Week 9: Network Security Tools - Comprehensive Exam Notes

Table of Contents

---

1. Firewalls

Overview and Core Concepts

Definition: Firewalls are security tools that implement various mechanisms to protect networks by controlling traffic based on predefined rules. They belong to:

- **Access Control Policies**
- **Network Security Monitoring Policies**

Core Function: **Packet Filtering** - inspects incoming/outgoing packets based on predefined security rules, checking:

- IP addresses
- Port numbers
- Protocol types

Types of Firewalls

Feature	Network Firewall	Host-Based Firewall
Scope	Protects network/subnet	Protects single device
Placement	Network perimeter/gateway	Host operating system
Traffic Type	Between networks	To/from specific host
Administration	Centrally managed	Per-device management

Filtering Criteria and Rules

Key Filtering Parameters:

1. **IP Addresses**: Source and destination
   - Example: Only 192.168.1.0/24 permitted access
2. **Port Numbers**: Application/service identification
   - Example: Allow HTTPS (443), block HTTP (80)
3. **Protocol Types**: TCP, UDP, ICMP
   - Example: Deny UDP to limit streaming services

Rule Actions:

- **Allow**: Permit packet through
- **Deny/Block**: Reject or discard packet
- **Limit**: Restrict packet count of same type

Firewall Rule Syntax:

```
[ACTION] [PROTOCOL] [SOURCE IP/SUBNET] [SOURCE PORT] -> [DESTINATION IP/SUBNET] [DESTINATION PORT]
```

Direction Indicators:

- **Inbound**: Traffic entering host (destination IP = local IP)
  - `INBOUND ALLOW TCP ANY ANY -> 192.168.1.10 3389`
- **Outbound**: Traffic leaving host (source IP = local IP)
  - `OUTBOUND BLOCK UDP 192.168.1.10 ANY -> ANY 53`

Rate Limiting Rules:

```
LIMIT <Protocol> <Source IP> -> <Destination IP> <Port> <Flags> rate <Rate>
```

Example: `LIMIT TCP ANY -> 192.168.1.1 80 SYN rate 200/s`

Attack Scenarios and Firewall Responses

1. SYN Flood Attack

Mechanism: Attacker sends many SYN requests without completing TCP handshake, consuming server resources with half-open connections.

TCP Handshake Process:

1. Client → Server: SYN
2. Server → Client: SYN-ACK
3. Client → Server: ACK (never sent in attack)

Firewall Countermeasures:

- Rate limiting: `LIMIT TCP ANY -> <Host IP> 80 SYN rate 50/s`
- Block known sources: `DENY TCP <Malicious IP> -> <Host IP> 80 SYN`

2. UDP Flooding (Amplification Attack)

Mechanism:

1. Attacker sends small UDP packets to servers
2. Spoofs source IP to victim's address
3. Server responds with larger payload to victim
4. Victim gets overwhelmed with amplified responses

Firewall Countermeasures:

- Limit DNS traffic: `LIMIT UDP ANY -> 192.168.1.100 53 rate 10/s`
- Drop unnecessary services: `DROP UDP ANY -> 192.168.1.100 123`
- Block large responses: `DENY UDP 192.168.1.100 -> ANY 53 size > 512`

3. ICMP Attacks

Types:

- **ICMP Flooding**: High volume of ping requests
- **Ping of Death**: Oversized ICMP packets causing crashes

Firewall Countermeasures:

- Rate limiting: `LIMIT ICMP ANY -> 192.168.1.100 echo-request rate 1/s`
- Complete blocking: `DENY ICMP ANY -> 192.168.1.100 echo-request`
- Size limiting: `LIMIT ICMP ANY -> ANY echo-request length 1000-65535`

Firewall Operation Layers

1. Internet Layer (Layer 3)

- Protocols: IP, ICMP

- Function: Filters based on IP addresses and network protocols

2. Transport Layer (Layer 4)

- Protocols: TCP, UDP
- Function: Filters based on port numbers and transport protocols

Stateless vs Stateful Firewalls

Stateless Firewall:

- Inspects each packet individually
- No connection state tracking
- Cannot distinguish legitimate session packets
- Treats each packet independently
- **Limitation**: Cannot track TCP handshake process

DMZ (Demilitarized Zone) Networks

Architecture:

- **External Firewall**: Edge of network
- **DMZ**: Between external and internal firewalls
- **Internal Firewall(s)**: Protect internal network

Internal Firewall Purposes:

1. More stringent filtering capability
2. Two-way DMZ protection
3. Segment internal network protection

---

2. Intrusion Detection and Prevention Systems

Intrusion Detection Systems (IDS)

Definition: Passive monitoring tools that detect suspicious behavior, policy violations, or unauthorized access without actively stopping threats.

Types:

- **Network-based IDS (NIDS)**: Monitors network traffic
- **Host-based IDS (HIDS)**: Monitors individual device activities

Detection Approaches

1. Misuse Detection (Signature-Based)

Mechanism: Uses rules specifying system events/sequences symptomatic of security incidents

- Operates on attack pattern databases (signatures)
- Uses pattern-matching algorithms

Advantages:

- High accuracy
- Few false alarms

Disadvantages:

- Cannot detect novel/unknown attacks
- Requires constant signature updates

2. Anomaly Detection

Mechanism: Searches for activity differing from normal behavior patterns

- Profiles normal system behavior
- Flags significant deviations

Advantages:

- Can detect previously unknown attacks
- Behavioral analysis capability

Disadvantages:

- High false positive/negative trade-off
- Requires extensive baseline training

Intrusion Prevention Systems (IPS)

Definition: Extends IDS functionality by actively blocking malicious activities in real-time

- Operates in-line with network traffic
- Can drop packets, reset connections, block access

Key Difference: IPS has firewall functions but uses pattern-based threat identification rather than firewall rules

IPS Application: SQL Injection Prevention

SQL Injection Attack: Malicious SQL queries inserted into input fields to manipulate backend databases

IPS Response:

1. **Detection**: Identifies malicious SQL patterns in payload (e.g., "OR 1=1")
2. **Prevention**: Blocks query or terminates connection before database access

---

3. Malware Defense

Malware Definition (NIST SP 800-83)

"A program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system."

Common Malware Types

- **Virus**: Self-replicating code
- **Worm**: Network-spreading malware
- **Trojan Horse**: Disguised malicious software
- **Spyware**: Information gathering malware
- **Rootkit**: System-level hiding malware
- **Backdoor**: Unauthorized access mechanism
- **Bot**: Remotely controlled malware
- **Ransomware**: Data encryption for extortion

Defense Strategies

1. Network Traffic Analysis

Techniques:

- **Misuse Detection**: Signature-based (e.g., DDoS traffic surge detection)
- **Anomaly Detection**: Profile-based deviation analysis
- **Example**: Anomalous DNS traffic indicates botnet activity

2. Payload Analysis

Methods:

- **Signature Detection**: Known malicious payload identification
- **Anomaly Detection**: Suspicious payload pattern recognition
- **Sandbox Environment**: Quarantine and behavioral analysis

3. Endpoint Behavior Analysis

Components:

- **Antivirus Software**: Signature and anomaly detection
- **Application Whitelisting**: Restrict to known good applications
- **Application Containers**: Virtual isolation for damage prevention

Incident Management

Key Elements:

- Data collection and aggregation
- Data normalization and correlation
- Alerting and reporting/compliance
- Detection, assessment, response, and learning processes

Digital Forensics (NIST SP 800-96)

Definition: Identification, collection, examination, and analysis of data while preserving integrity and maintaining chain of custody

Key Questions:

- What happened?
- When did events occur?
- In what order?
- What was the cause?
- Who caused the events?
- What enabled the events?
- What was affected and to what extent?

---

4. WEP/WPA Security Analysis

RC4 Cipher Overview

Process:

- Pseudo-random number generator produces keystream
- Plaintext XOR keystream = Ciphertext
- Same process for decryption: Ciphertext XOR keystream = Plaintext

WEP Vulnerabilities

1. IV Reuse Problem

Issues:

- Same shared key used bidirectionally
- IV often resets to 0 on initialization
- Only 2^24 (16 million) possible IVs
- Collision after ~5000 packets (Birthday Paradox)
- Busy AP (1000 packets/sec) = collision every 5 seconds

2. Keystream Reuse Attack

Mechanism:

- If two ciphertexts use same IV: $C_1 \oplus C_2 = P_1 \oplus P_2$
- XOR of plaintexts may reveal both messages
- Eavesdropper can decrypt without knowing key

3. Spoofed Packet Injection

Process:

1. Learn RC4(K, IV) from keystream reuse
2. Create valid ciphertexts using unkeyed checksum
3. Inject forged traffic accepted by receiver

4. Modification Attacks

CRC-32 Linearity: $crc(P \oplus P') = crc(P) \oplus crc(P')$

- Attacker can modify message while maintaining valid checksum
- Unkeyed integrity check allows manipulation

WPA Security Improvements

1. TKIP (Temporal Key Integrity Protocol)

Enhancements:

- 48-bit IV (vs 24-bit in WEP)
- Key mixing: TK (Temporal Key) + TA (Transmitter Address) + TSC (TKIP Sequence Counter)
- Dynamic key generation: TK = KeyGen(PMK from 802.1x)
- Per-packet key: IV||Key = Mix(Mix(TK, TA, TSC), TSC)

2. Keyed Integrity Check

MIC (Message Integrity Check):

- ICV = MIC(TA, DA, TEXT, MIC-key)
- Keyed checksum prevents modification attacks
- Ciphertext = RC4(IV||Key)[TEXT||ICV]

3. 802.1x Authentication

- Replaces static key sharing
- Multiple authentication schemes available
- Dynamic key distribution

WPA vs 802.11i Relationship

- **WPA**: Subset of 802.11i using TKIP with RC4
- **802.11i**: Full standard including AES support
- **WPA2**: Implements full 802.11i with AES

---

5. Hands-on Tasks

Task 1: Wireshark Network Analysis

Objective: Analyze network traffic for security threats

Steps:

1. Capture network traffic during normal operation
2. Identify different protocol types (TCP, UDP, ICMP)
3. Look for suspicious patterns:
    - Unusual port usage
    - High volume from single source
    - Malformed packets
4. Create filters for specific attack patterns

Task 2: Firewall Rule Configuration

Objective: Create firewall rules for common attack scenarios

Exercise A - SYN Flood Protection:

```
# Rate limit SYN packets
LIMIT TCP ANY -> 192.168.1.100 80 SYN rate 50/s

# Block known malicious sources
DENY TCP 10.0.0.0/8 -> 192.168.1.100 80 SYN
```

Exercise B - ICMP Flood Protection:

```
# Limit ping requests
LIMIT ICMP ANY -> 192.168.1.100 echo-request rate 1/s

# Block oversized ICMP packets
LIMIT ICMP ANY -> ANY echo-request length 1000-65535
```

Task 3: OpenSSL Certificate Analysis

Objective: Examine SSL/TLS certificates for security issues

Commands:

bash

```
# View certificate details
openssl x509 -in certificate.crt -text -noout

# Check certificate chain
openssl verify -CAfile ca.crt certificate.crt

# Test SSL connection
openssl s_client -connect example.com:443
```

Task 4: Malware Sandbox Analysis

Objective: Analyze suspicious files in isolated environment

Process:

1. Set up isolated virtual environment
2. Monitor file system changes
3. Analyze network connections
4. Document behavioral patterns
5. Generate threat report

---

6. Practice Questions

Multiple Choice Questions

1. Which layer does a firewall primarily operate at? a) Physical Layer b) Internet Layer and Transport Layer c) Application Layer d) Session Layer

Answer: b) Internet Layer and Transport Layer

2. What is the main difference between IDS and IPS? a) IDS is hardware-based, IPS is software-based b) IDS only monitors, IPS actively blocks threats c) IDS is faster than IPS d) IDS works at network level, IPS at host level

Answer: b) IDS only monitors, IPS actively blocks threats

3. In a SYN flood attack, what happens during the TCP handshake? a) The attacker sends ACK without SYN b) The server never sends SYN-ACK c) The attacker sends SYN but never sends final ACK d) The connection completes normally

Answer: c) The attacker sends SYN but never sends final ACK

Fill-in-the-Blanks

1. WEP uses a ___-bit IV, while WPA uses a ___-bit IV. Answer: 24, 48

2. The two main approaches to intrusion detection are ______ detection and ______ detection. Answer: misuse, anomaly

3. In firewall rules, ______ traffic means packets entering the host, while ______ traffic means packets leaving the host. Answer: inbound, outbound

Short Answer Questions

1. Explain why IV reuse is a critical vulnerability in WEP. Answer: IV reuse allows attackers to perform keystream reuse attacks. When the same IV is used with the same key, it produces identical keystream. If two ciphertexts use the same keystream, their XOR reveals the XOR of the original plaintexts ($C_1 \oplus C_2 = P_1 \oplus P_2$), potentially revealing both messages without knowing the key.

2. What are the three main purposes of internal firewalls in a DMZ architecture? Answer:

1. Provide more stringent filtering capability than external firewall
2. Provide two-way protection with respect to the DMZ
3. Enable multiple internal firewalls to protect different portions of the internal network from each other

3. How does an IPS prevent SQL injection attacks? Answer: IPS prevents SQL injection by detecting malicious SQL patterns in network traffic payload (signature-based detection) and immediately blocking the query or terminating the connection before it reaches the backend database. It looks for suspicious strings like "OR 1=1" and other SQL injection indicators.

Practical Scenarios

Scenario 1: Your network is experiencing a high volume of ICMP echo requests. Write appropriate firewall rules to mitigate this attack.

Solution:

```
# Rate limit ICMP requests to 1 per second
LIMIT ICMP ANY -> 192.168.1.100 echo-request rate 1/s

# Block oversized ICMP packets (Ping of Death protection)
LIMIT ICMP ANY -> ANY echo-request length 1000-65535

# Alternative: Completely block ICMP if not needed
DENY ICMP ANY -> 192.168.1.100 echo-request
```

Scenario 2: Analyze the security differences between WEP and WPA implementations.

Solution: WPA improvements over WEP:

- **Encryption**: TKIP with 48-bit IV vs 24-bit IV in WEP
- **Key Management**: Dynamic key mixing vs static key in WEP
- **Integrity**: Keyed MIC vs unkeyed CRC-32 in WEP
- **Authentication**: 802.1x support vs shared key authentication in WEP

---

7. Extended Practice Questions & Assessments

Multiple Choice Questions (MCQs)

Network Security Tools - Core Concepts

1. What is the primary difference between a stateless and stateful firewall? a) Stateless firewalls are faster b) Stateful firewalls track connection state and context c) Stateless firewalls are more secure d) Stateful firewalls only work with TCP

Answer: b) Stateful firewalls track connection state and context

2. Which of the following is NOT a typical firewall filtering criterion? a) Source IP address b) Destination port number c) File content d) Protocol type

Answer: c) File content

3. In a SYN flood attack, what resource is primarily consumed on the target server? a) CPU cycles b) Memory for half-open connections c) Disk space d) Network bandwidth

Answer: b) Memory for half-open connections

4. What does the "LIMIT" action in firewall rules accomplish? a) Blocks all traffic b) Allows unlimited traffic c) Restricts the number of packets per time unit d) Logs all traffic

Answer: c) Restricts the number of packets per time unit

5. Which attack exploits the stateless nature of UDP? a) SYN flood b) UDP amplification attack c) TCP hijacking d) ARP spoofing

Answer: b) UDP amplification attack

Intrusion Detection/Prevention Systems

6. What is the main advantage of anomaly detection over misuse detection? a) Fewer false positives b) Faster processing c) Can detect previously unknown attacks d) Requires less computational resources

Answer: c) Can detect previously unknown attacks

7. An IPS differs from an IDS primarily because it: a) Is hardware-based b) Actively blocks threats in real-time c) Only monitors network traffic d) Uses different detection algorithms

Answer: b) Actively blocks threats in real-time

8. Which detection method would be most effective against a zero-day attack? a) Signature-based detection b) Anomaly detection c) Rule-based detection d) Pattern matching

Answer: b) Anomaly detection

WEP/WPA Security

9. What is the main vulnerability that WEP's 24-bit IV creates? a) Too much encryption overhead b) IV collisions occur frequently c) Key exchange is insecure d) Authentication is weak

Answer: b) IV collisions occur frequently

10. Why can attackers decrypt WEP traffic without knowing the key? a) WEP uses weak algorithms b) IV reuse allows keystream reuse attacks c) WEP doesn't use encryption d) The key is transmitted in plaintext

Answer: b) IV reuse allows keystream reuse attacks

11. What improvement does WPA's TKIP provide over WEP? a) Uses AES encryption b) 48-bit IV and key mixing c) Eliminates the need for keys d) Provides perfect forward secrecy

Answer: b) 48-bit IV and key mixing

12. Which authentication framework does WPA utilize? a) RADIUS b) Kerberos c) 802.1x d) LDAP

Answer: c) 802.1x

Short Answer Questions (SAQs)

Firewall Concepts

1. Explain the difference between inbound and outbound firewall rules. Provide examples.

Answer: Inbound rules control traffic entering the host (destination IP matches local IP), while outbound rules control traffic leaving the host (source IP matches local IP).

- Inbound example: `INBOUND ALLOW TCP ANY ANY -> 192.168.1.10 3389` (allows RDP to host)

- Outbound example: `OUTBOUND BLOCK UDP 192.168.1.10 ANY -> ANY 53` (blocks DNS queries from host)

2. What are the three main purposes of internal firewalls in a DMZ architecture?

Answer:

1. Provide more stringent filtering capability than external firewall
2. Provide two-way protection with respect to the DMZ
3. Enable segmentation of internal network portions from each other

3. Why is rate limiting important in firewall configurations?

Answer: Rate limiting prevents DoS attacks by restricting the number of packets per time unit. It allows legitimate traffic while blocking excessive requests that could overwhelm system resources, such as SYN floods or ICMP floods.

IDS/IPS Systems

4. Compare and contrast misuse detection and anomaly detection approaches in IDS.

Answer:

- **Misuse Detection**: Uses predefined signatures/patterns; high accuracy, low false positives; cannot detect unknown attacks
- **Anomaly Detection**: Compares against normal behavior baseline; can detect unknown attacks; higher false positive rate; requires extensive training period

5. How does an IPS prevent SQL injection attacks?

Answer: IPS prevents SQL injection by analyzing payload content in real-time, detecting malicious SQL patterns (like "OR 1=1", "UNION SELECT"), and immediately blocking the malicious query or terminating the connection before it reaches the database.

6. What is the significance of operating "in-line" for an IPS?

Answer: Operating in-line means the IPS sits directly in the network path, allowing it to inspect and block malicious traffic in real-time. This enables active prevention rather than just detection and alerting.

WEP/WPA Security

7. Explain the keystream reuse vulnerability in WEP and how it can be exploited.

Answer: When two packets use the same IV with the same key, they produce identical keystreams. If $C_1 = P_1 \oplus Z$ and $C_2 = P_2 \oplus Z$ (same keystream Z), then $C_1 \oplus C_2 = P_1 \oplus P_2$. This XOR of plaintexts may reveal both original messages without knowing the key.

8. How does WPA's key mixing mechanism improve security over WEP?

Answer: WPA uses dynamic key mixing combining Temporal Key (TK), Transmitter Address (TA), and TKIP Sequence Counter (TSC). This creates unique per-packet keys: IV||Key = Mix(Mix(TK, TA, TSC), TSC), preventing keystream reuse even if IVs repeat.

9. Why is MIC (Message Integrity Check) more secure than CRC-32 in WEP?

Answer: MIC uses a keyed integrity check (ICV = MIC(TA, DA, TEXT, MIC-key)) while CRC-32 is unkeyed. The linear property of CRC-32 allows attackers to modify messages while maintaining valid checksums, whereas MIC prevents unauthorized modifications.

Evaluation Questions

1. Evaluate the effectiveness of stateless firewalls in modern network security environments.

Answer: Stateless firewalls have limited effectiveness in modern environments because:

- **Limitations**: Cannot track connection state, treat packets independently, vulnerable to session-based attacks
- **Advantages**: Fast processing, simple configuration, low resource usage
- **Modern relevance**: Suitable for basic filtering but inadequate against sophisticated attacks requiring context awareness
- **Recommendation**: Should be combined with stateful inspection and application-layer filtering

2. Assess the trade-offs between signature-based and anomaly-based intrusion detection systems.

Answer: **Signature-based advantages**: High accuracy, low false positives, immediate detection of known threats, easier to tune **Signature-based disadvantages**: Cannot detect zero-day attacks, requires constant updates, limited to known patterns

Anomaly-based advantages: Detects unknown attacks, adaptive to new threats, comprehensive behavioral analysis **Anomaly-based disadvantages**: High false positive rate, requires extensive training, computationally intensive

Optimal approach: Hybrid systems combining both methods for comprehensive coverage

3. Evaluate the security improvements that WPA provides over WEP, considering both strengths and remaining vulnerabilities.

Answer: **WPA Improvements**:

- TKIP with 48-bit IV reduces collision probability
- Key mixing provides per-packet key uniqueness
- MIC prevents message modification attacks
- 802.1x provides better authentication

Remaining Vulnerabilities:

- Still uses RC4 (though more securely)
- TKIP has known cryptographic weaknesses
- Vulnerable to dictionary attacks on weak passphrases
- Michael attack against MIC

Overall Assessment: Significant improvement over WEP but not perfect; WPA2 with AES addresses most remaining issues

Comparison Questions

1. Compare Network-based IDS (NIDS) and Host-based IDS (HIDS) in terms of deployment, capabilities, and limitations.

Answer:

Aspect	NIDS	HIDS
Deployment	Network perimeter/segments	Individual hosts
Visibility	Network traffic patterns	System calls, file changes
Scalability	High (monitors multiple hosts)	Low (per-host deployment)
Encrypted Traffic	Limited visibility	Can monitor before encryption
Resource Impact	Minimal on endpoints	Moderate on host performance
Attack Detection	Network-based attacks	Host-specific attacks
Management	Centralized	Distributed

2. Compare the security architectures of WEP and WPA, highlighting key differences in encryption, authentication, and integrity protection.

Answer:

Component	WEP	WPA
Encryption	RC4 with 24-bit IV	RC4 with 48-bit IV + TKIP
Key Management	Static shared key	Dynamic key mixing
Authentication	Shared key authentication	802.1x framework
Integrity	CRC-32 (unkeyed)	MIC (keyed)
Key Derivation	Simple concatenation	Complex mixing function
Vulnerability	IV reuse, keystream reuse	Reduced but not eliminated

3. Compare stateless and stateful firewall architectures in terms of security effectiveness, performance, and complexity.

Answer:

Aspect	Stateless	Stateful
Security	Basic packet filtering	Context-aware filtering
Performance	Fast processing	Moderate overhead
Complexity	Simple configuration	Complex rule management
Memory Usage	Low	High (connection tracking)
Attack Resistance	Vulnerable to session attacks	Better session protection
Scalability	High	Limited by state table size

Recommendation Questions

1. A company is experiencing frequent DDoS attacks. Recommend a comprehensive firewall strategy including specific rules and configurations.

Answer: **Recommended Strategy**:

1. **Rate Limiting Rules**:

   ```
   LIMIT TCP ANY -> SERVER_IP 80 SYN rate 100/s
   LIMIT ICMP ANY -> SERVER_IP echo-request rate 5/s
   LIMIT UDP ANY -> SERVER_IP 53 rate 50/s
   ```

2. **Geo-blocking**: Block traffic from suspicious geographic regions
3. **DDoS Protection Services**: Implement cloud-based DDoS mitigation
4. **Network Segmentation**: Use DMZ architecture with multiple firewall layers
5. **Monitoring**: Deploy IPS with anomaly detection for traffic pattern analysis

6. **Incident Response**: Automated blocking of attack sources

2. An organization wants to migrate from WEP to a more secure wireless solution. Provide detailed recommendations considering current security standards.

Answer: **Immediate Recommendations**:

1. **Upgrade to WPA3**: Latest standard with individualized data encryption
2. **Enterprise Authentication**: Implement 802.1x with RADIUS server
3. **Strong Passphrases**: Minimum 12 characters with complexity requirements
4. **Network Segmentation**: Separate guest and corporate networks
5. **Regular Updates**: Maintain firmware and security patches
6. **Monitoring**: Deploy wireless IDS for anomaly detection

Migration Plan:

- Phase 1: Upgrade infrastructure to support WPA3
- Phase 2: Implement 802.1x authentication
- Phase 3: Deploy monitoring and segmentation
- Phase 4: User training and policy enforcement

3. Design a layered security architecture for a medium-sized enterprise network, incorporating firewalls, IDS/IPS, and malware defense.

Answer: **Layered Security Architecture**:

Perimeter Layer:

- External firewall with DDoS protection
- IPS with signature and anomaly detection
- Web application firewall (WAF)

DMZ Layer:

- DMZ hosting public services
- Internal firewall with strict rules
- Network segmentation

Internal Network:

- Host-based firewalls on endpoints

- HIDS on critical servers
- Antivirus with behavioral analysis

Endpoint Layer:

- Application whitelisting
- Endpoint detection and response (EDR)
- Regular security updates

Management Layer:

- Centralized logging and monitoring
- Security information and event management (SIEM)
- Incident response procedures

Summary Key Points

1. **Firewalls** operate at Internet and Transport layers, filtering traffic based on IP addresses, ports, and protocols
2. **IDS** monitors and detects threats passively, while **IPS** actively blocks threats
3. **Malware defense** requires layered approach: network analysis, payload analysis, and endpoint protection
4. **WEP vulnerabilities** stem from IV reuse and unkeyed integrity checks
5. **WPA** addresses WEP weaknesses through TKIP, keyed integrity, and 802.1x authentication
6. **DMZ architecture** provides layered network protection with external and internal firewalls
7. **Rate limiting** is crucial for preventing DoS attacks at the firewall level