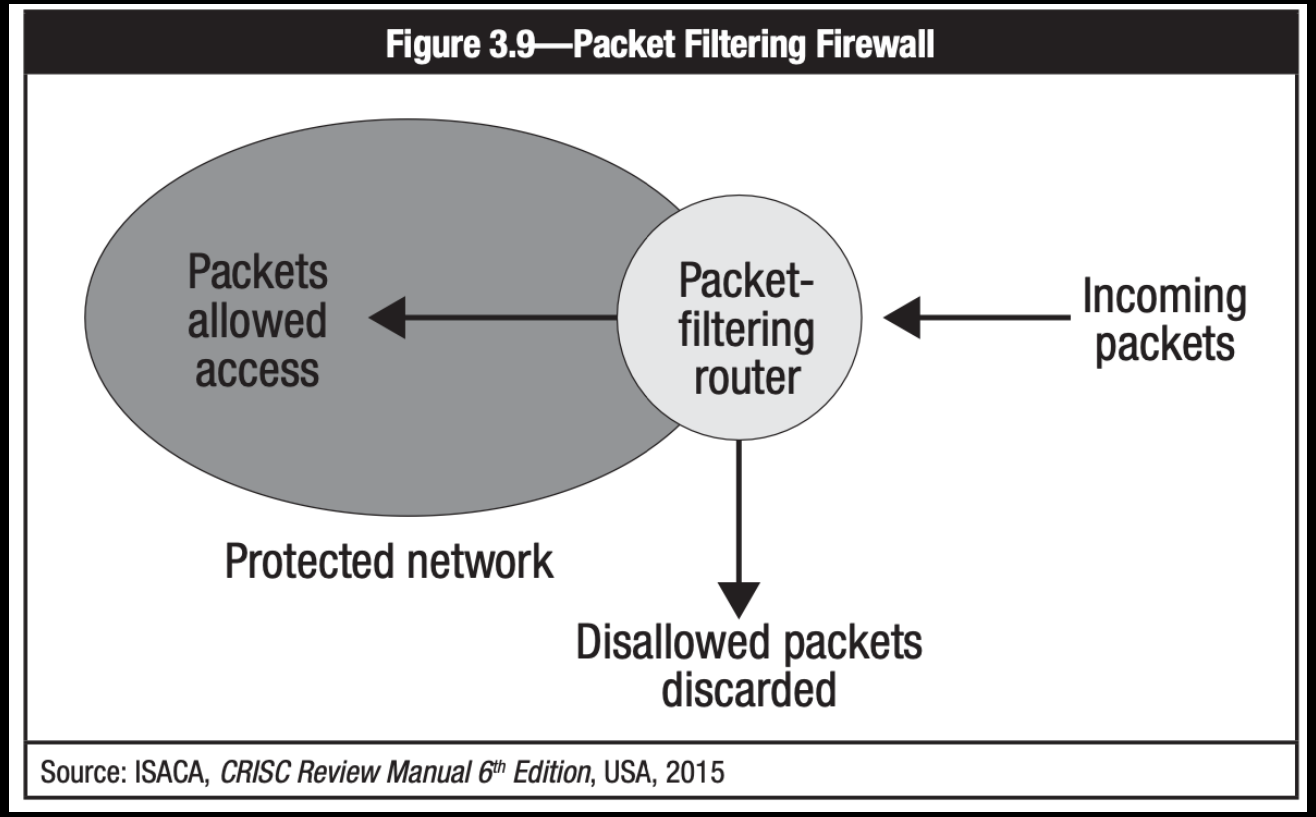


Figure 9.1 Types of Firewalls

Packet Filtering Firewall

- Filter based on
  - Source IP address
  - Destination IP address
  - Source and destination ports
  - IP protocol field
  - Direction
- Two default policies:
  - Deny all - prohibit unless expressly permitted
    - More conservative, controlled, visible to users
  - Permit all - permit unless expressly prohibited
    - Easier to manage and use but less secure



Packet Filtering Firewall

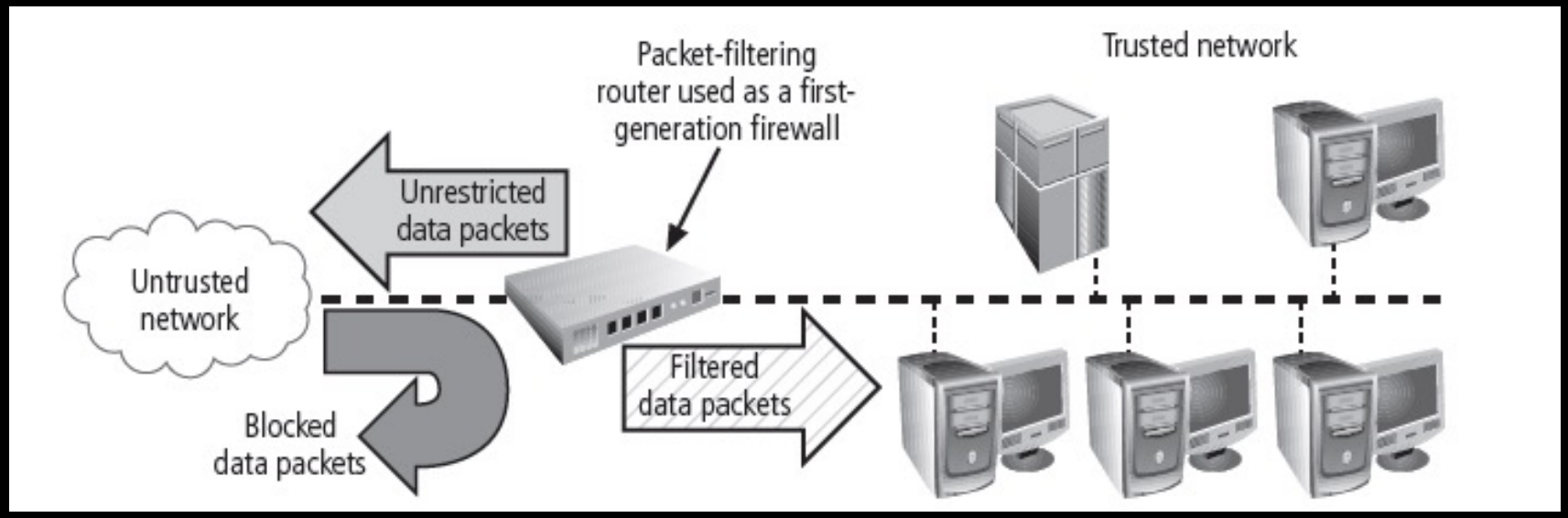


Figure 4-9 Packet Filtering Router

IP Packet

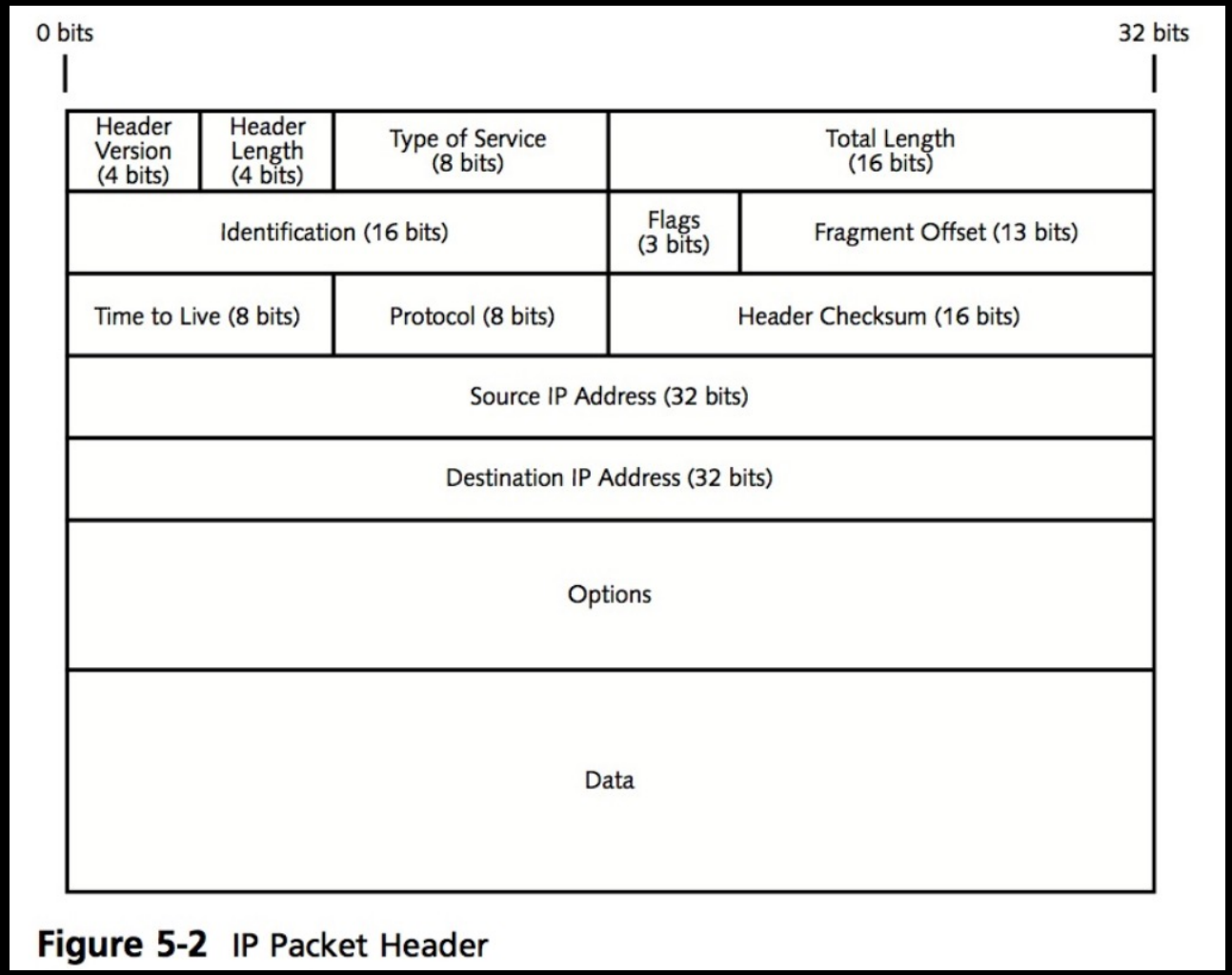


Figure 5-2 IP Packet Header

Table 9.1
Packet-Filtering Example

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

- Stable and simple

Figure 3.10—Packet Filtering Firewalls

Advantages	Disadvantages
Simplicity of one network "choke point"	Vulnerable to attacks from improperly configured filters
Minimal impact on network performance	Vulnerable to attacks tunneled over permitted services
Inexpensive or free	All private network systems vulnerable when a single packet filtering router is compromised

Packet Filtering Firewall

- **Common types of attacks**
  - IP spoofing
  - Source routing specification
  - Miniature fragment attack

Stateful Inspection Firewall

- Tracks the destination IP address of each packet that leaves the organization's internal network
- Checks if the incoming message is in response to a request that the organization sent out
- Provide control over the flow of IP traffic

Figure 3.12—Stateful Inspection Firewalls	
Advantages	**Disadvantages**
Provide greater control over the flow of IP traffic	Complex to administer
Greater efficiency in comparison to CPU-intensive, full-time application firewall systems	

Stateful Inspection Firewall

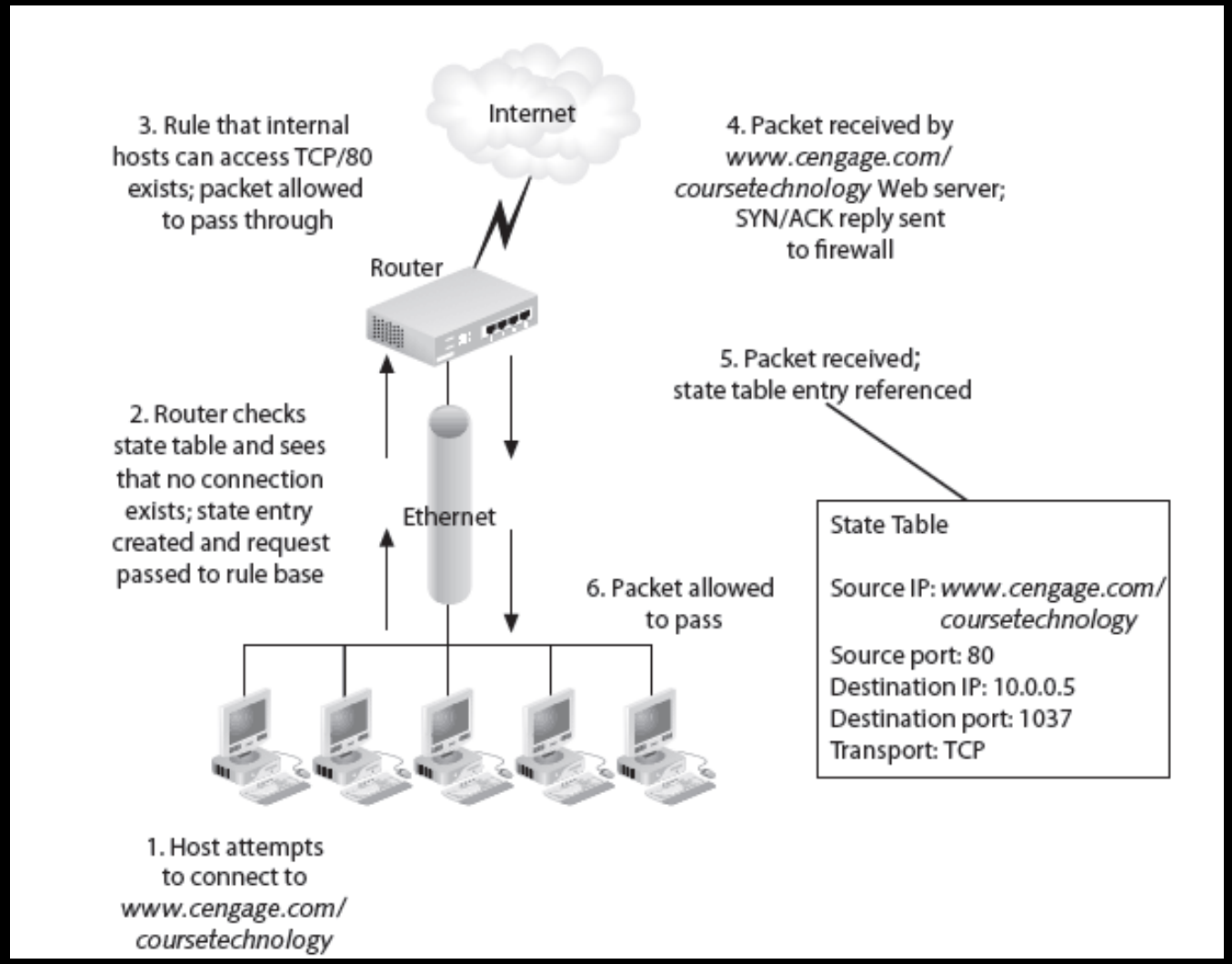
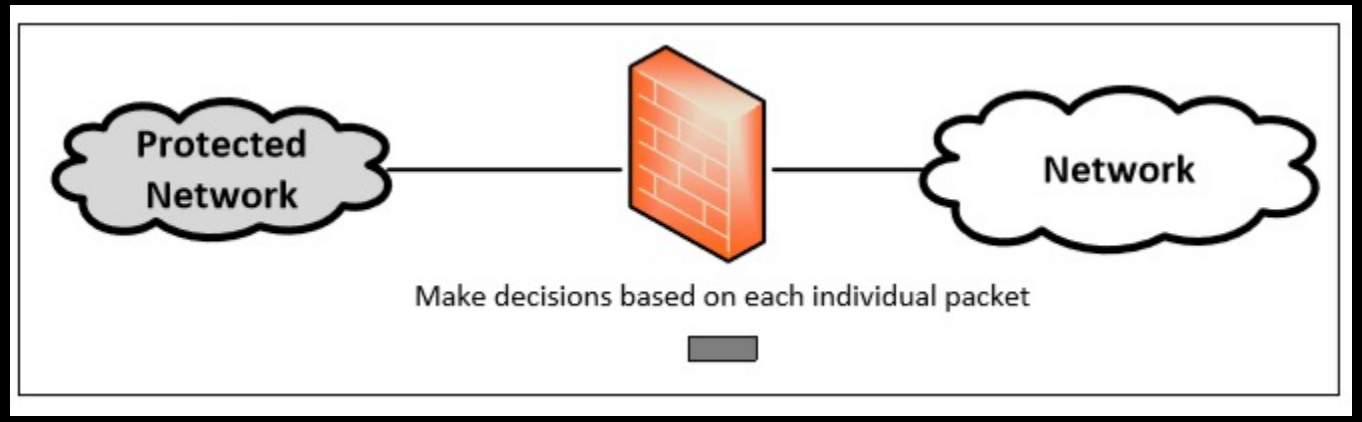


Table 9.2
Example Stateful Firewall Connection State Table

Source 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

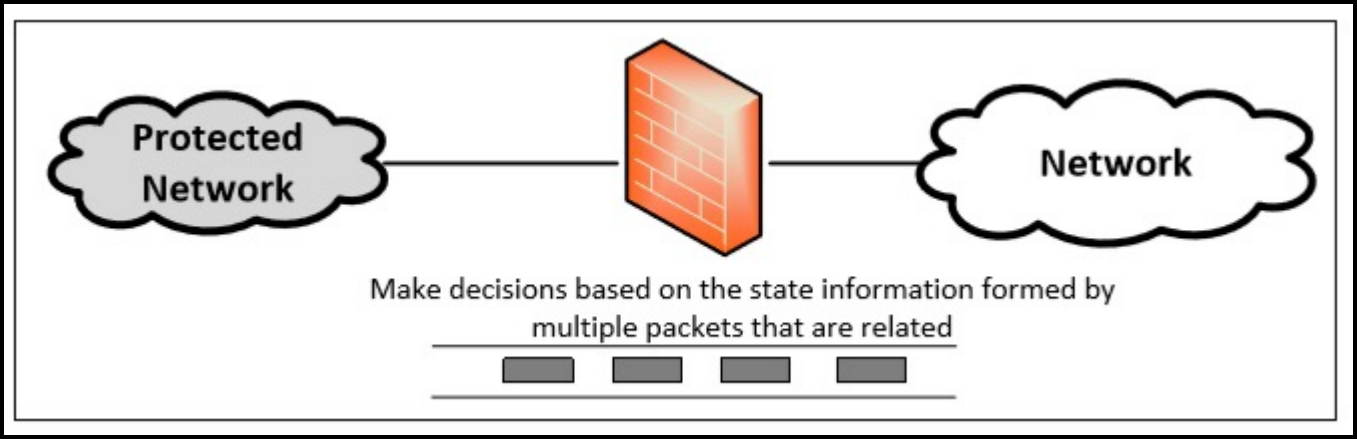
Packet Filter Firewall

- Doesn't pay attention to if the packet is a part of existing stream or traffic
- Doesn't maintain the states about packets. Also called Stateless Firewall



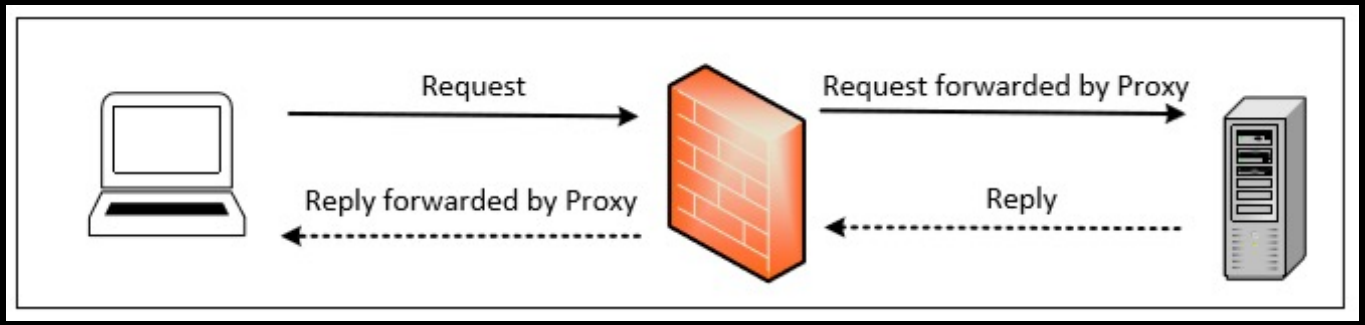
Stateful Inspection Firewall

- Tracks the state of traffic by monitoring all the connection interactions until is closed.
- Connection state table is maintained to understand the context of packets.



Application/Proxy Firewall

- The client's connection terminates at the proxy and a separate connection is initiated from the proxy to the destination host.
- Data on the connection is analyzed up to the application layer to determine if the packet should be allowed or rejected.



Application Firewall Systems

- Two types
  - Application gateway
    - Analyze packets through a set of proxies
  - Circuit-level gateway
    - Use one proxy server for all services
- Allow information to flow between systems but do not allow the direct exchange of packets
- Sit atop hardened operating systems
- Work at the application level of the OSI model

Application Firewall Systems

Figure 3.11—Application Firewalls	
Advantages	**Disadvantages**
Provide security for commonly used protocols	Reduced performance and scalability as Internet usage grows
Generally hide the network from outside untrusted networks	
Ability to protect the entire network by limiting break-ins to the firewall itself	
Ability to examine and secure program code	

Next Generation Firewall

- Addressing two key limitations
  - The inability to inspect packet payload
  - The inability to distinguish between types of web traffic
- Perform
  - Traditional functions
    - Packet filtering, stateful inspection and network address translation (NAT)
  - Application awareness
    - Deep packet inspection (DPI)
  - Integrated threat protection
    - Data loss prevention (DLP)
    - Intrusion prevention system (IPS)
    - Secure sockets layer (SSL)/secure shell (SSH) inspection
    - Web filtering

Next Generation Firewall

- **Application awareness**
  - The capacity of a system to maintain information about connected applications to optimize their operation and that of any subsystems that they run or control
- Deep Packet Inspection (DPI)
  - Allows for payload interrogation against signatures for known exploits, malware, etc.

Web Application Firewall

- A server plug-in, appliance or additional filter that can be used to apply rules to a specific web application
- Block many types of attacks
  - Cross-site scripting (XSS)
  - Structured Query Language (SQL) injection

Firewall Deployment

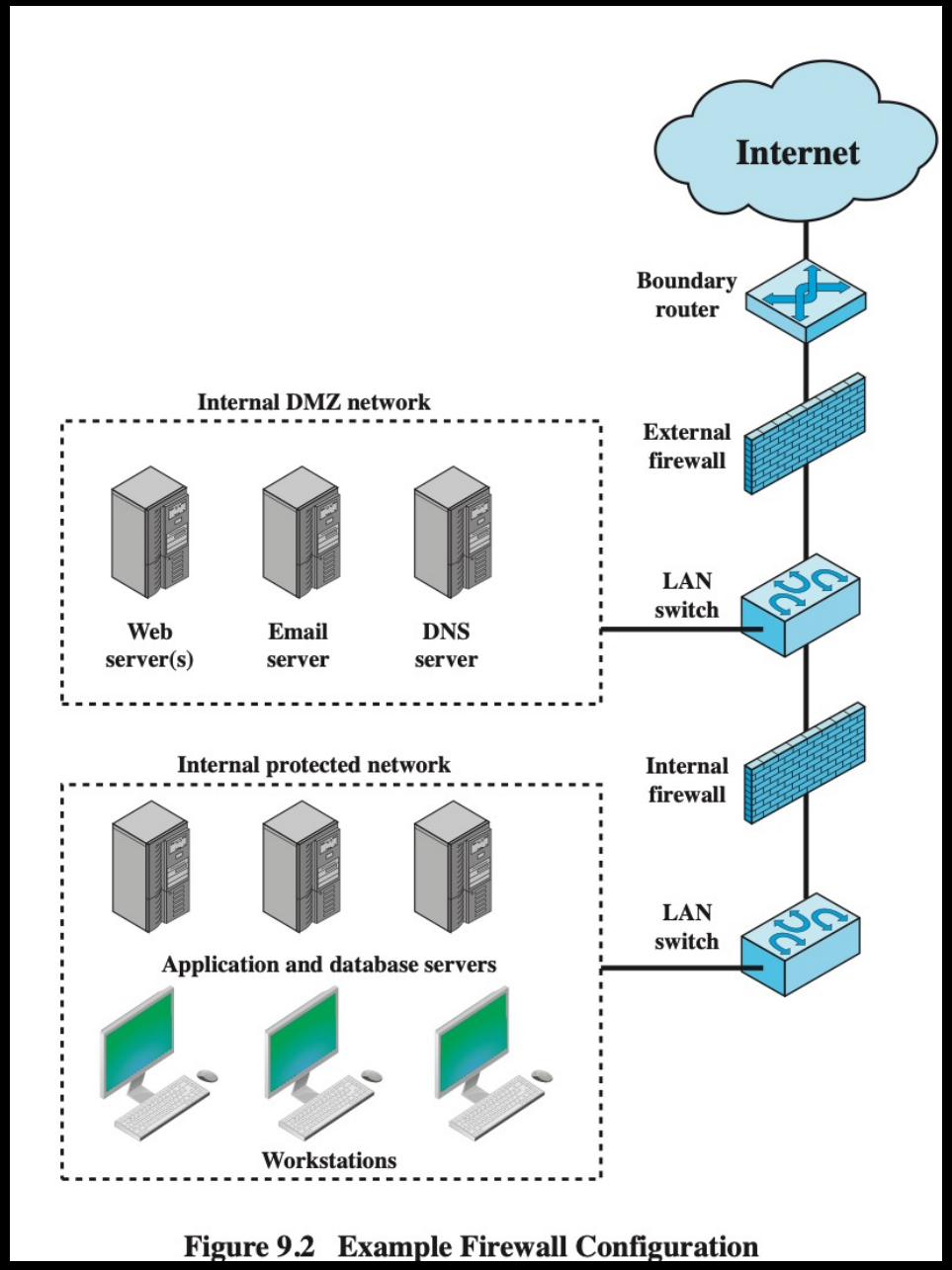


Figure 9.2 Example Firewall Configuration

Firewall Deployment

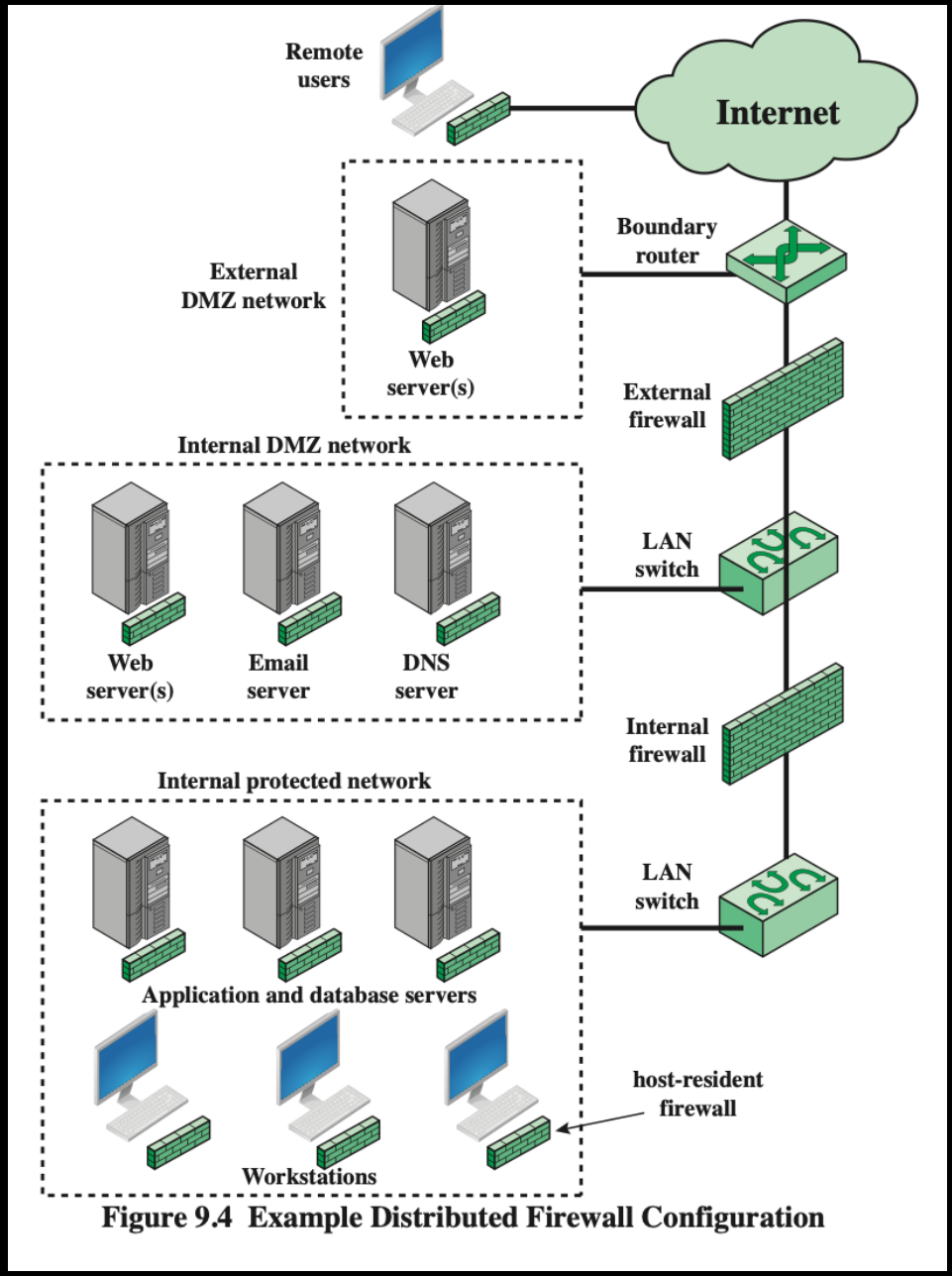


Figure 9.4 Example Distributed Firewall Configuration

Logging

- Monitoring, detection and logging are integral parts of cybersecurity
- Log
  - A record of events that occur within the systems and networks of an organization
  - Record of information
    - Time of the event
    - Changes to permissions
    - System startup or shutdown
    - Login or logout
    - Changes to data
    - Errors or violations
    - Job failures

Logging Challenges

- Common challenges relating to the effective use of logs
  - Having too many data
  - Difficulty in searching for relevant information
  - Improper configuration
  - Modification or deletion of data before they are read

Different Log Sources

- A myriad of security tools are used by organizations
  - Vulnerability assessments
  - Firewalls
  - IDS
- Security teams have to analyze and interpret this overwhelming amount of data

Security Event Management (SEM)

- SEM systems automatically aggregate and correlate security event log data across multiple security devices
- SEM types
  - Rule-based
  - Statistical
- Security Information and Event Management (SIEM)
  - Take the SEM capabilities and combine them with the historical analysis and reporting features of security information management (SIM) systems

Data Loss Prevention

- Two types of attack vectors
  - Ingress
  - Egress (data exfiltration)
- Data loss prevention (DLP)
  - Prevents the data exfiltration of sensitive data
- Three primary states of information
  - Data at rest
  - Data in transit
  - Data in use

Antivirus and Anti-Malware

- Malicious software is one of the most common attack vectors
- Antimalware checkers
  - Historically used, also called virus checkers
  - Host-based applications that scanned incoming traffic looking for patterns
- Heuristic-based methods
- Antimalware can be controlled
  - Restriction of outbound traffic
    - Prevent malware from exfiltrating data or communicating with control systems used by the adversary
  - Policies and awareness that train users
    - Avoid opening suspect emails or attachments and to recognize Uniform resource locators (URLs) that may introduce malicious code
  - A combination of signature identification and heuristic analysis

Intrusion Detection Systems

- An IDS works in conjunction with routers and firewalls by monitoring network usage anomalies
- Broad categories of IDSs
  - **Network-based IDSs**
    - Monitor network
  - **Host-based IDSs**
    - Monitor various internal resources of the operating system
- Components of an IDS
  - Sensors
  - Analyzers
  - Administration console

IDS Sensor

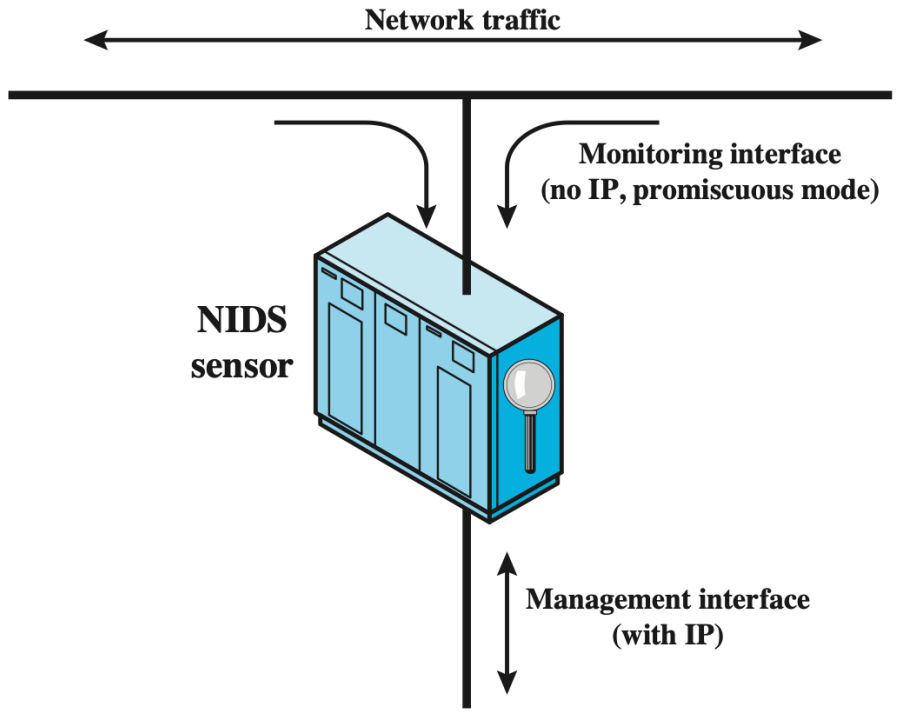


Figure 8.4 Passive NIDS Sensor

IDS Sensor

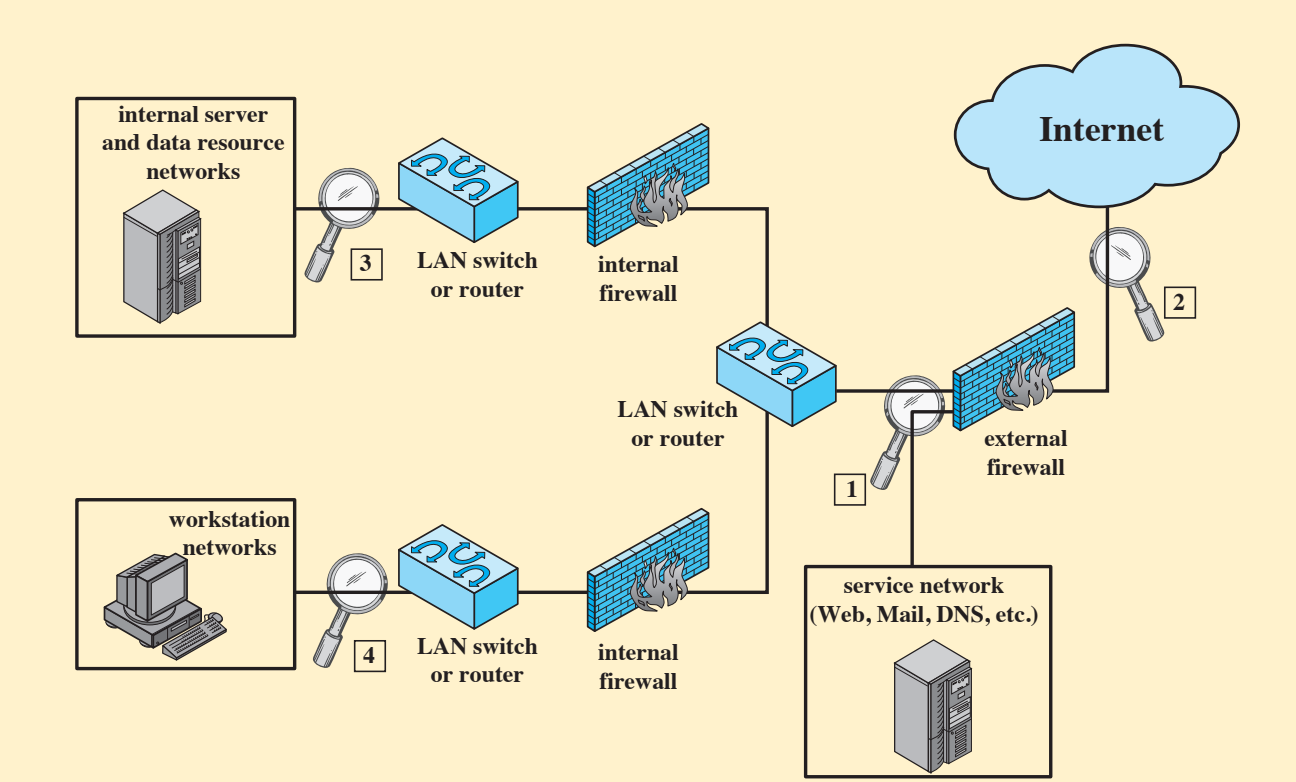


Figure 8.5 Example of NIDS Sensor Deployment

Intrusion Detection Systems

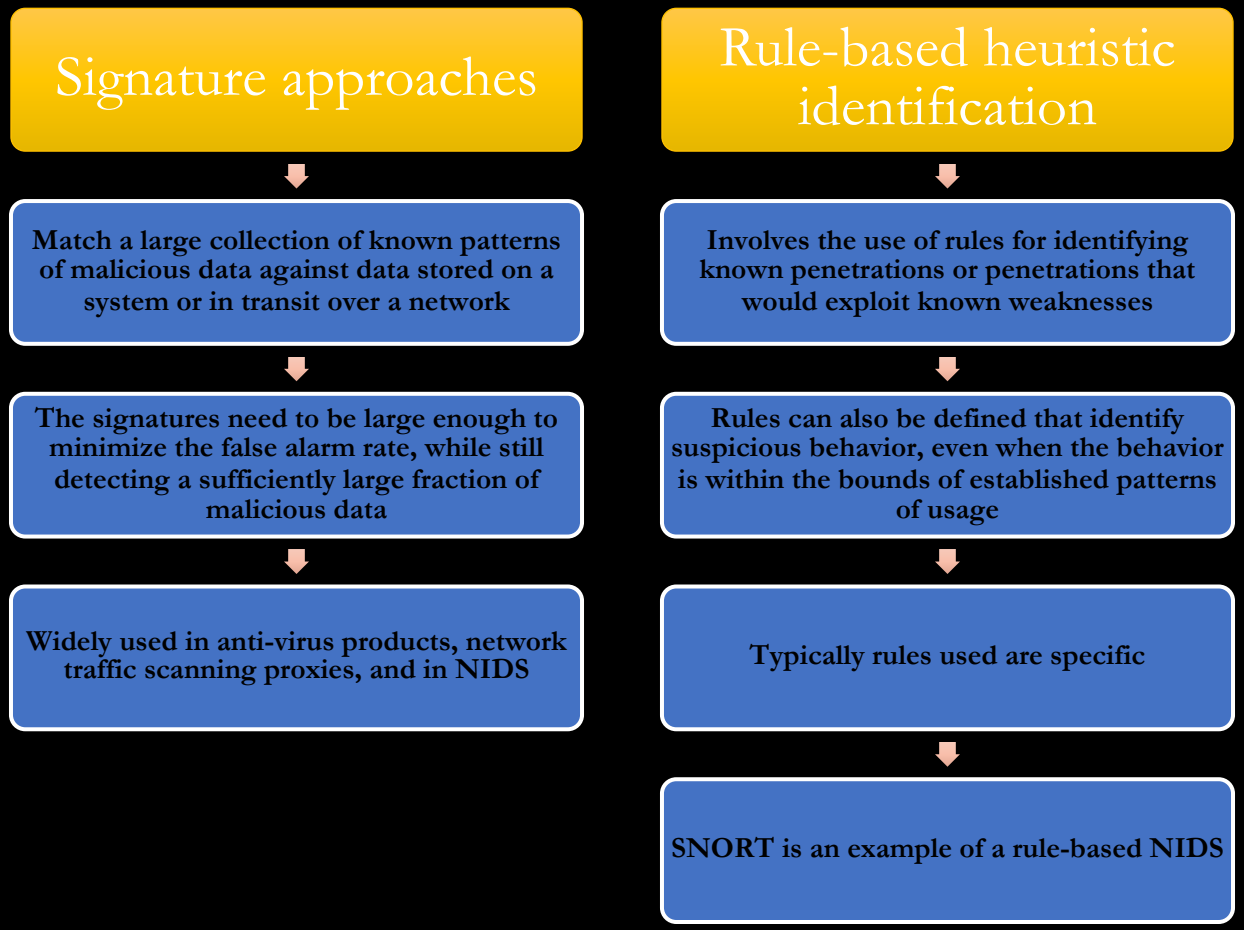
- Types of IDSs
  - Signature-based
    - Known as Misuse detection
    - Uses a set of known malicious data patterns or attack rules that are compared with current behavior
    - Can only identify known attacks for which it has patterns or rules
  - Anomaly Detection
    - Involves the collection of 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

Anomaly Detection

A variety of classification approaches are used:

Statistical	Knowledge based	Machine-learning
• Analysis of the observed behavior using univariate, multivariate, or time-series models of observed metrics	• Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior	• Approaches automatically determine a suitable classification model from the training data using data mining techniques

Signature or Heuristic Detection



Intrusion Detection Systems

- IDS Policy
  - An IDS policy should establish the action to be taken by security personnel in the event that an intruder is detected.
  - Terminate the access
  - Trace the access

Intrusion Detection Techniques

- Attacks suitable for signature detection
  - Application layer reconnaissance and attacks
  - Transport layer reconnaissance and attacks
  - Network layer reconnaissance and attacks
  - Unexpected application services
  - Policy violations
- Attacks suitable for anomaly detection
  - Denial-of-service (DoS) attacks
  - Scanning
  - Worms

Intrusion Prevention Systems

- An IPS is a system designed to not only detect attacks, but also to prevent the intended victim hosts from being affected by the attacks
- The biggest advantage
  - It can help block an attack when it occurs; rather than simply sending an alert, it actively helps to block malicious and unwanted traffic

Honeypots

- Decoy systems designed to:
  - Tempt a potential attacker away from critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to respond
- 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

Honeypot Deployment

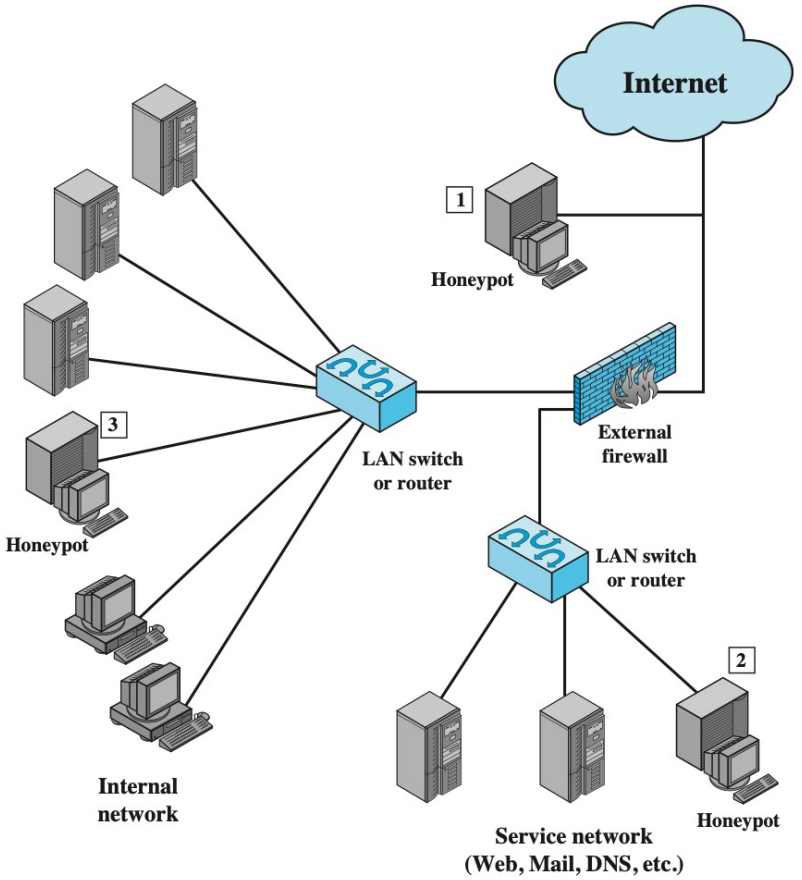


Figure 8.8 Example of Honeypot Deployment

Summary

- Defense in depth
  - Layering method
- Firewall
  - Packet filtering
  - Stateful
  - Application proxy
  - Next generation
- Logging
  - SEM
  - SIEM
- Intrusion detection systems
  - Anomaly detection
  - Signature-based detection
- Intrusion prevention systems
- Honeypot

References

- [Textbook 1] Chapter 8 & 9
- [Textbook 2] Section 3