CMPS 380
Spring 2025

Lecture 8

Basics of Network Security

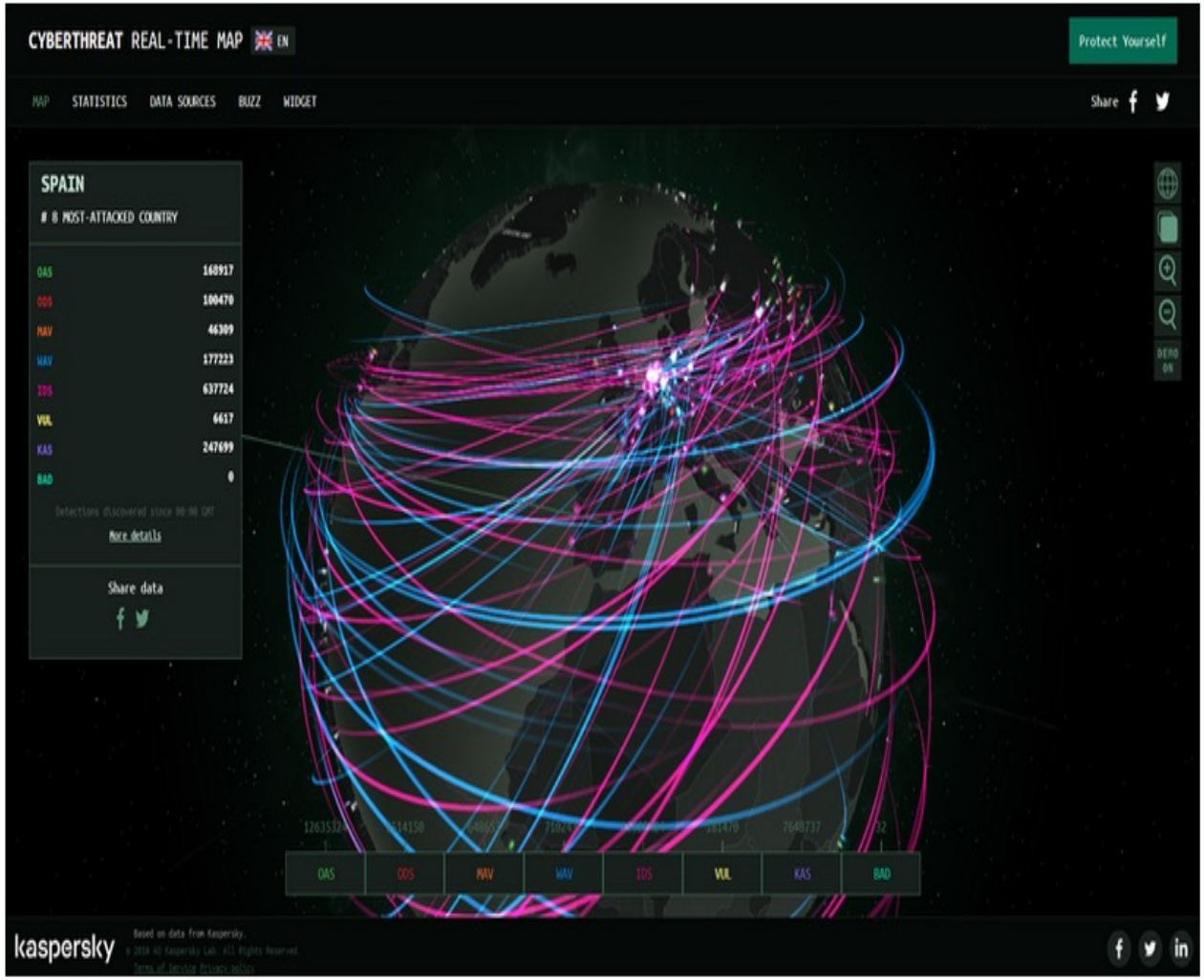
Dr Khaled Khan

Outline

- What is Network Security?
  - Common Risks to Networks
  - Types of Network Attacks
- How Networks Protect Themselves
  - Firewalls
  - Virtual Private Networks (VPNs)
  - Intrusion Detection and Prevention Systems

Networks are Targets

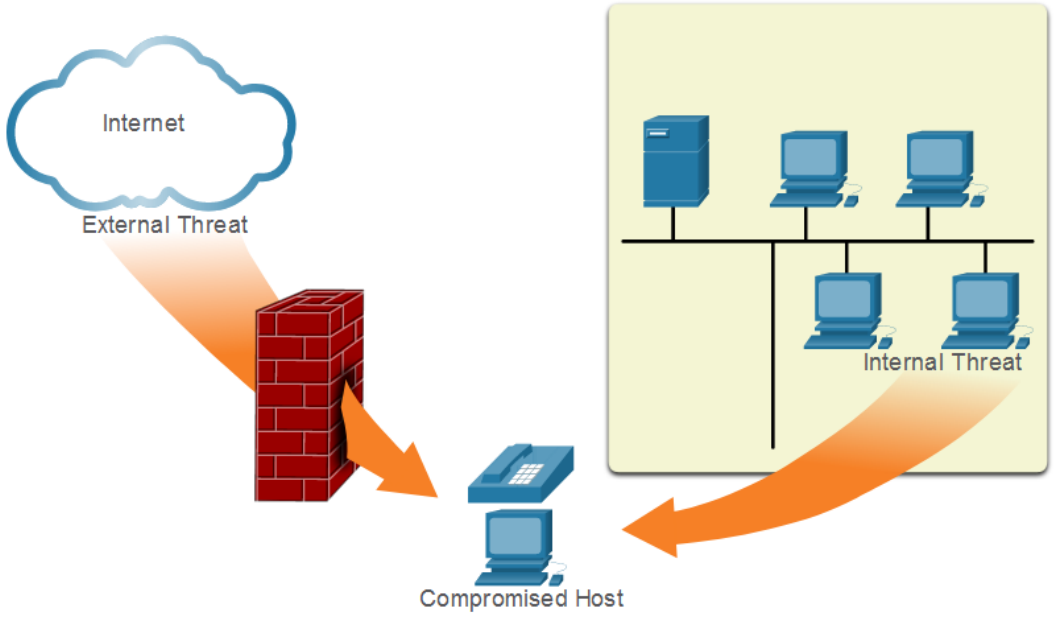
- Networks are routinely under attack.
- Kapersky maintains the interactive **Cyberthreat Real-Time Map** display of current network attacks.
- The attack data are available from Kapersky network security



https://cybermap.kaspersky.com

Vectors of Network Attacks

- An attack vector is a path by which a threat actor can gain access to a server, host, or network.
- Attack vectors originate from inside or outside the corporate network.
- Threat actors may target a network through the internet, to disrupt network operations and create a denial of service (DoS) attack.)



Types of Network Attacks

- To mitigate attacks, it is useful to first categorize the various types of attacks.
- By categorizing network attacks, it is possible to address **types of attacks** rather than individual attacks.
- Although there is no standardized way of categorizing network attacks, the method used in this course classifies attacks in three major categories.
    - Reconnaissance Attacks
    - Access Attacks
    - DoS Attacks

Reconnaissance Attacks

- Reconnaissance is information gathering.
- Attackers use reconnaissance (or recon) to do **unauthorized** discovery and mapping of systems.
- Some of the techniques used by malicious threat actors to conduct reconnaissance attacks are described in the table.

Technique	Description
Perform an information query of a target	• Attackers look for initial information about a target. • Various tools can be used, including the Google search, target website, whois, etc
Initiate a ping sweep of the target network	• A single ping usually reveals the target's network address. • The attacker can initiate a **ping sweep** to determine active IP addresses. • In contrast to a single ping, a ping sweep uses ICMP (Internet Control Message Protocol) ECHO requests to communicate with multiple hosts simultaneously.
Tools-based port scan of active IP addresses	• This is used to determine which ports or services are available. • Examples of port scanners include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
Run vulnerability scanners	• This is to query the identified ports to **determine the type and version of the application** and operating system that is running on the host. • Examples of tools include Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT, and Open VAS.
Run exploitation tools	• Attackers attempt to **discover vulnerable services** that can be exploited. • A variety of vulnerability exploitation tools exist including Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.

Access Attacks

- Access attacks exploit **known vulnerabilities in authentication services**, FTP services, and web services.
- The purpose of this type of attack is **to gain entry to web accounts**, confidential databases, and other sensitive information.

Technique	Description
Password Attacks	• In a password attack, attackers attempt to discover passwords using various methods.
Spoofing Attacks	• In spoofing attacks, attackers' attempt to pose as another device by falsifying data. • Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP (**Dynamic Host Configuration Protocol**) spoofing.
Trust Exploitation	• Attackers exploit authorized access or trust to gain unauthorized privileges access to a system, possibly compromising the target.
Port redirection	• In a port redirection attack, attackers use a compromised system as a base for attacks against other targets.
Man-in-the-Middle	• In a man-in-the-middle attack, an attacker is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties.
Buffer Overflow Attack	• In a buffer overflow attack, an attacker exploits the buffer memory and **overwhelms it with unexpected values.** • This usually renders the system inoperable, resulting in a DoS attack.

**DHCP is a network protocol used to configure devices on IP networks, thus allowing them to use network services such as DNS, and any communication protocol based on UDP or TCP.

DoS Attacks

- A **Denial of Service (DoS)** attack is when an attacker tries to make a network, website, or online service unavailable by overwhelming it with excessive traffic or requests.
- Imagine too many people trying to enter a building at once, causing a traffic jam at the entrance so no one can get in.
- Similarly, in a DoS attack, the network or service becomes so overloaded that it can't handle legitimate users' requests, effectively "shutting down" access.
- In network security, DoS attacks are dangerous because they disrupt normal operations, affecting businesses, websites, and users.
- Attackers may use botnets (large networks of infected computers) to generate massive amounts of fake traffic to carry out these attacks.
- Key points:
  - Overloads the system.
  - Legitimate users can't access services.
  - No data is typically stolen, but operations are disrupted.

How Networks Protect Themselves

Mitigating Reconnaissance Attacks

- Reconnaissance typically is an indication of actual attacks that are designed to gain unauthorized access to a network or disrupt network functionality.
- You can detect when a reconnaissance attack is underway by receiving notifications from **preconfigured alarms.**
- These alarms are triggered when certain parameters are exceeded, such as the number of ICMP **(**Internet Control Message Protocol) requests per second.
- Reconnaissance attacks can be mitigated in several ways, including the following:
    - Implementing authentication to ensure proper access.
    - Using encryption to render packet sniffer attacks useless.
    - Using anti-sniffer tools to detect packet sniffer attacks.
    - Implementing a switched infrastructure.
    - Using a firewall and IPS (Intrusion prevention systems).
- It is impossible to mitigate port scanning.
- Using an IPS and firewall can limit the information that can be discovered with a port scanner.
- Ping sweeps can be stopped if **ICMP echo and echo-reply are turned off** on edge routers
- However, when these services are turned off, network diagnostic data is lost.

Basic Authentication

- The simplest method of remote access authentication is to configure a login and password combination.
- Remote User Authentication allows users to verify their identity to access a system or network from a different location than the system's physical location, for example, SSH.
- Instead of using local credentials stored directly on the system they're trying to access, users authenticate themselves through credentials managed and stored on an external authentication service such as an authenticator based on mobile phone.

SSH (Secure Shell or Secure Socket Shell)

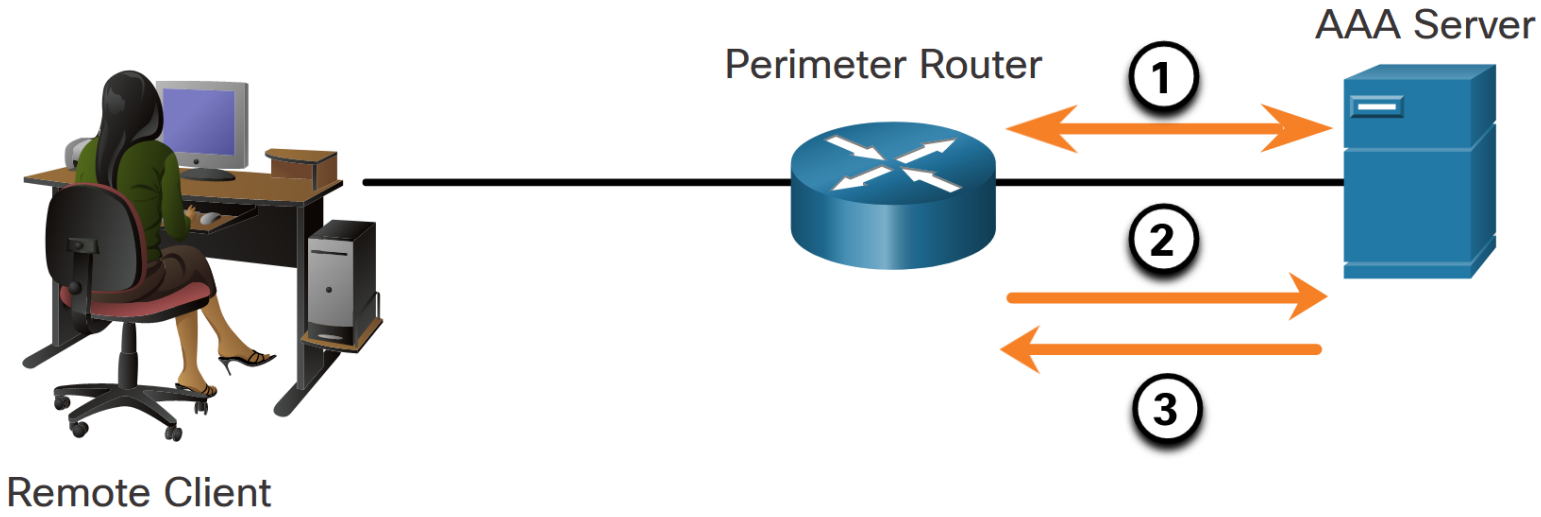
- SSH is a more secure form of remote access.
- SSH requires both a username and a password, both of which are encrypted during transmissions.
- The user accounts must be configured with SSH locally on each device.

AAA (Authentication, Authorization, Access Control)

- Network and administrative AAA security has three functional components:
  - **Authentication** –
    - Users and administrators must prove their identity before accessing the network and network resources.
    - Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods.
      - For example: “I am user ‘student’ and I know the password to prove it.”
  - **Authorization** –
    - After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform.
      - An example is “User ‘student’ can access host serverXYZ using SSH only.”
  - **Accounting and auditing** –
    - Accounting records **what the user does**, including what is accessed, the amount of time the resource is accessed, any attempts to access unauthorized privileges, or any changes that were made.
    - Accounting keeps track of how network resources are used.
      - An example is "User 'student' accessed host serverXYZ using SSH for 15 minutes."

Authentication, Authorization, and Accounting (AAA)

- After users are successfully authenticated against the selected AAA (Authentication, Authorization, and Accounting) protected data source, either local or server-based, they are then authorized for specific network resources, as shown in the figure.



- AAA server controls access to computer resources, enforces policies, and audits usage.
- AAA "guards" access to your wired and wireless networks by checking each user or device connecting to the network.
- AAA handles user requests for access to computer resources

Firewalls

All firewalls share some common properties:

- Firewalls are resistant to network attacks.
- Firewalls are the only transit point between internal corporate networks and external networks because all traffic flows through the firewall.
- Firewalls enforce the access control policy.

Different types of firewalls have different benefits and limitations.

Allow traffic from any external address to the web server.

Allow traffic to FTP server.

Allow traffic to SMTP server.

Allow traffic to internal IMAP server.

Deny all inbound traffic with network addresses matching internal-registered IP addresses.

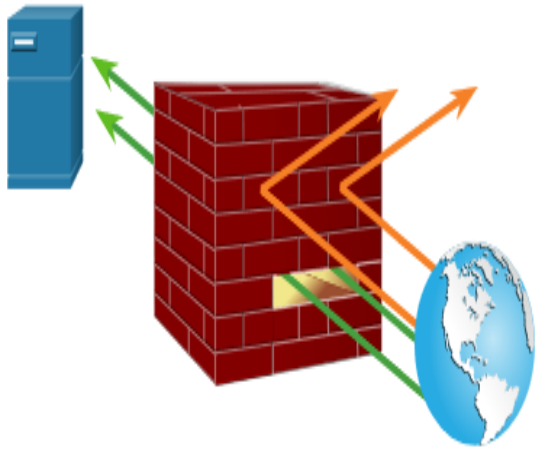
Deny all inbound traffic to server from external addresses.

Deny all inbound ICMP echo request traffic.

Deny all inbound MS Active Directory queries.

Deny all inbound traffic to MS SQL server queries.

Deny all MS Domain Local Broadcasts.



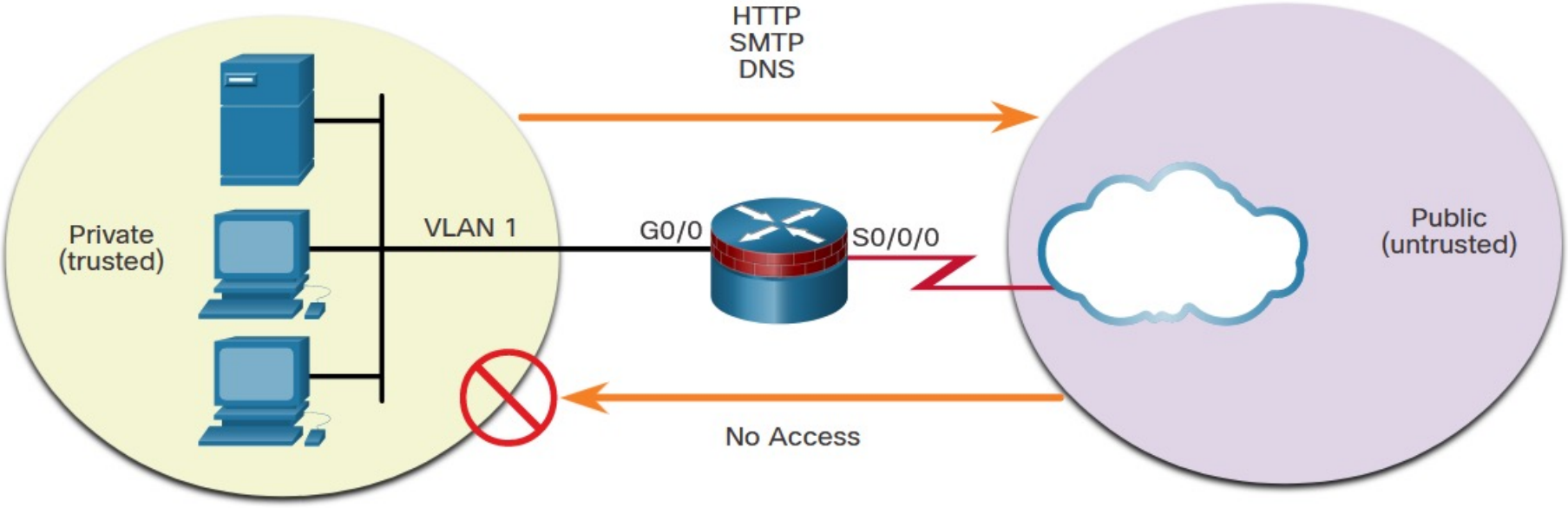
Common Security Architectures

Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic.
Here are two common firewall designs:

- **Private and Public**
- **Demilitarized Zone (DMZ)**

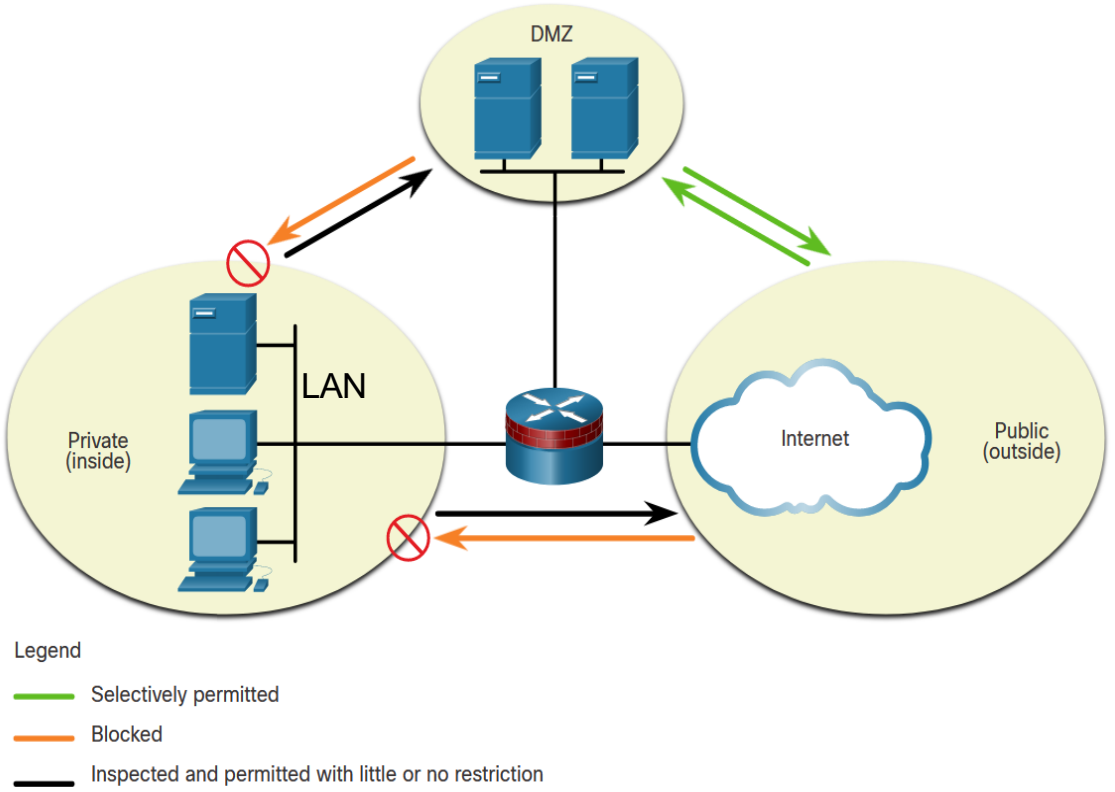
Private and Public

- The public network (or outside network) is untrusted, and the private network (or inside network) is trusted.



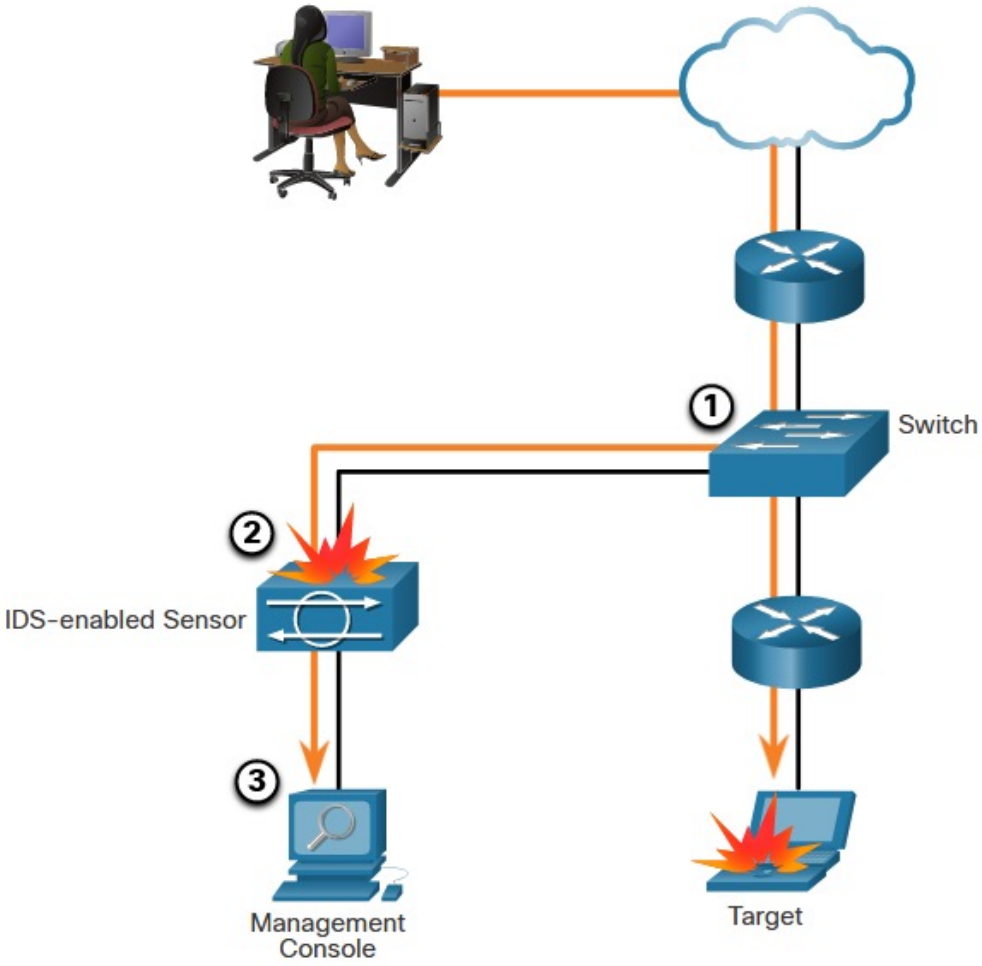
DMZ Firewall Design Considerations

- **Demilitarized Zone (DMZ)** is a firewall design where there is typically one inside interface connected to the private network, one outside interface connected to the public network, and one DMZ interface.
- A physical or logical subnet that separates a local area network (LAN) from other untrusted networks -- usually, the public internet.
- DMZ isolates public networks from private networks and is used as a third-party middleman to translate information from private and public networks.
- DNS firewalls work to filter inbound and outbound traffic on a network and block suspicious activity.



Monitor for Attacks

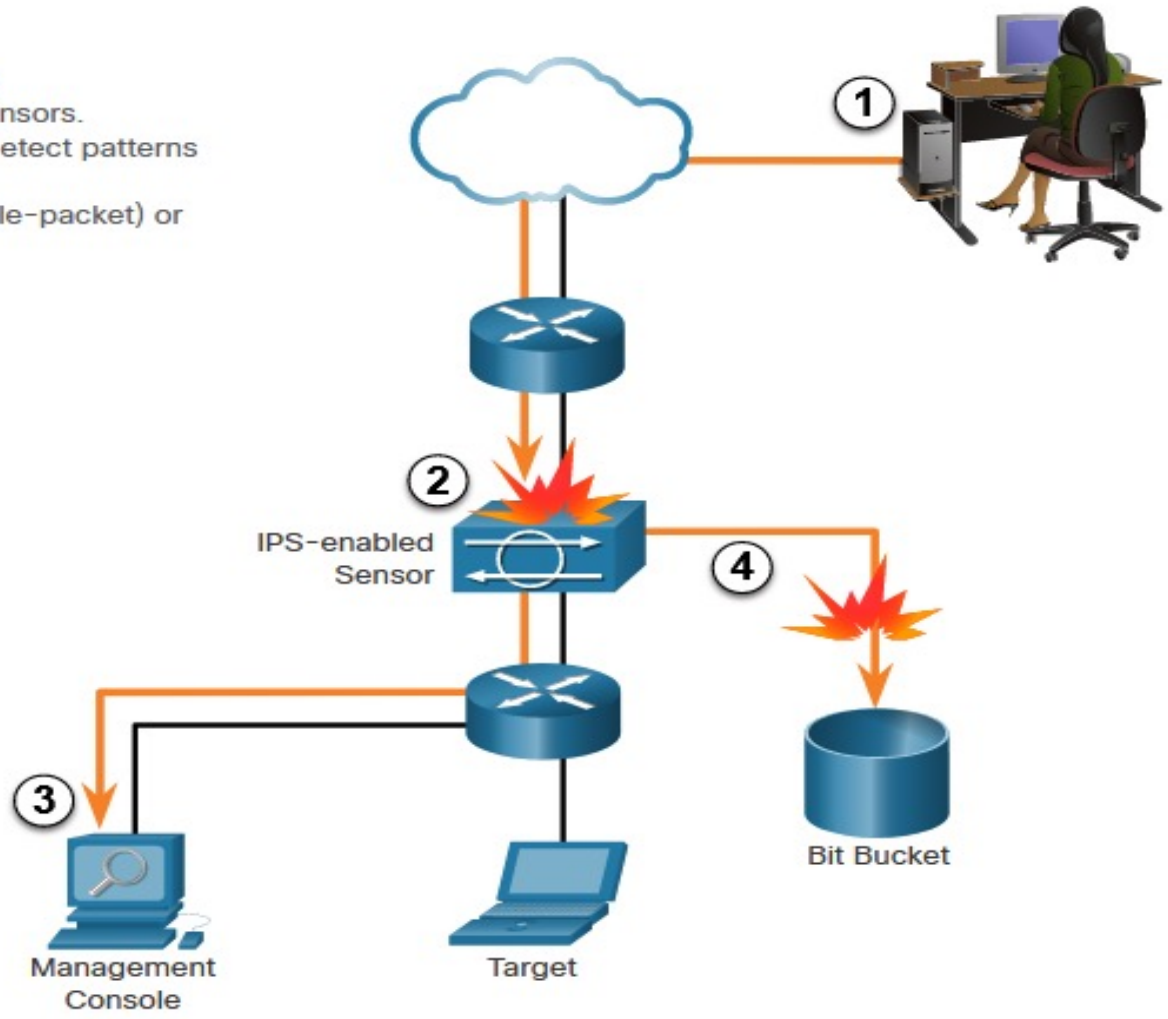
- Intrusion Detection Systems (IDS) were implemented to **monitor the traffic on a network passively**.
- The figure shows that an IDS-enabled device **copies the traffic stream** and analyzes the copied traffic.
- IDS decides if the packet is an attempt for unauthorized or malicious access.
- On the other hand, an intrusion prevention s**ystem (IPS)** can immediately detect and stop an attack.



Intrusion Prevention and Detection Devices

Common Characteristics of IDS and IPS

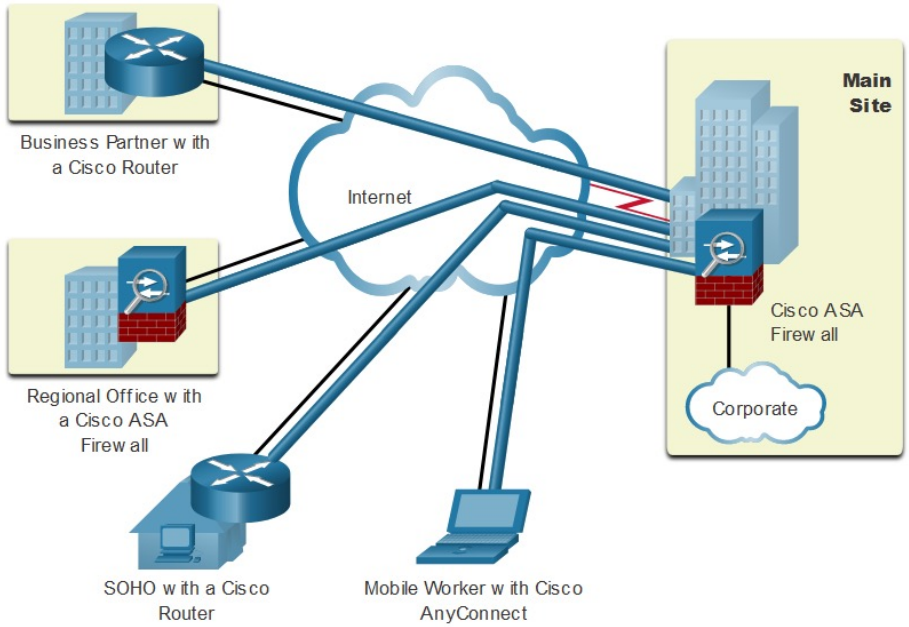
- Both technologies are deployed as sensors.
- Both technologies use signatures to detect patterns of misuse in network traffic.
- Both can detect atomic patterns (single-packet) or composite patterns (multi-packet).



1. Malicious traffic is sent to the target host that is inside the network.
2. The traffic is routed into the network and received by an IPS-enabled sensor where it is blocked.
3. The IPS-enabled sensor sends logging information regarding the traffic to the network security management console.
4. The IPS-enabled sensor kills the traffic. (It is sent to the "Bit Bucket.")

Virtual Private Networks (VPN)

- To secure network traffic between sites and users, organizations use virtual private networks (VPNs) to create end-to-end private network connections.
- A VPN is virtual in that it carries information within a private network, but that information is transported over a public network.
- A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network.
- The figure shows a collection of various types of VPNs managed by an enterprise's main site.
- The tunnel enables remote sites and users to access main site's network resources securely.
- A VPN, which stands for virtual private network, protects its users by encrypting their data and masking their IP addresses.
- This hides their browsing activity, identity, and location, allowing for greater privacy and autonomy.
- Provides anonymity of IP masking and location spoofing, ensures your online presence nearly untraceable.



VPN Benefits

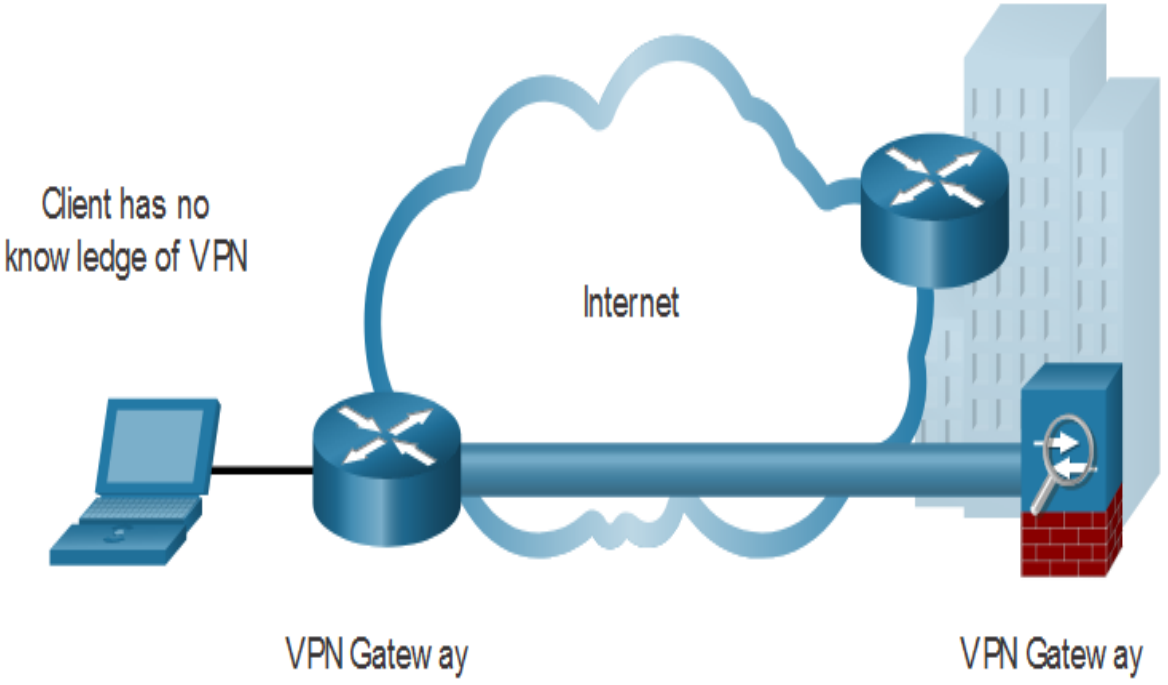
Modern VPNs now support encryption features, such as Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL) VPNs to secure network traffic between sites.

Major benefits of VPNs are shown in the table.

Benefit	Description
Cost Savings	• With the advent of cost-effective, high-bandwidth technologies, organizations can use VPNs to reduce their connectivity costs while simultaneously increasing remote connection bandwidth.
Security	• VPNs provide the highest level of security available, by using advanced encryption and authentication protocols that protect data from unauthorized access.
Scalability	• VPNs allow organizations to use the internet, making it easy to add new users without adding significant infrastructure.
Compatibility	• VPNs can be implemented across a wide variety of WAN link options including all the popular broadband technologies. • Remote workers can take advantage of these high-speed connections to gain secure access to their corporate networks.

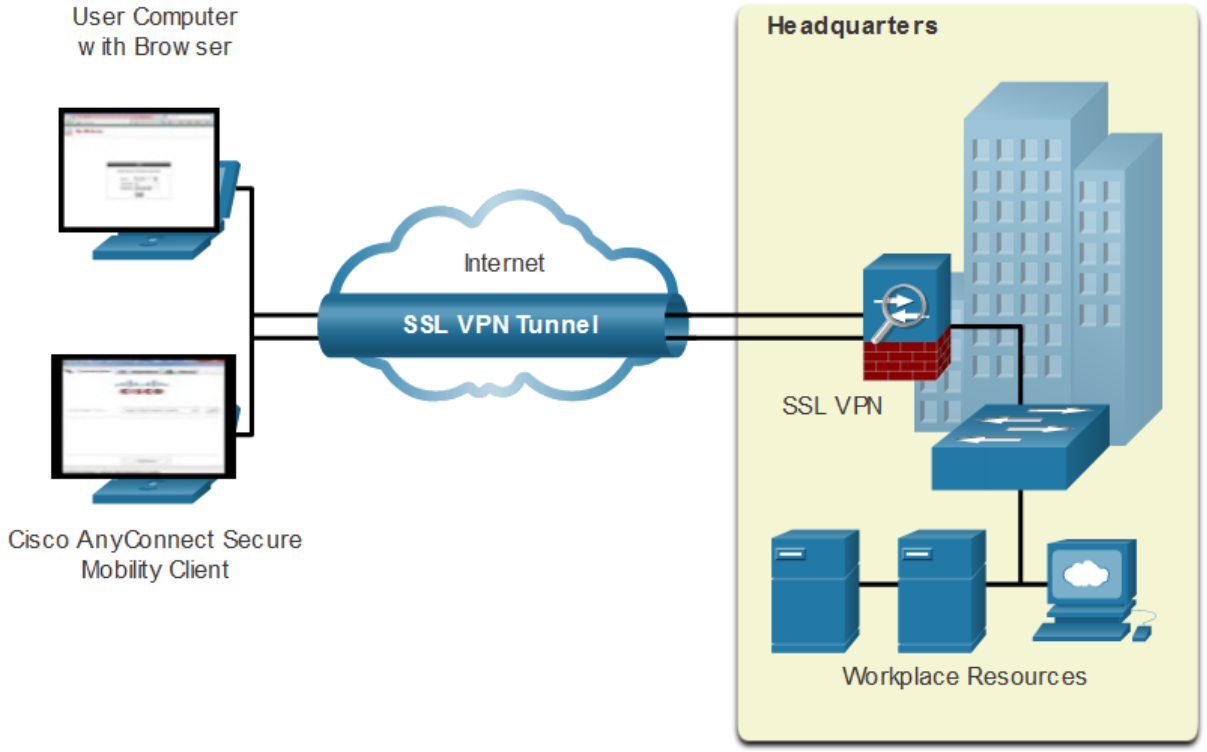
Site-to-Site VPNs

- A site-to-site VPN is created when VPN terminating devices, also called VPN gateways, are preconfigured with information to establish a secure tunnel.
- VPN traffic is only encrypted between these devices.
- Internal hosts have no knowledge that a VPN is being used.
- Unlike site-to-site connections, point-to-site connections don't require an on-premises public-facing IP address or a VPN device.
- Point-to-site connections can be used with site-to-site connections through the same VPN gateway.



Remote-Access VPNs

- Remote-access VPNs are typically enabled dynamically by the user when required.
- A remote user must initiate a remote access VPN connection.
- Remote access VPNs can be created using either **IPsec or SSL.**
- The figure displays two ways that a remote user can initiate a remote access VPN connection: clientless VPN and client-based VPN.



- **Internet Protocol (IP)** is the common standard that determines how data travels over the internet.
- **IPSec** is a set of communication rules or protocols for setting up secure connections over a network.
- IPSec adds encryption and authentication to make the protocol more secure.
- **Secure Sockets Layer (SSL)** is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser, or a mail server and a mail client.
- SSL VPNs are generally more user friendly and easier to use, providing secure access without requiring client software.
- IPSec VPNs are often preferred for their ability to secure all network traffic at the IP layer, but these consume a lot of network bandwidth which makes IPSec a less attractive option for networks handling large numbers of small data packets.

Summary

- Understanding the network is the backbone of computer security
- Various network protocols
- Types of network attacks
- AAA
- Firewalls
- DMZ
- IDS
- IPS
- VPN
- IPSec
- SSL