What is Network Security?

- Critical aspect of managing any computer network to protect the confidentiality, integrity, and availability of information and resources on the network

- The primary goal is to prevent unauthorized access, misuse, modification, or denial of service

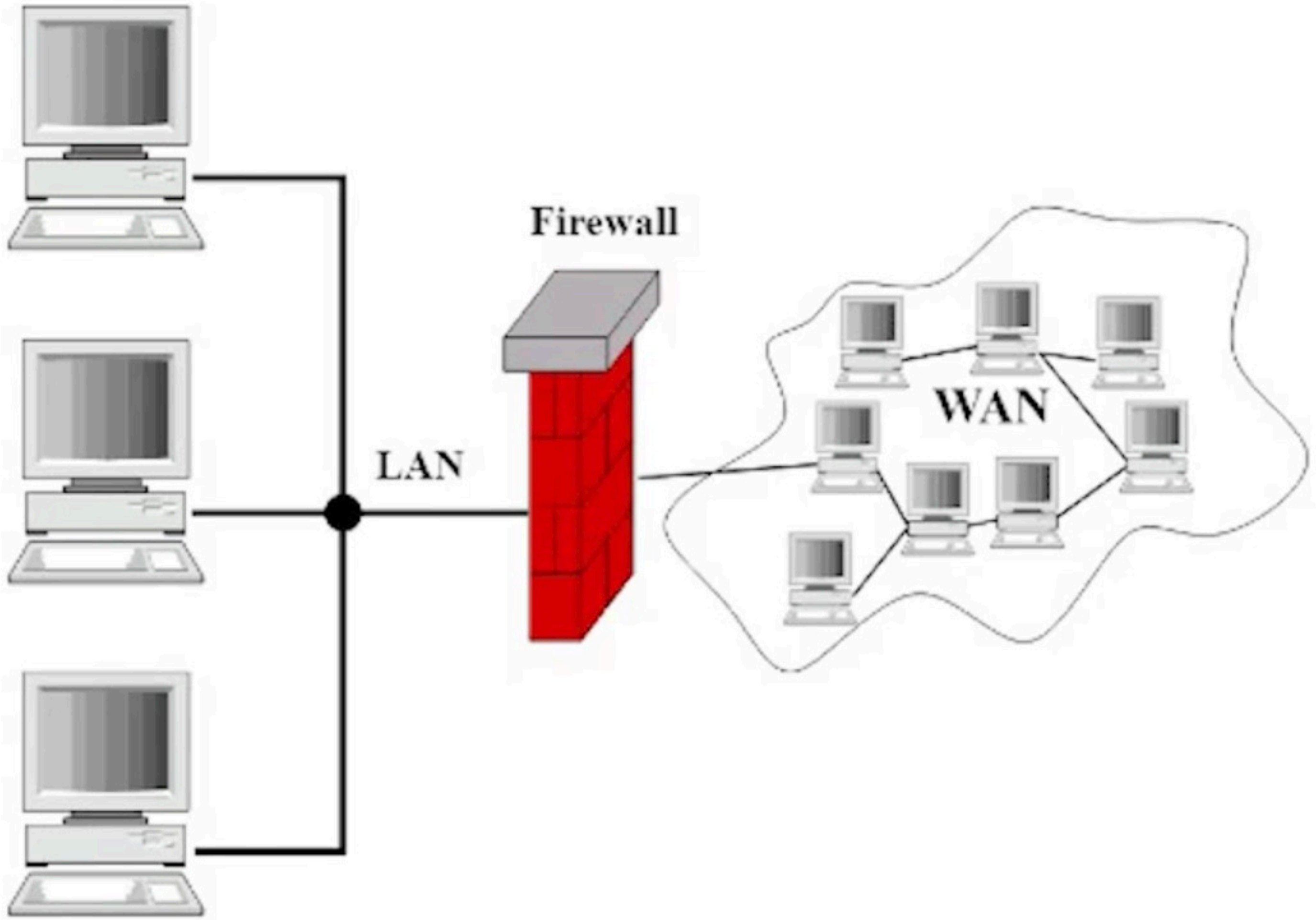
Basic Security Measures: Firewalls

What are Firewalls?

- Firewalls act as a barrier between your internal network and external networks, preventing unauthorized access and malicious traffic from entering your network

- They can be implemented as hardware devices, software applications, or a combination of both

- Common types of firewalls include:
  - Packet-Filtering Firewalls
  - Stateful Inspection Firewalls
  - Application-Layer Firewalls

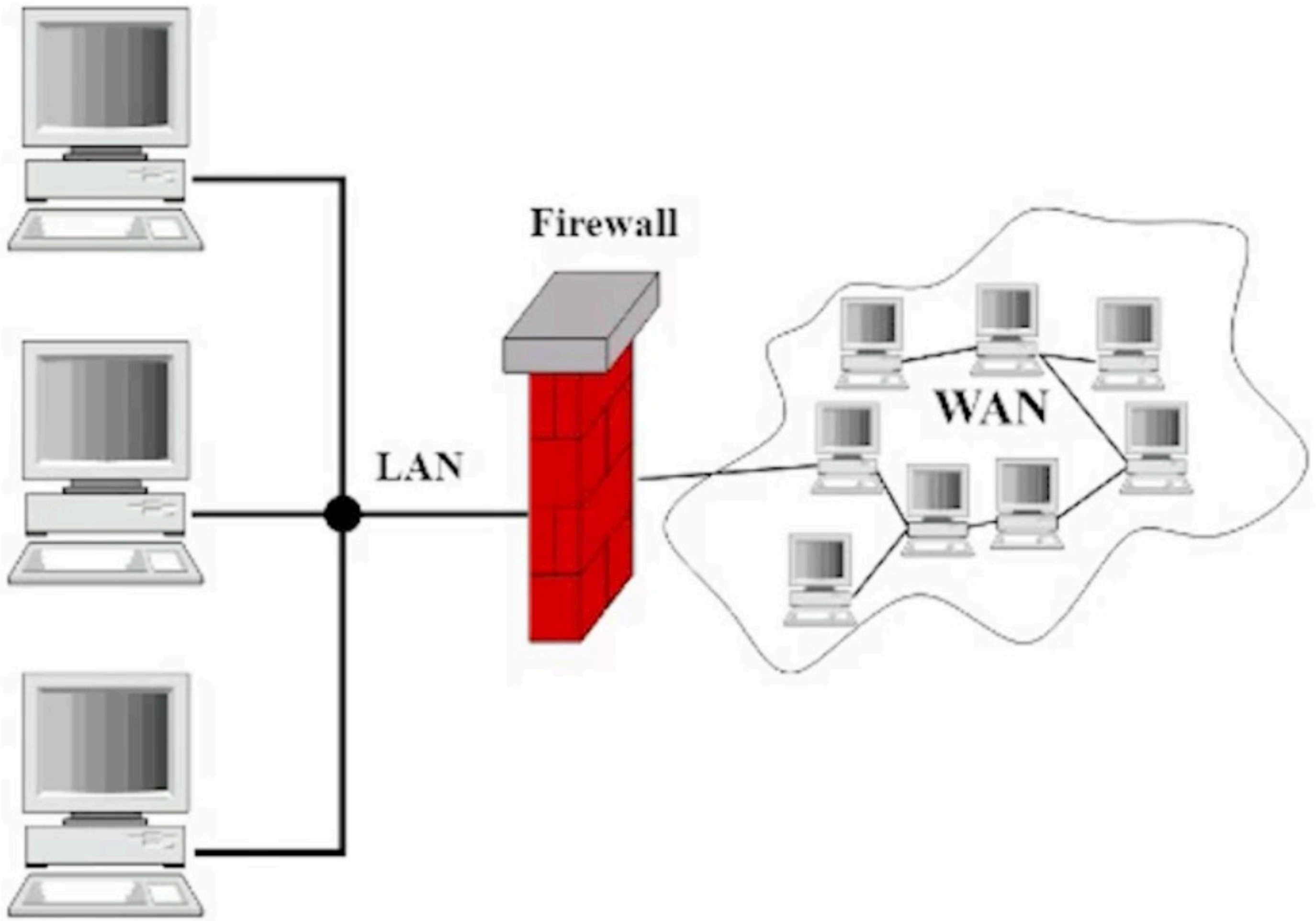


Basic Security Measures: Firewalls (Cont.)

Types of Firewalls and Their Functions:

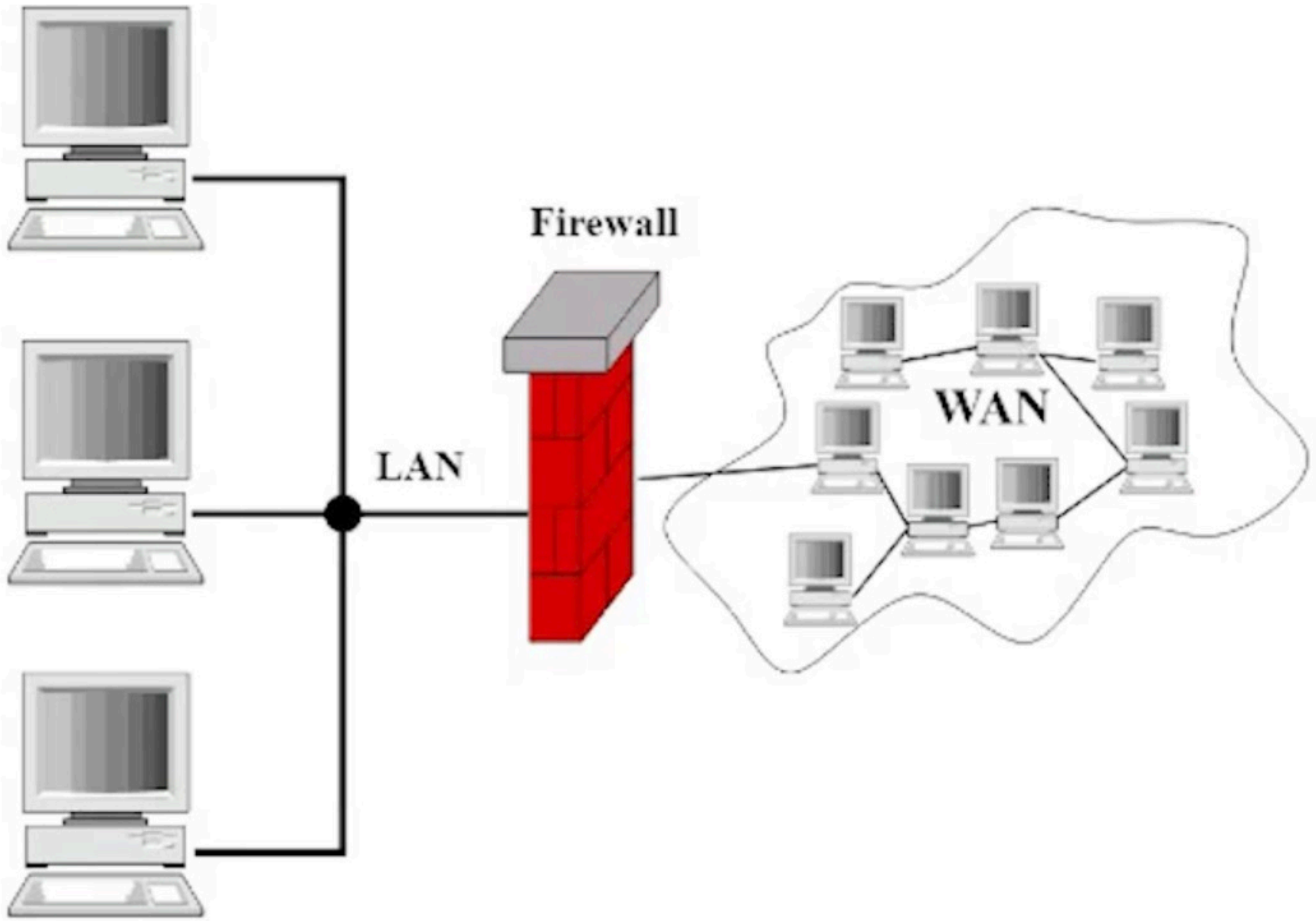
1. **Packet-Filtering Firewalls:**
   a. Operate at the network layer and examine packets based on information in their headers

   a. Allow or block packets based on predefined rules and can be effective against basic network attacks



Basic Security Measures: Firewalls (Cont.)

2. **Stateful Inspection Firewalls:**
   a. Operate at the transport layer and monitor active connections to track the entire communication process between devices
   b. Allow or block packets based on their context and the connection's current state
   c. Provides a higher level of security than packet-filtering firewalls and can help protect against more advanced attacks

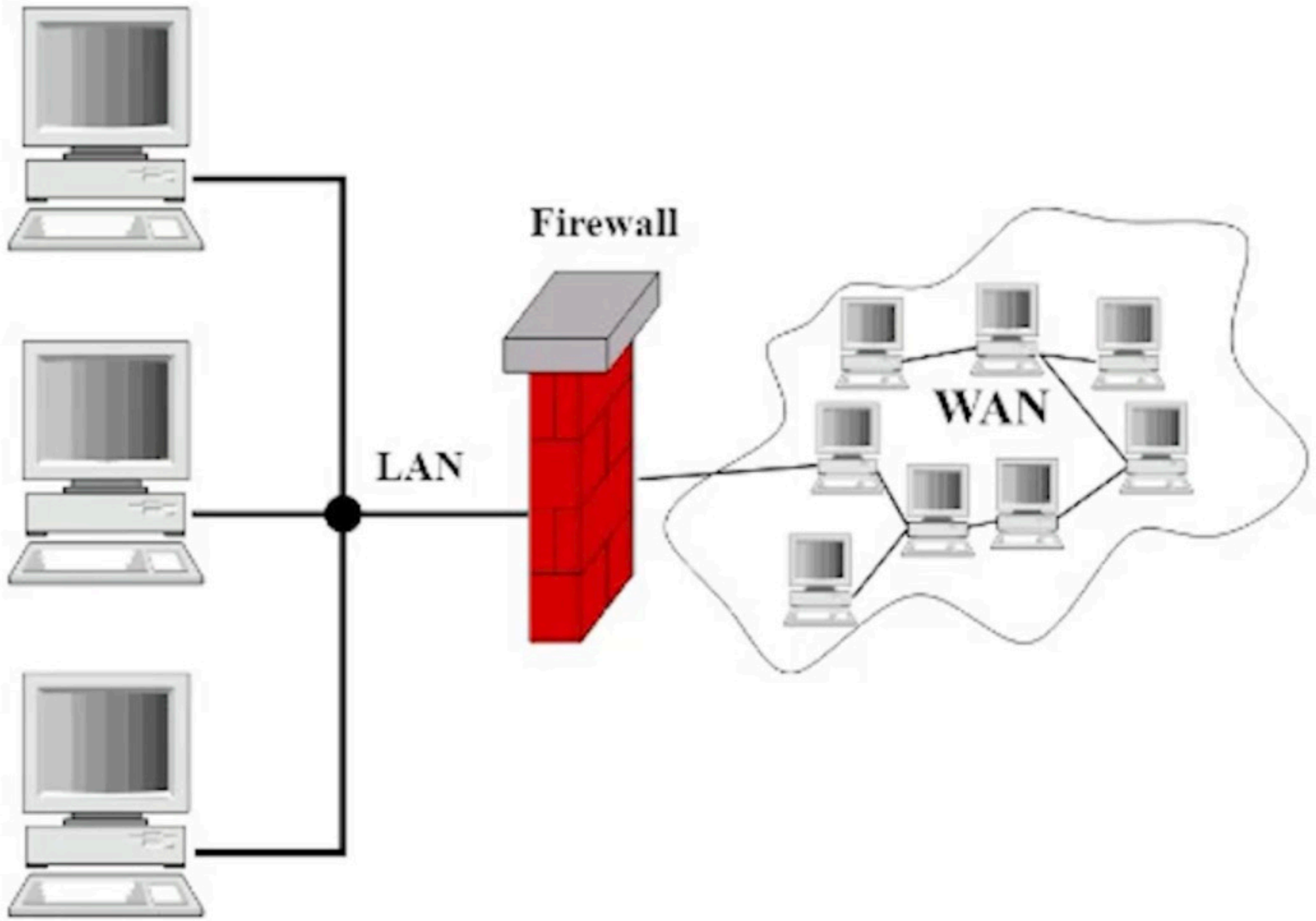


3. **Application-Layer Firewalls:**
   a. Operate at the transport layer and monitor active connections to track the entire communication process between devices

Basic Security Measures: Firewalls (Cont.)

Firewall Best Practices:

- Configure your firewall with appropriate security rules and policies
- Regularly update its software and monitor its logs and alerts for signs of suspicious activity
- Consider using multiple firewalls to create a layered defense, known as a "defense-in-depth" strategy



Basic Security Measures: Anti-Virus Software

<u>What is Anti-Virus Software?</u>

- A security measure for protecting networks against malware such as viruses, worms, trojans, ransomware, and spyware

- Scans files and data for known malware signatures or suspicious behavior patterns

- Quarantine, delete, or repair infected files to minimize the impact of the threat

Basic Security Measures: Anti-Virus Software (Cont.)

Features and Benefits of Anti-Virus Software:

- Real-time protection to monitor systems for potential hazards and block them before they can infect devices

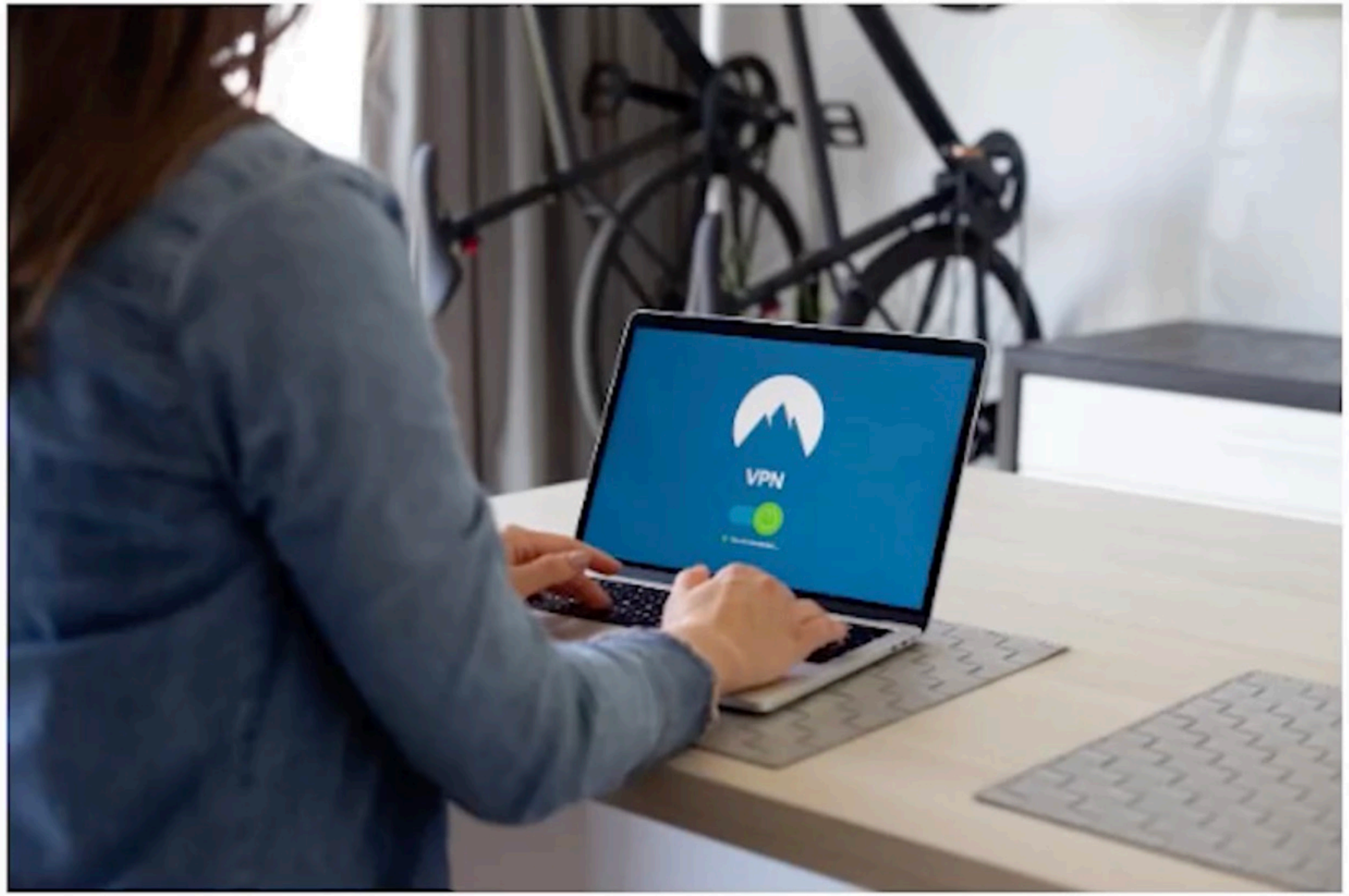
- Regularly updated with the latest malware definitions to ensure adequate protection

- Configured to maximize efficiency and minimize disruptions to services

Basic Security Measures: Virtual Private Networks (VPNs)

Introduction to VPNs:

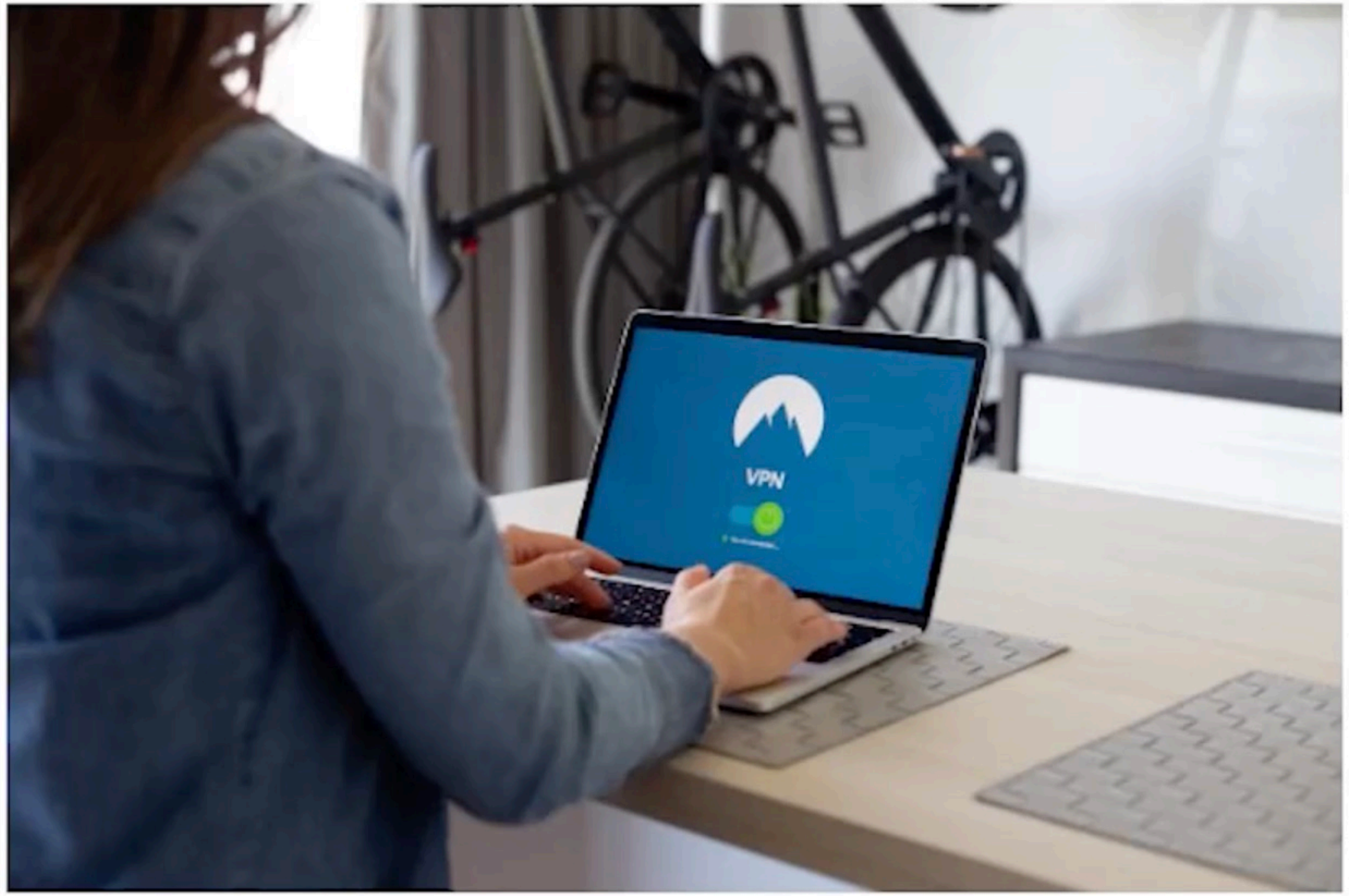
- Security technology that allows secure, encrypted connections over public networks
- Useful for remote workers or organizations with multiple locations
- Enables secure communication between devices and networks, even when separated by large distances



Basic Security Measures: Virtual Private Networks (VPNs) (Cont.)

Choosing a VPN Solution:

- Various VPN protocols are available:
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)
  - Secure Socket Tunneling Protocol (SSTP)
  - OpenVPN
- Each protocol offers different levels of security and performance
- Consider ease of use, compatibility, scalability, and level of encryption and authentication provided

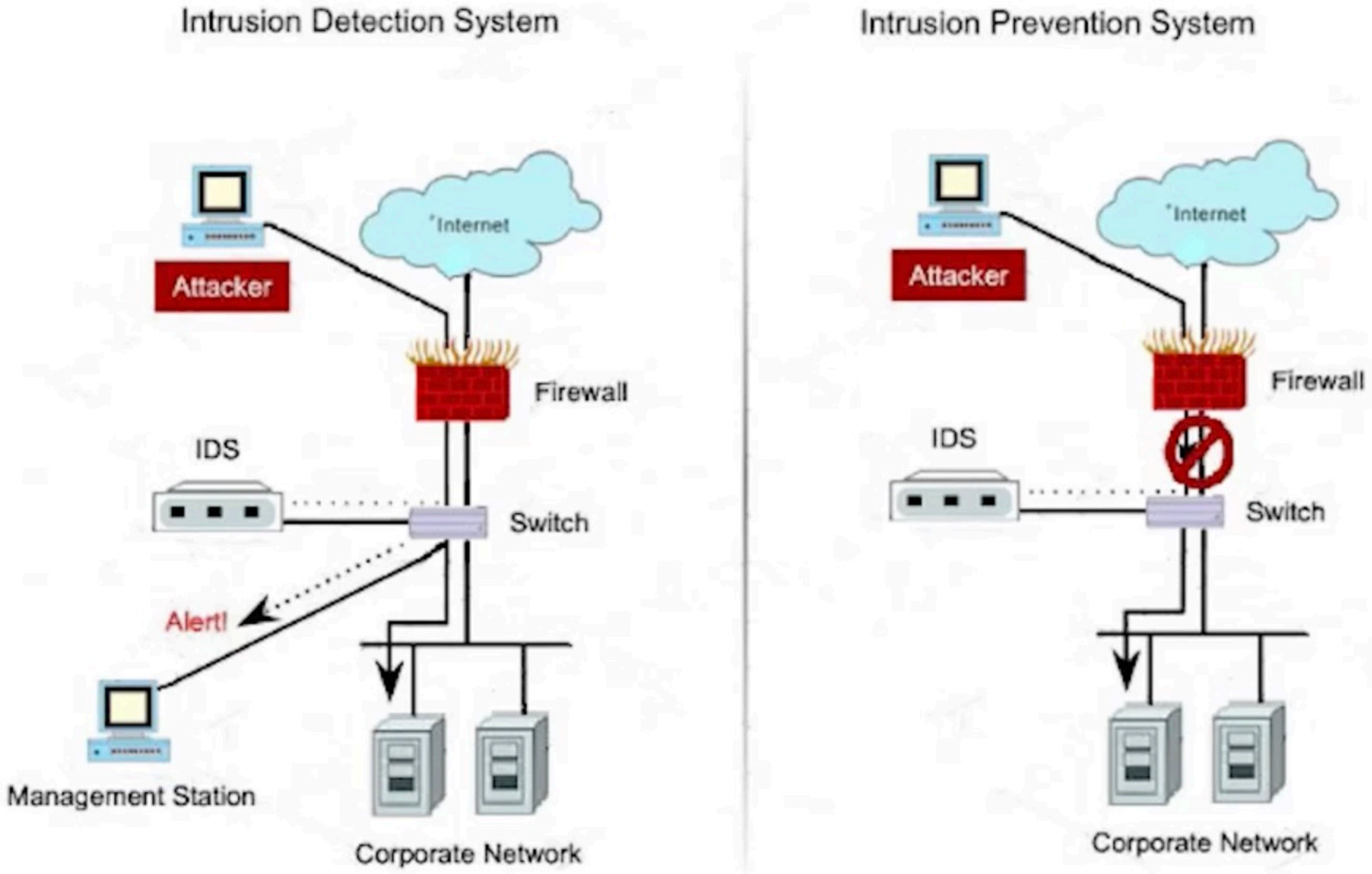


Basic Security Measures: IDS and IPS

What are IDS and IPS?

- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are network security technologies designed to detect and respond to potential threats and attacks on your network

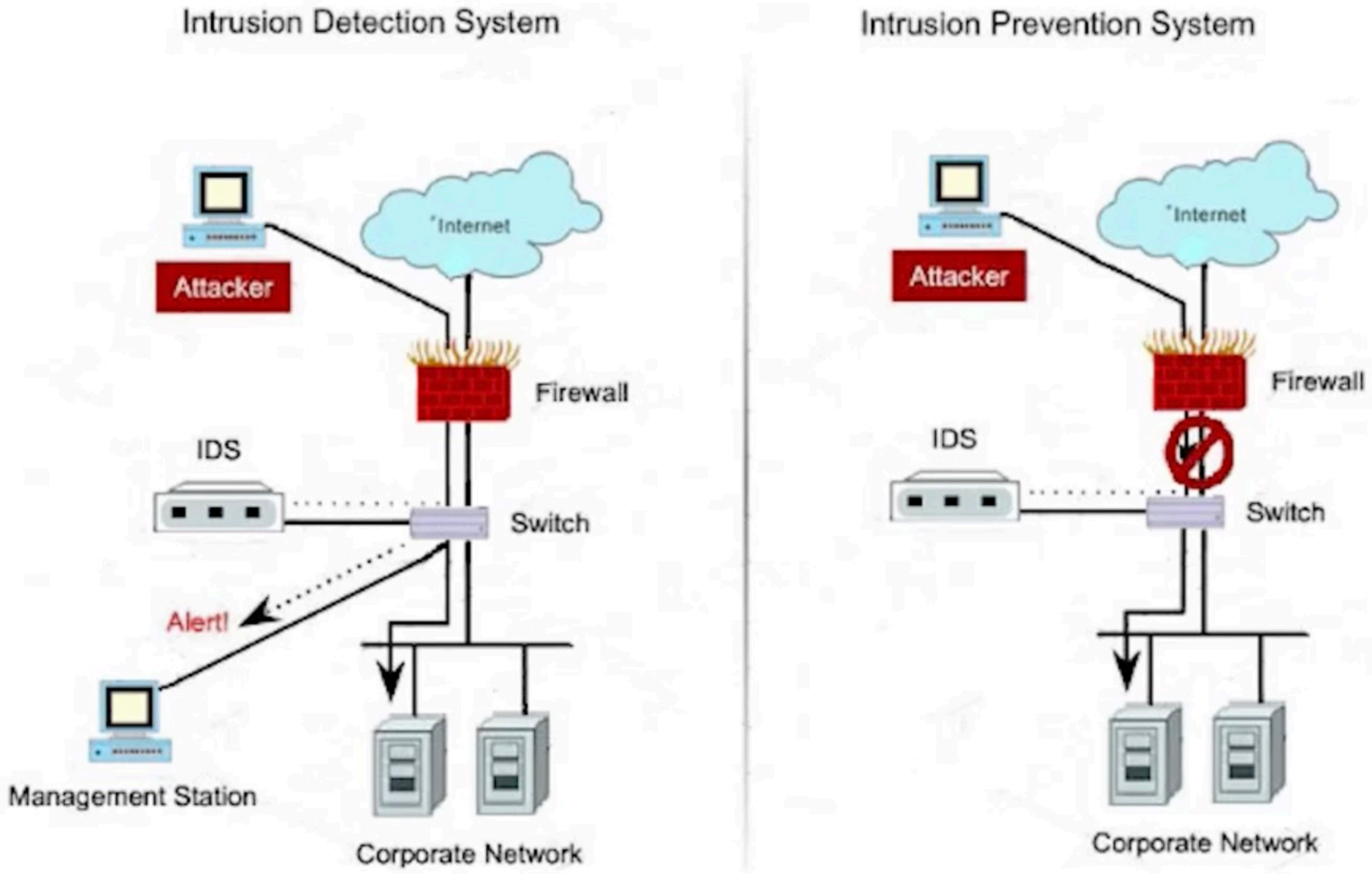
- Monitor network traffic, identify suspicious behavior, and take actions to protect your network from unauthorized access or malicious activity



Basic Security Measures: IDS and IPS (Cont.)

Intrusion Detection Systems (IDS):

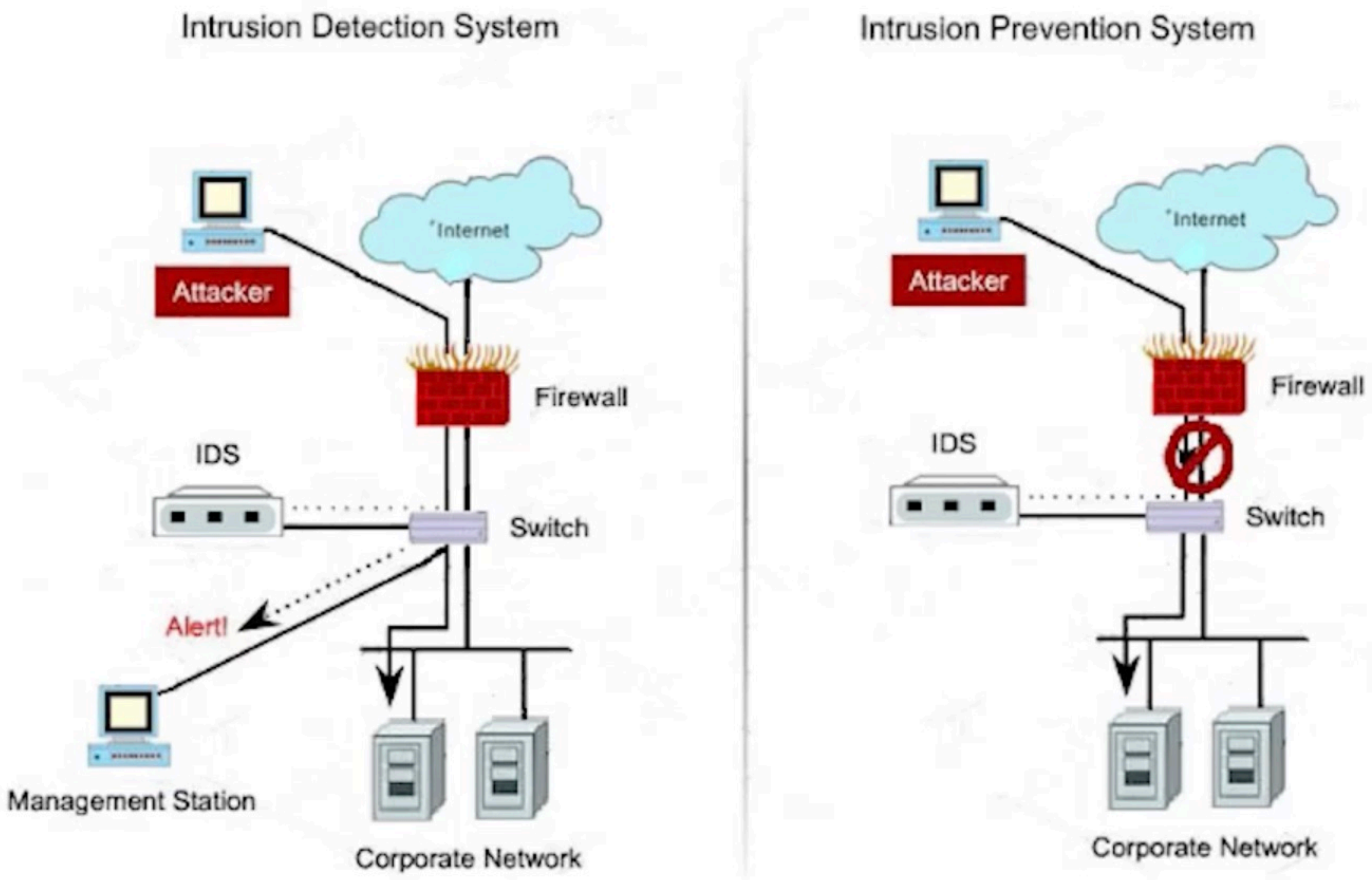
- Passive monitoring system that analyzes network traffic for signs of intrusion or malicious activity
- Generates alerts and logs the event for security administrators to investigate and take corrective action
- Can be network-based (NIDS) or host-based (HIDS)



Basic Security Measures: IDS and IPS (Cont.)

Intrusion Prevention Systems (IPS):

- Active security system that not only detects threats but also takes automated actions to block or mitigate them
- Examines network traffic in real-time, using signature-based, anomaly-based, and behavior-based detection methods to identify potential attacks
- Can take various actions such as blocking the offending IP address, resetting the connection, or alerting the security administrator


Intrusion Detection System
Internet
Attacker
Firewall
IDS
Switch
Alert!
Management Station
Corporate Network
Intrusion Prevention System
Internet
Attacker
Firewall
IDS
Switch
Corporate Network