Lecture Six

# Security in Network Operating Systems

Protecting Resources, Data, and Communication

Dr. Tarfa Yaseen Hamed

Department of Networks

College of Computer Science and Mathematics

University of Mosul

2025

# Introduction to NOS Security

- **Why Security Matters in NOS**:
  - **Protects Resources**: Ensures that network resources (e.g., files, printers, applications) are accessible only to authorized users.
  - **Safeguards Data**: Prevents unauthorized access, modification, or theft of sensitive data.
  - **Ensures Availability**: Protects against attacks that could disrupt network services (e.g., Denial-of-Service attacks).

# Key Security Goals (CIA Triad)

- **Confidentiality**: Ensuring that data is accessible only to authorized users.
- **Integrity**: Protecting data from unauthorized modification or corruption.
- **Availability**: Ensuring that network resources are accessible when needed.

# Common Threats to NOS

- **Unauthorized Access**: Hackers gaining access to sensitive data or systems.
- **Malware**: Viruses, worms, and ransomware that disrupt operations.
- **Denial-of-Service (DoS) Attacks**: Overloading the network to make it unavailable.
- **Insider Threats**: Malicious or negligent actions by employees or users.

# Key Security Challenges in NOS

1. **Scalability**:

- **Definition**: Ensuring security measures can handle the growth of the network (e.g., more users, devices, and data).
- **Challenges**:
  - Managing security policies across large, distributed networks.
  - Ensuring consistent protection as the network expands.

# Key Security Challenges in NOS (cont.)

2. **Complexity**:

- **Definition**: Managing diverse devices, protocols, and applications in a networked environment.
- **Challenges**:
  - Integrating security across heterogeneous systems (e.g., Windows, Linux, IoT devices).
  - Balancing usability and security.

# Key Security Challenges in NOS (cont.)

## 3. Emerging Threats:

- **Definition**: New and evolving threats that exploit vulnerabilities in NOS.
- **Examples**:
  - **Zero-Day Exploits**: Attacks targeting unknown vulnerabilities.
  - **Ransomware**: Malware that encrypts data and demands payment.
  - **Advanced Persistent Threats (APTs)**: Long-term, targeted attacks by skilled adversaries.

# Key Security Challenges in NOS (cont.)

4. **Insider Threats**:

- **Definition**: Security risks posed by employees, contractors, or other trusted individuals.
- **Types**:
  - **Malicious Insiders**: Deliberate sabotage or data theft.
  - **Negligent Insiders**: Accidental exposure of sensitive data.

# Key Security Challenges in NOS (cont.)

5. **Resource Constraints**:

- **Definition**: Limited budget, personnel, or tools for implementing robust security measures.
- **Challenges**:
  - Prioritizing security investments.
  - Training staff to handle security incidents.

# Authentication and Authorization in NOS

1. **Authentication**:

- **Definition**: The process of verifying the identity of a user, device, or system.
- **Purpose**: Ensures that only legitimate users can access the network.
- **Methods**:
  - **Passwords**: Simple but vulnerable to brute-force attacks.
  - **Multi-Factor Authentication (MFA)**: Combines multiple verification methods (e.g., password + OTP).
  - **Biometrics**: Uses unique biological traits (e.g., fingerprints, facial recognition).

# Authentication and Authorization in NOS (cont.)

2. **Authorization**:

- **Definition**: The process of granting or denying access to resources based on user roles or permissions.
- **Purpose**: Ensures that users can only access resources they are permitted to use.
- **Methods**:
  - **Role-Based Access Control (RBAC)**: Assigns permissions based on user roles (e.g., admin, user, guest).
  - **Access Control Lists (ACLs)**: Specifies which users or systems can access specific resources.

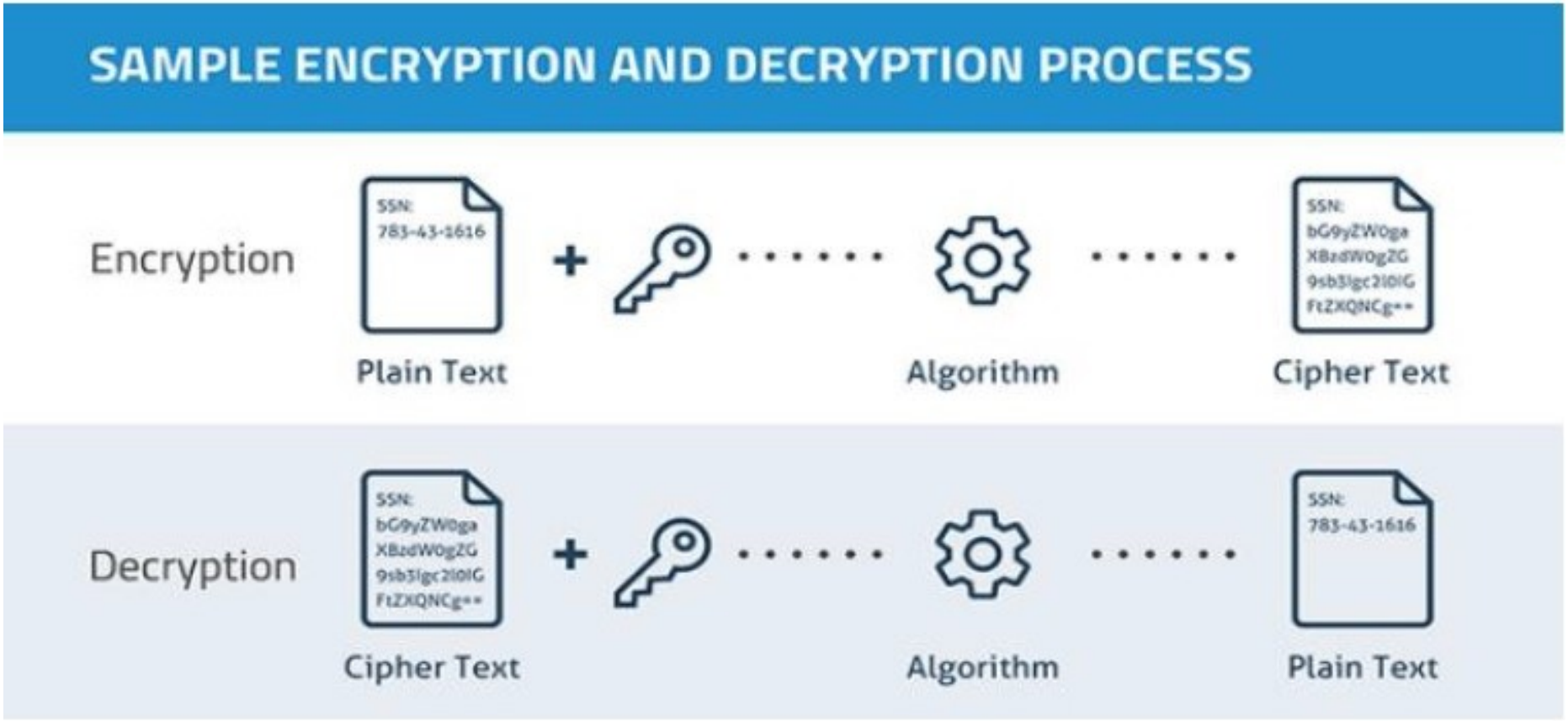
# Authentication and Authorization in NOS (cont.)

- **Importance of Authentication and Authorization**:
  - **Prevents Unauthorized Access**: Protects sensitive data and resources.
  - **Enhances Accountability**: Tracks user actions for auditing purposes.
  - **Supports Compliance**: Meets regulatory requirements (e.g., GDPR, HIPAA).
- **Examples in NOS**:
  - **Active Directory (Windows Server)**: Centralized authentication and authorization.
  - **Linux PAM (Pluggable Authentication Modules)**: Flexible authentication framework.

# Encryption Techniques in NOS

- **What is Encryption?**
- **Definition**: The process of converting plaintext into ciphertext to protect data from unauthorized access.
- **Purpose**:
  Ensures **confidentiality** and **integrity** of data during storage and transmission.

# Encryption and Decryption



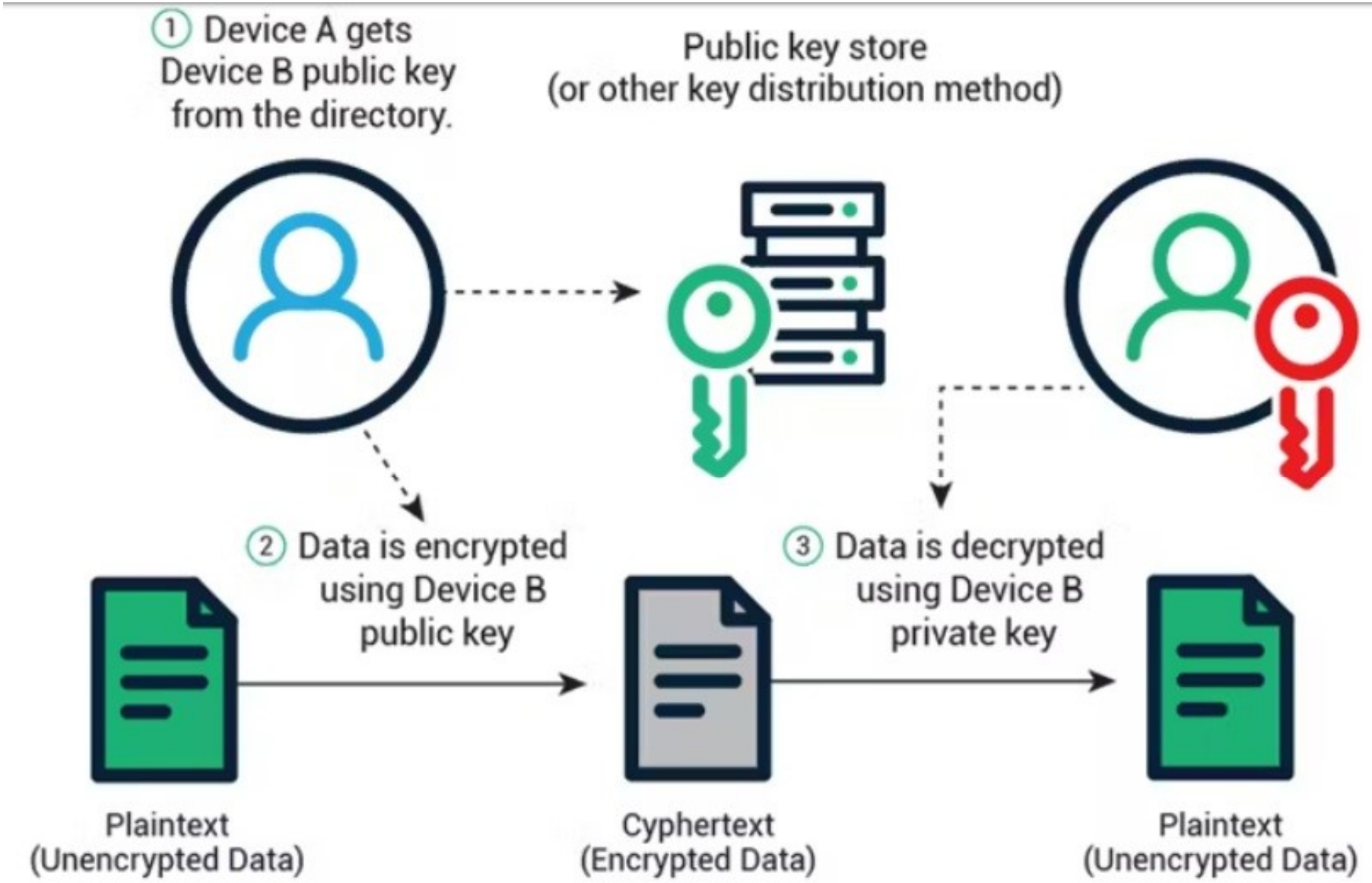
# Types of Encryption:

1. **Symmetric Encryption**:
   - Uses a **single key** for both encryption and decryption.
   - **Examples**: AES (Advanced Encryption Standard), DES (Data Encryption Standard).
   - **Pros**: Fast and efficient for large data volumes.
   - **Cons**: Key distribution can be challenging.


Symmetric Cryptography
Encryption
Decryption
Plain Text
Cipher Text
Plain Text

# Types of Encryption: (cont.)

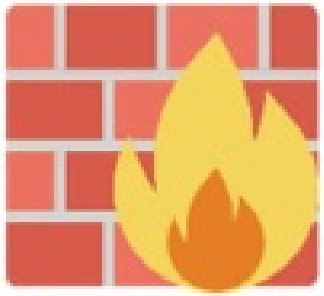
2. **Asymmetric Encryption**:
   - Uses a **pair of keys** (public and private) for encryption and decryption.
   - **Examples**: RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography).
   - **Pros**: Solves the key distribution problem.
   - **Cons**: Slower and computationally intensive.


1 Device A gets Device B public key from the directory.
Public key store (or other key distribution method)
2 Data is encrypted using Device B public key
3 Data is decrypted using Device B private key
Plaintext (Unencrypted Data)
Cyphertext (Encrypted Data)
Plaintext (Unencrypted Data)

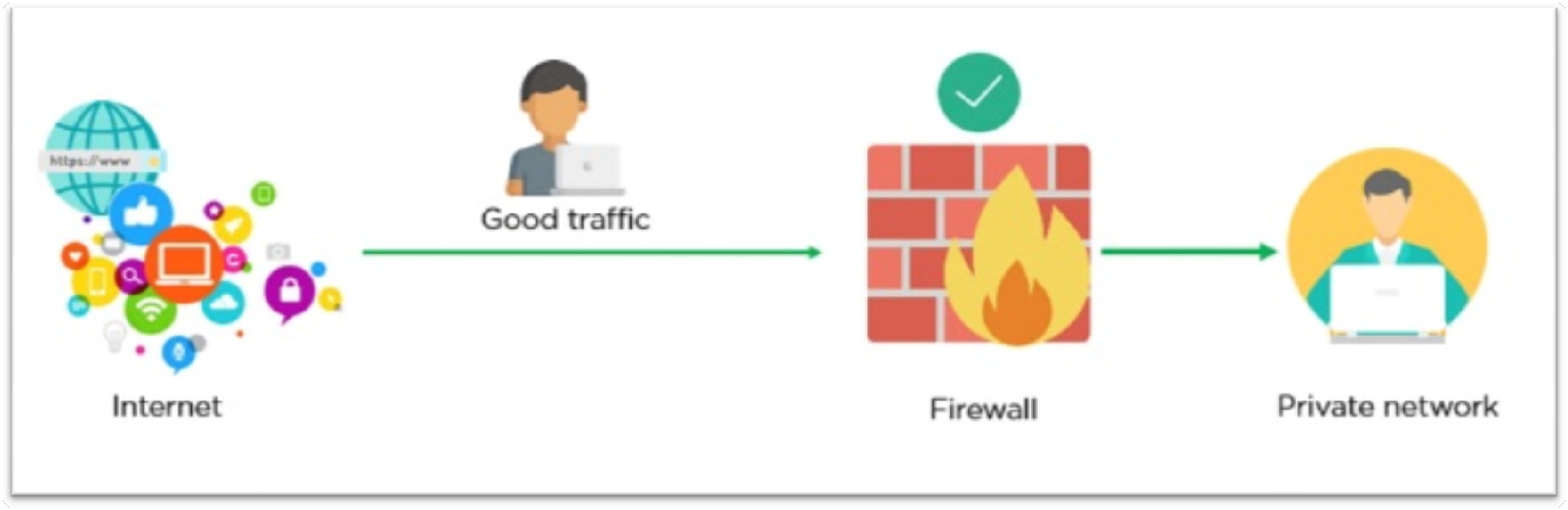
# **Applications of Encryption in NOS**:

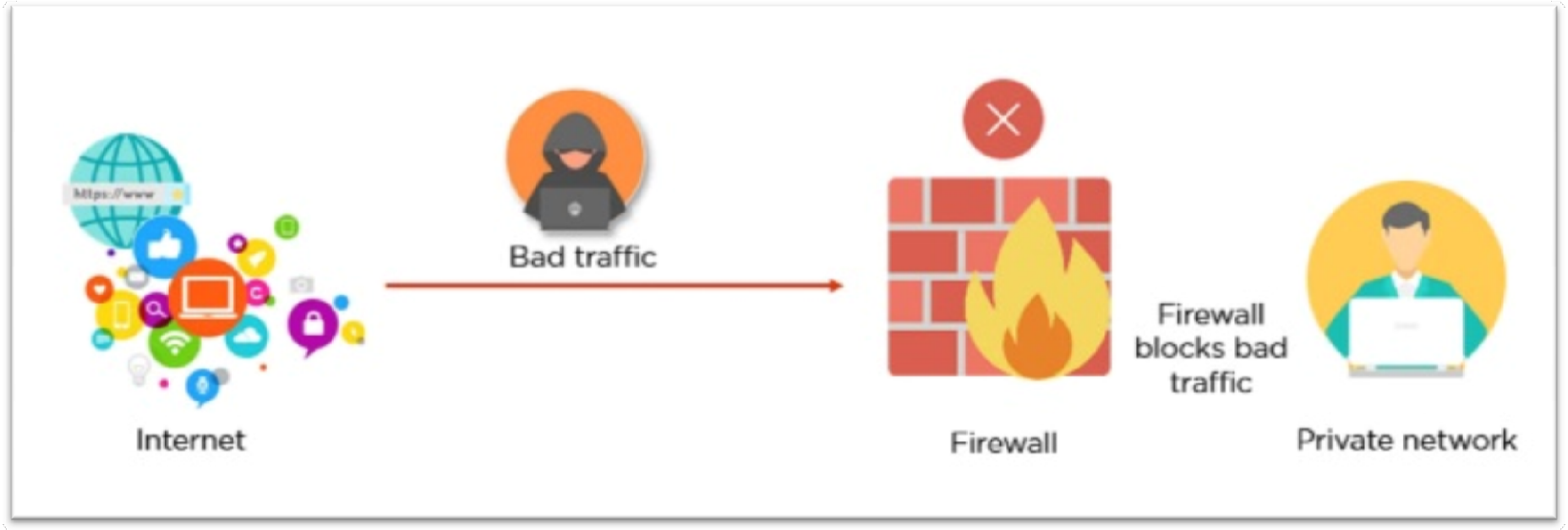
- **Data at Rest**: Encrypting files and databases stored on servers.
- **Data in Transit**: Securing communication over networks (e.g., SSL/TLS for HTTPS).
- **Authentication**: Verifying identities using digital certificates.

# Firewalls in NOS



- **What is a Firewall?**
- **Definition**: A network security device that monitors and controls incoming and outgoing traffic based on predefined security rules.
- **Purpose**: Acts as a barrier between a trusted internal network and untrusted external networks (e.g., the internet).


Internet
Good traffic
Firewall
Private network


Internet
Bad traffic
Firewall
Firewall blocks bad traffic
Private network

# Types of Firewalls:

1. **Packet Filtering Firewalls**:
   - Examines packets based on source/destination IP addresses, ports, and protocols.
   - **Pros**: Fast and efficient.
   - **Cons**: Limited ability to detect advanced threats.
2. **Stateful Inspection Firewalls**:
   - Tracks the state of active connections and makes decisions based on context.
   - **Pros**: More secure than packet filtering.
   - **Cons**: Slower due to additional processing.

# **Types of Firewalls**: (cont.)

3. **Proxy Firewalls**:
   - Acts as an intermediary between users and the internet, filtering traffic at the application layer.
   - **Pros**: Provides deep packet inspection and hides internal network details.
   - **Cons**: Can introduce latency.
4. **Next-Generation Firewalls (NGFW)**:
   - Combines traditional firewall features with advanced capabilities like intrusion prevention, deep packet inspection, and application awareness.
   - **Pros**: Highly effective against modern threats.
   - **Cons**: Expensive and complex to configure.

# How Firewalls Work:

- **Rule-Based Filtering**: Uses predefined rules to allow or block traffic.
- **Default Deny**: Blocks all traffic unless explicitly allowed.
- **Logging and Alerts**: Records traffic and notifies administrators of suspicious activity.

# Firewall Deployment in NOS:

- **Network Perimeter**: Protects the boundary between the internal network and the internet.
- **Internal Segmentation**: Divides the internal network into secure zones (e.g., separating finance and HR departments).
- **Host-Based Firewalls**: Installed on individual devices for additional protection.

# **Benefits of Firewalls** and **Challenges in Firewall Management**:

- **Benefits**
  - **Prevents Unauthorized Access**: Blocks malicious traffic.
  - **Protects Against Malware**: Filters out harmful content.
  - **Enhances Privacy**: Hides internal network details from external users.
- **Challenges**
  - **Complex Configuration:** Requires expertise to set up and maintain.
  - **False Positives/Negatives:** Legitimate traffic may be blocked, or malicious traffic may be allowed.
  - **Performance Impact:** Can slow down network traffic, especially with deep packet inspection.

# Intrusion Detection Systems (IDS) in NOS

- **What is an IDS?**
- **Definition**: A security tool that monitors network traffic or system activities for malicious behavior or policy violations.
- **Purpose**: Detects and alerts administrators about potential security breaches.

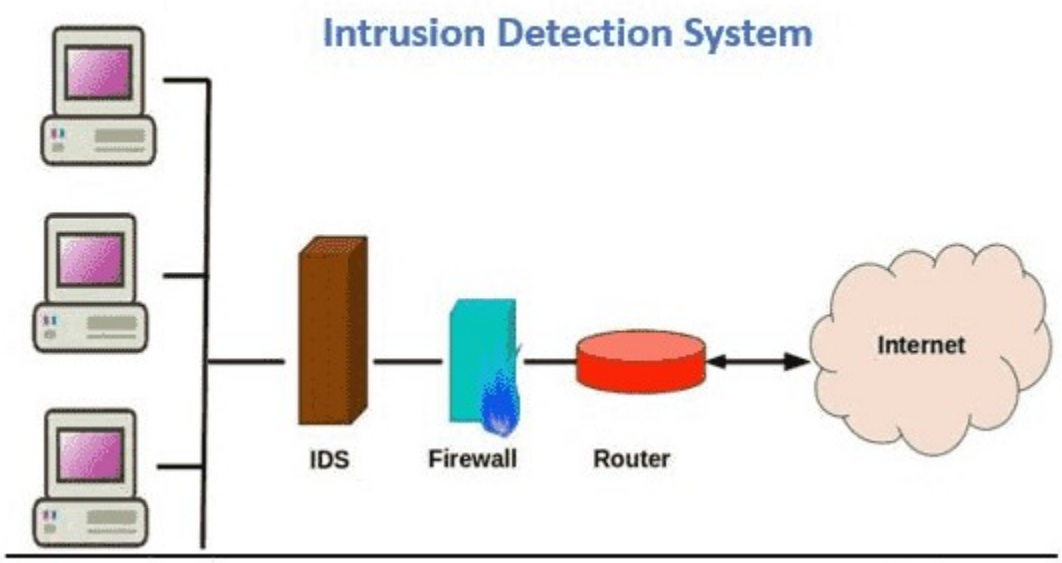
# Types of IDS:

1. **Network-Based IDS (NIDS)**:
   - Monitors network traffic for suspicious activity.
   - **Pros**: Can detect attacks targeting multiple systems.
   - **Cons**: May generate false positives.
2. **Host-Based IDS (HIDS)**:
   - Monitors activities on individual devices (e.g., servers, workstations).
   - **Pros**: Provides detailed insights into system-level events.
   - **Cons**: Limited to the host it is installed on.

# **Types of IDS**: (cont.)

3. **Signature-Based IDS**:
   - Detects known threats by matching patterns (signatures) in traffic or logs.
   - **Pros**: Effective against known attacks.
   - **Cons**: Cannot detect zero-day exploits.
4. **Anomaly-Based IDS**:
   - Detects unusual behavior by comparing current activities to a baseline.
   - **Pros**: Can detect unknown or zero-day attacks.
   - **Cons**: May generate false positives.

# How Firewalls and IDS Work Together




**Complementary Roles:**

- **Firewalls**: Focus on **prevention** by blocking unauthorized traffic.
- **IDS**: Focuses on **detection** by identifying suspicious activities that bypass the firewall.

# How Firewalls and IDS Work Together

- **Workflow:**
- **Traffic Filtering by Firewall**:
  - The firewall inspects incoming and outgoing traffic based on predefined rules.
  - It blocks traffic that violates the rules (e.g., traffic from blacklisted IP addresses or to unauthorized ports).
- **Traffic Monitoring by IDS**:
  - The IDS analyzes the traffic that passes through the firewall.
  - It looks for patterns or behaviors that indicate potential threats (e.g., unusual login attempts, malware signatures).
- **Alerting and Response**:
  - If the IDS detects suspicious activity, it sends an alert to the administrator.
  - The administrator can then take action, such as updating firewall rules to block the threat or investigating further.