Network Security Threats and countermeasures

UNIT – II

Contents

- Network Security Devices,
- Types of Network Securities,
- Network Access Control,
- Characteristics of Network Access Control,
- Application Security,
- Application Security Tools,
- Firewalls and its types,
- virtual private network,
- Tunneling protocol and types,
- IDS vs. IPS,IDS, IPS and their Types,
- Introduction to Web Application Vulnerabilities

Introduction

- A threat is any potential danger that can harm your systems, data, or operations.
- In cybersecurity, threats include activities like hacking, malware attacks, or data breaches that aim to exploit vulnerabilities.
- Recognizing and understanding these threats is crucial for implementing effective security measures.

What Is Network Security?

- Network security incorporates various technologies, processes, and devices into a broad strategy that protects the integrity, confidentiality, and accessibility of computer networks.
- Organizations of all sizes, industries, or infrastructure types require network security to protect against an ever-evolving cyber threat landscape.
- Traditional network security consists of rules and configurations that employ software and hardware technologies to protect the network and its data.
- However, this mechanism cannot cover the needs of today's complex network architectures, which have a bigger, more vulnerable attack surface than the traditional perimeter-based network of past days.

Network Security Devices

- Network security devices are critical for protecting an organization's IT infrastructure from various threats, both internal and external.
- These devices monitor, control, and safeguard network traffic, ensuring that only authorized users and data packets can enter or leave the network.

- Here's an overview of common network security devices:
  - Firewall
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)
  - Virtual Private Network (VPN) Gateway
  - Unified Threat Management (UTM) Device
  - Web Application Firewall (WAF)
  - Network Access Control (NAC)
  - Proxy Server
  - Network Address Translation (NAT) Gateway

Firewall

- Purpose: A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's predefined security rules.
- Types:
  - Packet Filtering Firewall: Filters packets based on source/destination IP address, protocol, and port number.
  - Stateful Inspection Firewall: Tracks the state of active connections and makes decisions based on context (state) and rule sets.
  - Next-Generation Firewall (NGFW): Includes more advanced features like deep packet inspection, application awareness, and intrusion prevention.
- Usage: Blocks malicious traffic while allowing legitimate communication.

Intrusion Detection System (IDS)

- Purpose: IDS monitors network traffic for suspicious activity and known threats, sending alerts to administrators if malicious activity is detected.
- Types:
  - Network-based IDS (NIDS): Monitors entire network traffic.
  - Host-based IDS (HIDS): Monitors traffic to and from a single device or host.
- Usage: Detects and alerts potential security incidents but does not take direct action to prevent them.

Intrusion Prevention System (IPS)

- Purpose: IPS actively monitors network traffic for malicious activity and takes action to block, reject, or mitigate the detected threat.
- Difference from IDS: While IDS only detects and alerts, IPS takes real-time action to prevent the attack.
- Usage: Stops threats like DDoS attacks, malware, and other vulnerabilities by dropping malicious traffic packets.

Virtual Private Network (VPN) Gateway

- Purpose: VPN gateways establish secure, encrypted tunnels for remote users to securely access the internal network over the internet.
- Types:
  - SSL VPN: Uses Secure Sockets Layer for encryption.
  - IPsec VPN: A more traditional VPN that secures IP traffic.
- Usage: Ensures confidentiality, integrity, and authenticity of data exchanged between the remote user and the corporate network.

Unified Threat Management (UTM) Device

- Purpose: UTM devices consolidate multiple security functions such as firewall, IDS/IPS, VPN, anti-virus, anti-spam, and content filtering into a single device.
- Usage: Provides a centralized, simplified approach to managing multiple security systems, reducing complexity and cost.

Web Application Firewall (WAF)

- Purpose: A WAF specifically protects web applications by filtering and monitoring HTTP traffic between the web application and the internet.
- Usage: Blocks attacks such as SQL injection, cross-site scripting (XSS), and session hijacking targeting web applications.

Network Access Control (NAC)

- Purpose: NAC controls which devices can connect to the network, enforcing policies such as device authentication, endpoint security checks, and user role-based access control.
- Usage: Prevents unauthorized or non-compliant devices from connecting to the network.

Proxy Server

- Purpose: Proxy servers act as intermediaries between users and the internet, providing anonymity, security, and control over web traffic.
- Types:
  - Forward Proxy: Used to fetch content on behalf of the user, providing content filtering and caching.
  - Reverse Proxy: Protects internal servers by masking their identity and filtering traffic.
- Usage: Protects user privacy, blocks harmful content, and mitigates external threats.

Network Address Translation (NAT) Gateway

- Purpose: NAT gateways hide internal IP addresses by mapping them to a single or a few external IP addresses, providing an additional layer of security.
- Usage: Prevents external attackers from directly accessing internal network resources by making internal systems "invisible."

Types of Network Securities

- Network security encompasses a range of measures designed to protect the integrity, confidentiality, and availability of data transmitted across or stored in a network. Here are the main types of network security:

1. Physical Network Security

- Description: This involves protecting the physical hardware and infrastructure of a network, including servers, routers, switches, and cables.
- Examples:
- Securing access to data centers and server rooms with locks, biometric scanners, and surveillance cameras.
- Implementing environmental controls like fire suppression and climate regulation.
- Purpose: Prevent unauthorized physical access that could lead to theft, damage, or tampering with network equipment.

2. Network Access Control (NAC)

- **Description**: NAC ensures that only authorized users and devices can access the network. It enforces policies based on user roles, device compliance, and network conditions.
- **Examples**:
  - Authentication through username, password, and multi-factor authentication (MFA).
  - Device verification to ensure compliance with security policies.
- **Purpose**: Prevent unauthorized or non-compliant devices and users from accessing the network.

3. Firewalls

- **Description**: Firewalls act as gatekeepers, monitoring and controlling network traffic based on predefined security rules. They can block malicious traffic while allowing legitimate traffic to flow.
- **Examples**:
  - **Hardware Firewalls**: Separate devices placed between the network and the internet.
  - **Software Firewalls**: Installed on individual devices, protecting them from external threats.
- **Purpose**: Protect networks from external threats such as hackers, malware, and unwanted traffic.

4. Intrusion Detection and Prevention Systems (IDS/IPS)

- **Description**: IDS monitors network traffic for suspicious activity and alerts administrators, while IPS actively blocks malicious activity.
- **Examples**:
  - **Network-based IDS/IPS**: Monitors all network traffic for suspicious patterns.
  - **Host-based IDS/IPS**: Monitors traffic on specific devices for malicious activity.
- **Purpose**: Detect and prevent cyberattacks, including malware and denial-of-service (DoS) attacks.

5. Virtual Private Network (VPN)

- **Description**: VPNs create secure, encrypted tunnels over public networks, allowing users to access the network remotely as if they were on-site.
- **Examples**:
  - **SSL VPN**: Provides secure web access through a browser.
  - **IPsec VPN**: Encrypts and authenticates data at the IP layer.
- **Purpose**: Ensure secure remote access for employees, partners, and clients, protecting data from interception.

6. Encryption

- **Description**: Encryption secures data by converting it into an unreadable format, which can only be deciphered by those with the decryption key.
- **Examples**:
  - **Encryption of Data in Transit**: Protects data being transferred across networks using protocols like SSL/TLS.
  - **Encryption of Data at Rest**: Encrypts stored data on servers, devices, or cloud platforms.
- **Purpose**: Protect sensitive information from unauthorized access, whether in transit or at rest.

7. Anti-Malware and Antivirus Protection

- **Description**: Anti-malware and antivirus software detects, blocks, and removes malicious software such as viruses, ransomware, worms, and Trojan horses.
- **Examples**:
  - Regularly updated antivirus software on all endpoints and servers.
  - Advanced threat detection tools that use artificial intelligence (AI) and machine learning to identify new threats.
- **Purpose**: Prevent malware infections and minimize damage caused by malicious software.

8. Data Loss Prevention (DLP)

- **Description**: DLP systems monitor and control network traffic to prevent unauthorized sharing or leakage of sensitive data.
- **Examples**:
  - Monitoring for unauthorized data transfers via email or cloud services.
  - Blocking the upload or transmission of sensitive data like credit card numbers or intellectual property.
- **Purpose**: Prevent data breaches and ensure that sensitive data does not leave the network without authorization.

9. Access Control and Authentication

- **Description**: Access control systems ensure that only authorized users can access certain resources within the network, while authentication verifies the identity of users.
- **Examples**:
  - Role-based access control (RBAC) which grants access based on the user's role within the organization.
  - Two-factor or multi-factor authentication (MFA) requiring users to verify their identity with multiple forms of authentication.
- **Purpose**: Restrict access to critical systems and data, ensuring that only those with proper permissions can view or modify sensitive information.

10. Web Security

- **Description**: Web security tools protect users from web-based threats and ensure that harmful websites cannot compromise the network.
- **Examples**:
  - Web application firewalls (WAFs) that protect against attacks like cross-site scripting (XSS) and SQL injection.
  - URL filtering to block access to malicious or inappropriate websites.
- **Purpose**: Safeguard web applications and users from online threats.

Network Access Control

- Network Access Control (NAC) is a security solution designed to manage and control access to network resources based on predefined security policies.
- It allows organizations to enforce who can and cannot connect to their network and under what conditions.
- NAC ensures that only authorized, compliant devices (such as computers, mobile devices, or Internet of Things (IoT) devices) can access a network, reducing the risk of unauthorized access and potential security threats.

- ## Key Functions of NAC:
  - Authentication: Ensures that users and devices are authenticated before they are granted access to the network. This typically involves verifying user credentials (e.g., usernames, passwords, certificates).
  - Authorization: Based on the authentication results and the policies defined by the organization, NAC determines what resources the user or device is allowed to access.
  - Compliance Checking: NAC can enforce security policies by checking if a device complies with the organization's security requirements, such as up-to-date antivirus software, patched operating systems, or the absence of known vulnerabilities.
  - Network Segmentation: NAC can limit network access based on the role of the user or the compliance state of the device. For example, a compliant device may have full access, while a non-compliant device may be limited to a remediation network where it can update its software or install antivirus.
  - Monitoring and Enforcement: Continuous monitoring ensures that users and devices remain compliant. If a device becomes non-compliant (e.g., if its antivirus becomes outdated), access can be restricted or revoked.

- **Types of NAC:**
- **Pre-admission NAC**: This type of NAC evaluates devices before they are allowed to connect to the network. The device must pass authentication and compliance checks before it is admitted.
- **Post-admission NAC**: In this case, the device is allowed to connect to the network but is continuously monitored. If it violates the security policies after connection, its access can be restricted.

- **Benefits of NAC:**
  - **Improved Security**: Ensures that only authorized and secure devices access the network.
  - **Compliance Enforcement**: Automates the enforcement of security policies and regulatory compliance.
  - **Network Visibility**: Provides detailed visibility into the devices connected to the network.
  - **Reduced Threat Surface**: Limits the exposure to malware and attacks by restricting access for non-compliant devices.

Characteristics of Network Access Control

- **Device visibility**
  - NAC provides visibility into connected devices and their users, which can help improve endpoint security and incident response.
- **Guest access**
  - NAC can provide secure guest access.
- **Authentication**
  - Authentication, or verifying a user's identity, is a key component of access control. Two-factor authentication (2FA) can make networks more secure.
- **Advanced sensor-based visibility**
  - NAC tools can help detect suspicious traffic patterns, bottlenecks, and other anomalies.
- **Incident response**
  - A robust NAC solution should be able to respond to threats quickly and effectively.
- **Monitoring**
  - Network monitoring tools can help detect unusual traffic patterns or user activity, which can be an indicator of an attack

Application Security

- Application security is the process of protecting software applications from cyber threats by identifying, mitigating, and preventing security vulnerabilities.
- Application security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.

Application Security Tools

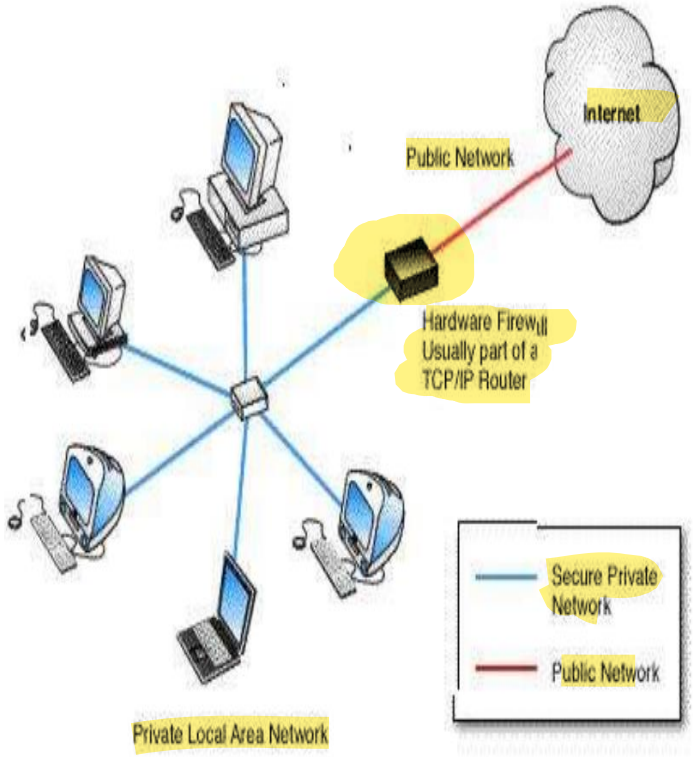
- Secure design and development
  - Integrate security considerations into the application architecture and coding practices.
- Code review and testing
  - Conduct comprehensive code reviews and testing to identify and address security vulnerabilities.
- Security testing and evaluation
  - Perform security testing to assess the effectiveness of implemented security controls.
- Deployment and monitoring
  - Ensure continued security through ongoing monitoring and maintenance.
- Authentication and authorization controls
  - Verify the identity of users or systems accessing an application, and determine what actions or resources a user can access.
- Security systems
  - Use security systems such as firewalls, web application firewalls (WAF), and intrusion prevention systems (IPS).
- Application security testing tools
  - Use tools such as Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), and Dependency scanners to detect vulnerabilities

Firewalls and its types

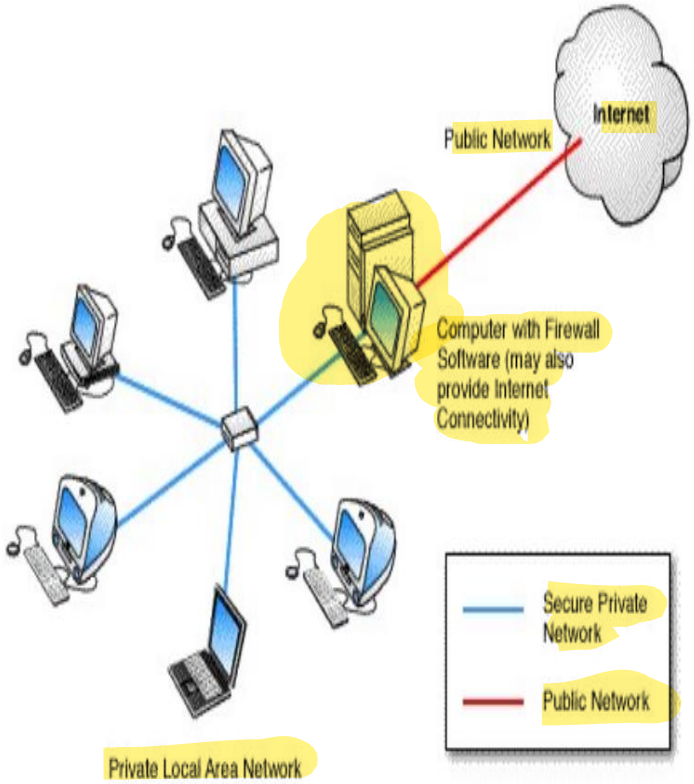
- A firewall is a security system that monitors and controls network traffic to prevent unauthorized access to a computer network.
- **Purpose**
  - A firewall's primary purpose is to create a barrier between a trusted internal network and an untrusted external network, like the internet.
- **How it works**
  - Firewalls inspect data packets and decide whether to allow or block them based on a set of rules. These rules can be based on criteria such as source and destination IP addresses, port numbers, and protocol type

Types of Firewall

Hardware firewall



Software firewall

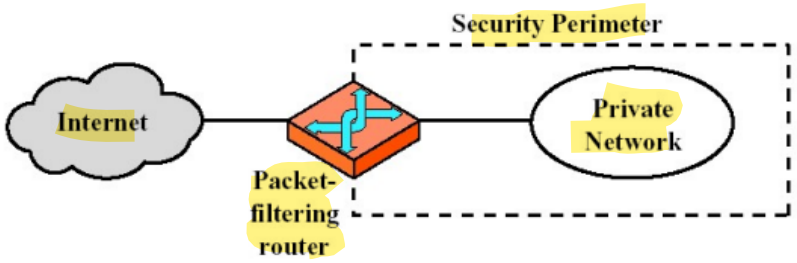


- Limitations of the firewalls
  - Cannot protect against attacks that bypass the firewall.
  - Does not protect against internal threats.
  - Cannot protect, in general, against transfer of virus-infected programs or files.

Types of firewalls

- Packet filtering router (works at the network layer, IP)
- Circuit-level gateway (works at the transport layer, TCP)
- Application-level gateway (works at higher layers)

Packet-filtering router



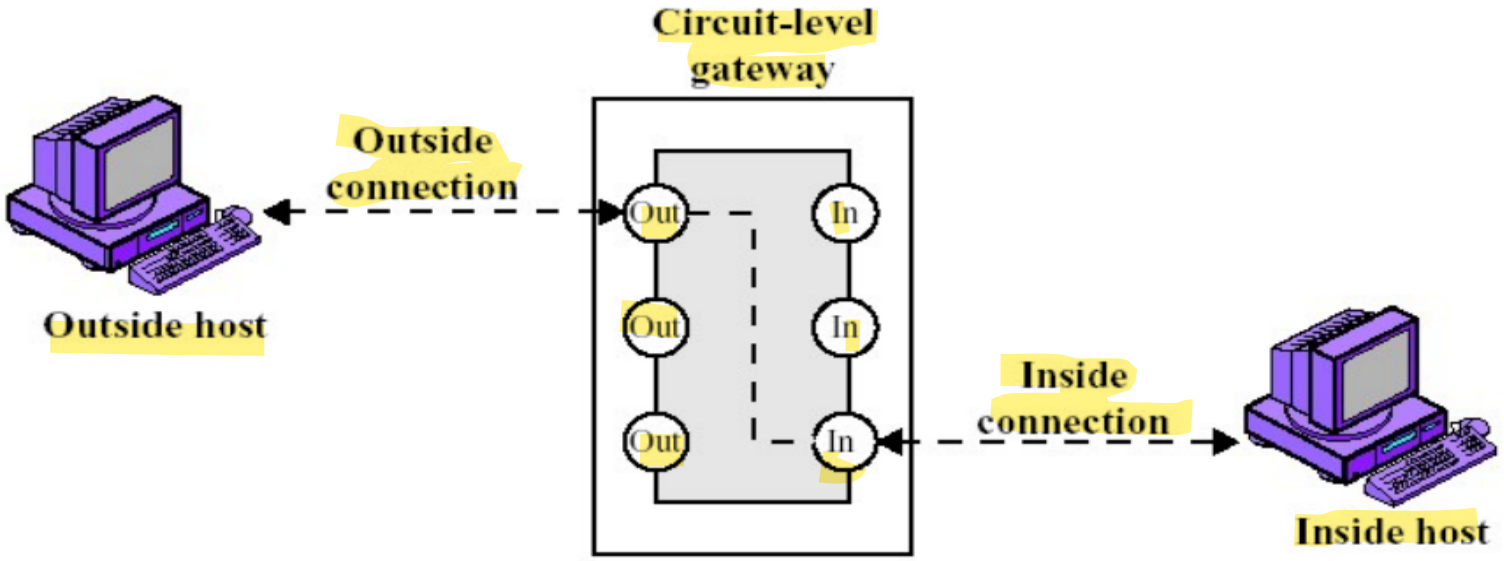
(a) Packet-filtering router

- A packet-filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet.
- Filtering is based on information contained in a network packet

Filtering rules

- Filtering rules are based on
- **Source IP address**
- **Destination IP address**
- **Source and Destination transport-level address**: transport level port number
- **IP protocol field**: defines the transport protocol

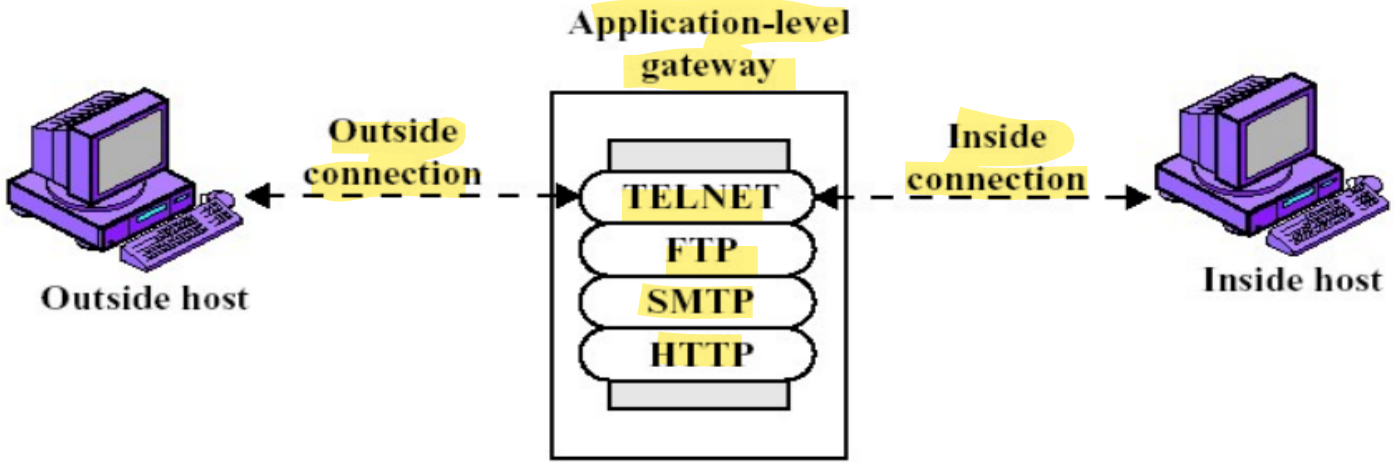
Circuit-level gateway



(c) Circuit-level gateway

- Traffic is filtered based on specified *session* rules, like:
  - a session is initiated by a recognized computer;
- A circuit-level gateway sets up two connections:
  - One between itself and a TCP user on the inner host;
  - One between itself and a TCP user on the outer host;
- Once connections are established and security criteria are met , both connections are linked by the gateway;

Application-level gateway



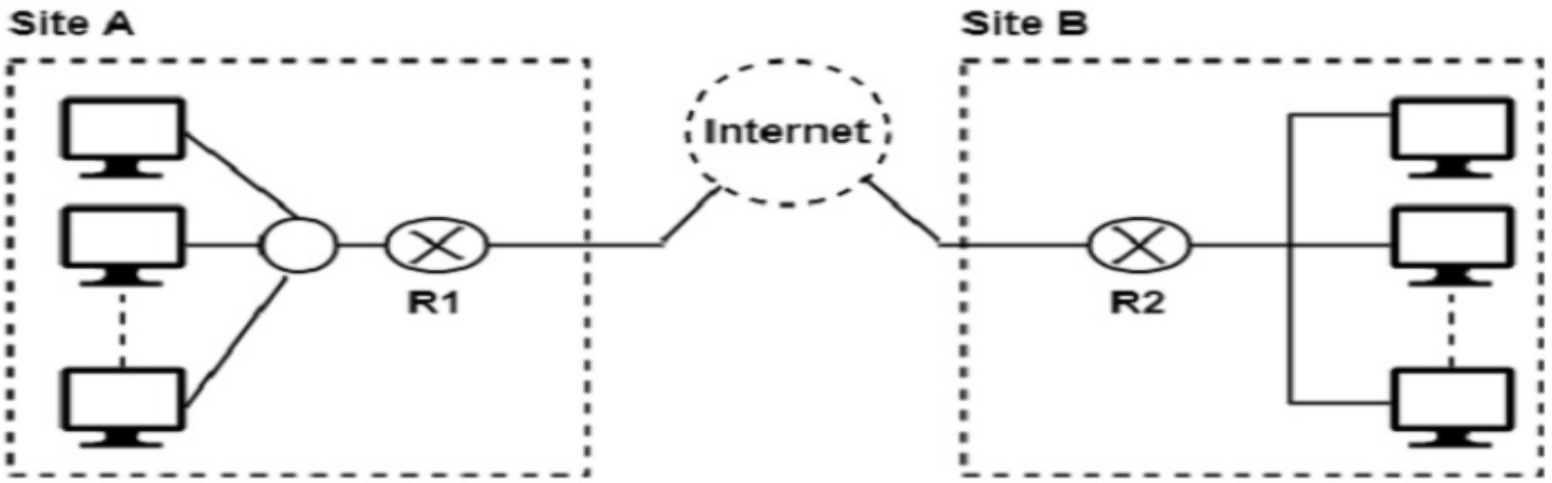
(b) Application-level gateway

- They can filter packets at the application layer of the OSI model.
- Incoming or outgoing packets cannot access services for which there is no proxy:
  - for example, an application level gateway that is configured to be a web proxy will not allow any ftp, telnet or other traffic through.
- They can filter application specific commands such as http:post and get, etc.

virtual private network

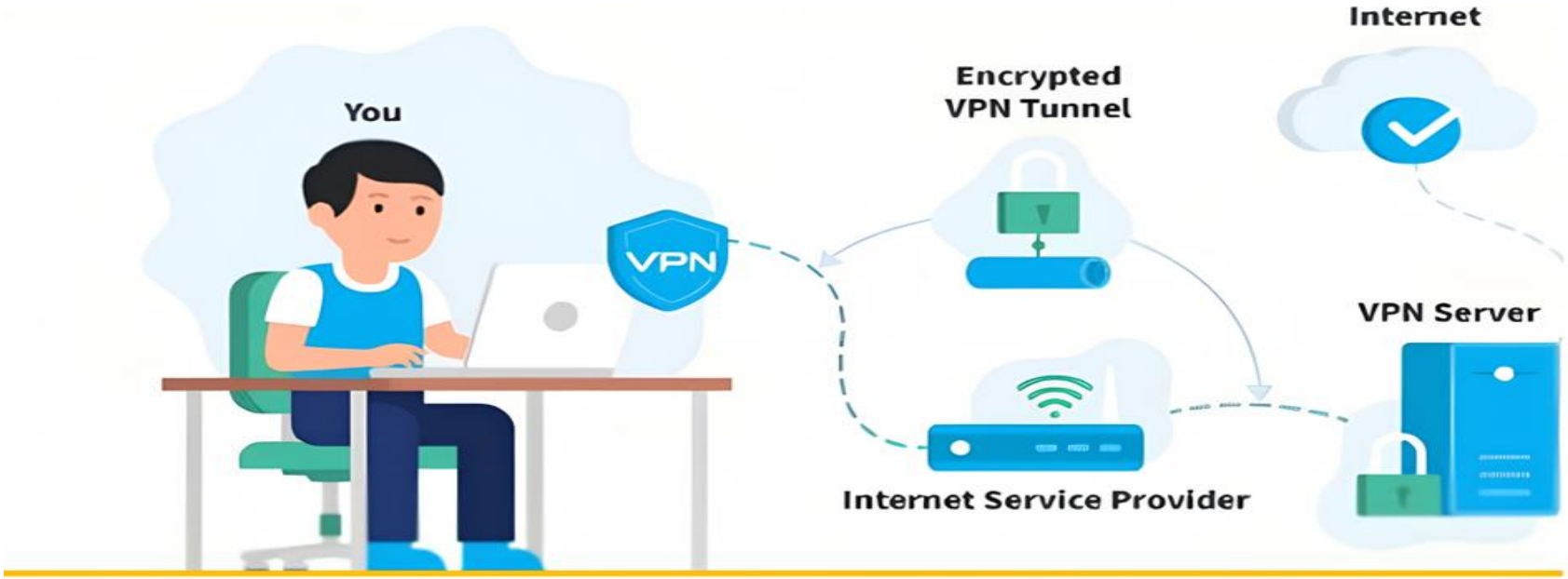
- A virtual private network (VPN) is a network architecture that creates a secure connection between a device and a remote server over the internet.
- VPNs are used to protect sensitive data, mask IP addresses, and bypass firewalls and website blocks.

A VPN connection is shown in the figure below –



In this figure, Routers R1 and R2 use VPN technology to guarantee privacy for the organization.

- # Types of VPNs
  - **Router VPN**
  - The first type uses a router with added VPN capabilities. A VPN router cannot only handle normal routine duties, but it can also be configured to form VPNs over the internet to other similar routers located in remote networks.
  - **Firewall VPN**
  - The second type of VPN is one built into a firewall device. Firewall VPN can be used both to support remote users and also to provide VPN links.
  - **Network Operating System**
  - The third type of VPNs include those offered as part of a network operating system like Windows NT, Windows 2000, and Netware 5. These VPNs are commonly used to support remote access, and they are generally the least expensive to purchase and install.



Tunneling protocol and types

- Tunnelling is a protocol for transferring data securely from one network to another.
- Using a method known as *encapsulation*, Tunnelling allows private network communications to be sent across a public network, such as the Internet.
- Encapsulation enables data packets to appear general to a public network when they are private data packets, allowing them to pass unnoticed.

- Tunneling protocols are a common way to establish a VPN connection. Here are some types of tunneling protocols:
- **Layer 2 Tunneling Protocol (L2TP)**
  - A protective tunnel for data that's often used with IPsec to keep information safe while traveling between a computer and a corporate network.
- **Point-to-point Tunneling Protocol (PPTP)**
  - Uses PPP and TCP/IP to create secure, virtual connections across networks. PPTP uses encrypted connections, or "tunnels", to send network data packets to servers.
- **Internet Protocol Security (IPsec)**
  - A tunneling protocol that secures data communication between two networks. It restricts access from unwanted sources and allows organizations to securely connect two networks that may operate on different protocols.
- **OpenVPN**
  - An open-source tunneling protocol that's considered one of the best tunneling protocols because many developers have tested it for weaknesses.
- **Secure Socket Tunneling Protocol (SSTP)**
  - A tunneling protocol that's built off of previous generations like L2TP to offer more robust encryption and connectivity. SSTP is based on a combination of SSL and TCP technologies.

IDS vs. IPS

Objective	IPS		IDS	
	In-line, Automatic Block	Priority	Out-of-band, Human Alert	Priority
Stability	› Crash is catastrophic – network goes down	1	› Crash is annoying to security analysts who lose visibility – but no impact on network or apps	4
Performance	› Processing designed for peak network load (Gbps) › Small memory buffers (µsecs of latency) › Above required for interior network deployment and application transparency	2	› Processing designed for average network loads › Large memory buffers to absorb traffic bursts, creating seconds to minutes of latency › Above okay since out-of-band and well within human response time	3
Accuracy - False Positives	› False blocks @ Gbps rates and thousands of filters – kills applications	3	› Burdens security analysts with chasing false alarms	2
Accuracy - False Negatives	› Preventing automatic blocking of good traffic trumps failure to detect anomalies	4	› Missed anomalies may be missed attacks (information is power)	1

IPS and their Types

- **Network-Based IPS:** A Network-Based IPS is installed at the network perimeter and monitors all traffic that enters and exits the network.
- **Host-Based IPS:** A Host-Based IPS is installed on individual hosts and monitors the traffic that goes in and out of that host.
- **Content-based IPS (CBIPS)** – A content-based IPS (CBIPS) check the content of network packets for specific sequences, known as signatures. It can identify and hopefully prevent known types of attack including worm infections and hacks.
- **Rate-based IPS (RBIPS)** – Rate-based IPS (RBIPS) are primarily designed to avoid Denial of Service and Distributed Denial of Service attacks. They work by monitoring and understanding normal network behaviors.

Introduction to Web Application Vulnerabilities

- Web application vulnerabilities involve a system flaw or weakness in a web-based application.
- **SQL Injection Attacks**
  - Structured Query Language (SQL) is now so commonly used to manage and direct information on applications that hackers have come up with ways to slip their own SQL commands into the database.
- **Cross-Site Scripting (XSS)**
  - In an SQL injection attack, an attacker goes after a vulnerable website to target its stored data, such as user credentials or sensitive financial data. But if the attacker would rather directly target a website's users, they may opt for a cross-site scripting attack. Similar to an SQL injection attack, this attack also involves injecting malicious code into a website or web-based app.

- **Cross-Site Request Forgery (CSRF)**
  - A Cross-Site Request Forgery (CSRF) attack is when a victim is forced to perform an unintended action on a web application they are logged into. The web application will have already deemed the victim and their browser trustworthy, and so executes an action intended by the hacker when the victim is tricked into submitting a malicious request to the application.

END