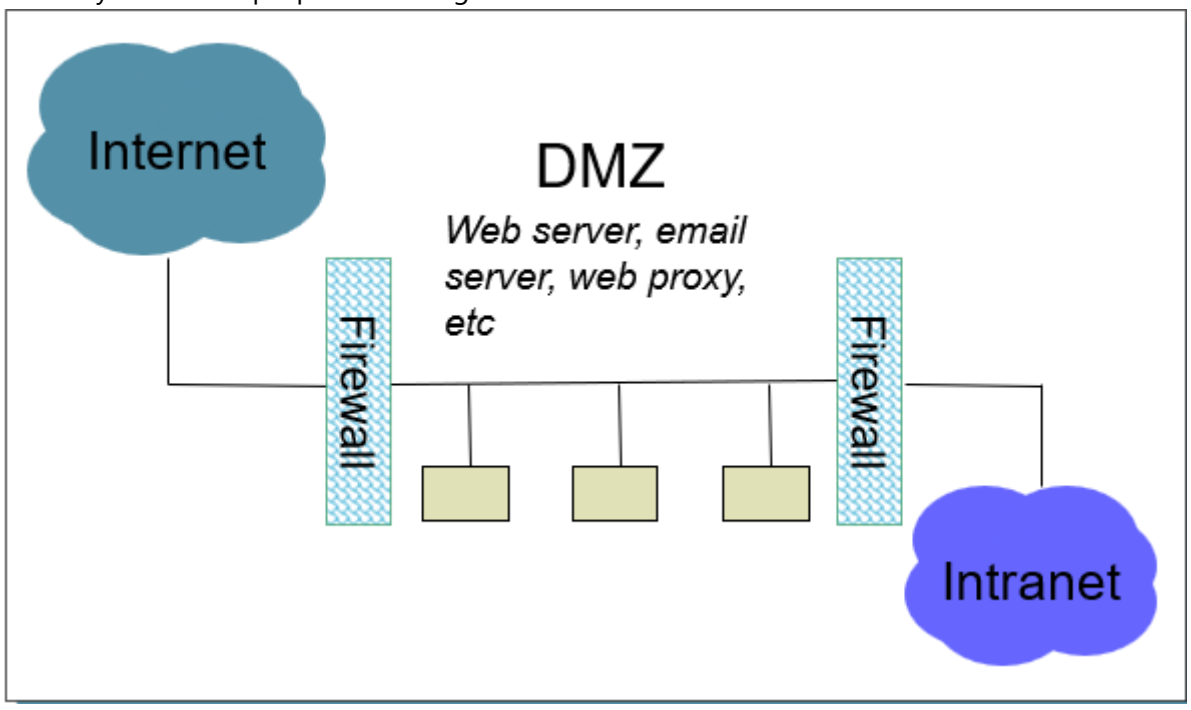
UNIT-3

Network security

- why is security needed
  - protect vital information while still allowing access to those that need it
  - provide auth and access control for resources
  - guarantee availability of resources

> anyone on the network is vulnerable to attacks

- common security attacks and countermeasures
  - finding ways into a net - firewall
  - exploiting S/W bugs - IDS
  - DoS - IDS
  - TCP hijacking - IPSec
  - packet sniffing - SSH, SSL, HTTPS
  - social problems - education
- firewall
  - net sec device that prevents unauth access to a net
  - monitors incoming + outgoing traffic using a predefined set of security rules to detect and prevent threats
  - separates a private net from the open Internet
  - H/W or S/W
  - filters incoming and outgoing traffic; if it goes down, the internal network is completely cut off and may also be suspceptible to congestion



  - types
    - packet filtering

            - control net qaccess by monitoring outgoing and incoming packets and allowing them to pass or stop based on source and dest IP addresses, protocols, and ports
            - treats each packet in isolation
        - stateful inspection
            - able to determine state of network connection travelling across such as TCP streams
            - only allow inbound TCP apcekts that are in response to conn initiated from within the internal network
        - stateless inspection
            - doesn't remember context wrt packets it processes
            - treats each packets in isolation, without considering previously processed packets
        - application layers
            - works like a proxy
            - inspect contents of traffic, blocking what it views as inapporpriate
        - software
            - set up locally or on cloud server
        - hardware
            - halts malicious data before it reaches the network endpoint that is in danger
    - DMZ(demilitarized zone)
        - phy or logical subnet that separates internal net from the Internet
        - exposes an org's external-facing services to an untrusted and larger net like the Internet
        - often found of corporate nets
        - net barrier b/w trusted and untrusted net
    - filtering rules
        - blacklist
            - all packets allowed except for those that fit the rules defined in the list
            - flexible in ensuring taht service to internal net is not disrupted
            - unexpected forms of malicious traffic could go through
        - whitelist
            - packets are dropped unless they are specifically allowed by the firewall
            - safer approach
            - however, must consider all possible forms of legitimate traffic
    - tunneling
        - tunneling protocols - comm b/w client and server is automatically encrypted to prevent eavesdropping
        - end-to-end encryption + decryption

- IDS(intrusion detection systems)
    - observes net traffic for malicious transactions and sends immediate alerts to the administrator
    - analyzes data looking for patterns(intrusion signatures) or abnormal behaviour
    - IDS managers compile data from IDS sensors to determine if an intrusion has occurred; raises an alarm if one has occurred
    - types
        - based on working
            - rule-based intrusion detection
                - rules and signatures identify the types of action that match known profiles of attacks

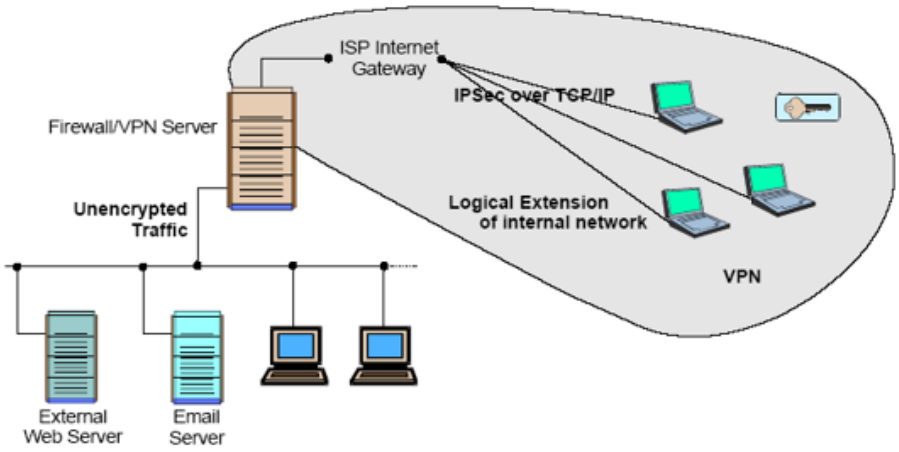
        - cannot detect unknown attacks
    - statistical
        - detremine when a user/host is acting unusually
        - alarm raised with host deviates significantly from teh stored profile for that person/machine
        - usually has a high false positive rate
- based on mode of deployment
    - NIDS(network)
        - set up at planned point within network to observe and examine traffic
    - HIDS(host)
        - run on independent hosts or devices on the net
        - only analyses incoming and outgoing net packets from that device
    - PIDS(protocol)
        - at the front end of a server, controlling and interpreting the protocol b/w a device and the server
    - APIDS(application protocol-based)
        - resides within a group of servers
        - interprets comm on application-specific protocols
    - hybrid
        - a combination of 2 or more of the types discussed above

- threats and vulnerabilities
    - threats
        - DoS(denial of service)
            - flooding target machine/server with surplus requests in an attempt to overload systems and rpevent some or all legitimate requests from being served
            - types
                - SYN attack
                - SMURF
            - how to handle
                - ingress filtering
                    - process of monitoring, controlling and restricting traffic entering a net to ensure that only legitimate traffic enters and unauth/malicious traffic is not
                - have refular security patches to fix vulnerabilities on a network
        - DDoS(distributed denial of service)
            - variant of DoS where a botnet is used to flood a server with illegitimate requests
            - harder to address than its basic counterpart
        - malware
            - malicious S/W to damage and gain access to unauth comp sys
            - viruses, worms, Trojans
        - phishing attacks
            - fradulent attempts to obtain sensitive info by posing as a trustworthy entity
        - MiTM
            - attacker secretly intercepts and alters comm b/w parties that think they;re directly comm b/w each other

        - packet sniffing/eavesdropping
            - unauth interception of net traffic to capture data transmitted over a net
            - attacker can learn sensitive info
            - how to protect yourself against such attacks
                - SSH over Telnet
                    - provides encryption
                - HTTP over SSL
                - SFTP over FTP
                - IPSec
        - zero-day exploits
            - target S/W vulnerabilities that are unknown to the S/W vendor or developer
            - attack performed before a fix or patch is available
        - TCP attacks
            - attacker intrudes in between a conn and sends false packets on the TCP connection
            - alters source IP, uses same sequence number and port numbers to pose as the legitimate source
            - mitigation
                - IPSec
                    - set of protools to provide confidentiality and authenticity for IP packets
                    - provides source authentication
                    - encrypts data before transporting it
                    - auth header provides integrity and data origin auth for IP datagrams
                    - ESP(encapsulating security payload) headers provide confidentiality, integrity and data origin auth
                    - modes
                        - transport mode
                        - tunnel mode
        - social engineering
    - vulnerabilities
        - weak passwords
        - unpatched S/W
            - leaving sys vulnerable to known exploits
        - insufficient net segmentation
            - allows attacker sto move within a network laterally if they compromise one such part
        - lack of encryption
            - not encrpyting sensitive data that is transmitted and stored on a network leaves it vulnerable to interception
        - outdated/unsupported sys
            - running S/W that is no longer supported/maintained exposes sys to known vulnerabilities

- VPN(virtual private network)
    - allows private nets to secruely comm b/w each other via a potentially unsecure public net, like the Internet
    - ensures data confidentiality, integrity and auth

- constructed on top of existing protocols
- types
  - remote access
    - allow authorized clients to access a priv net(intranet)
    - makes use of internal IPs
  - site-to-site
    - secure bridge b/w 2 or more physically distant nets



- IKE(Internet key exchange)
- secure network design

1. Network Segmentation:

- **Purpose**: Divide the network into smaller segments to reduce the attack surface and limit the impact of breaches.
- **Implementation**: Use VLANs (Virtual Local Area Networks) to logically segment traffic based on departments, functions, or security levels.
- **Benefits**: Isolation of critical assets, easier enforcement of security policies, and containment of threats.

2. Secure Perimeter:

- **Purpose**: Establish a strong boundary to protect internal resources from external threats.
- **Implementation**: Deploy firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gateway devices.
- **Benefits**: Control inbound and outbound traffic, block unauthorized access attempts, and detect/prevent malicious activities.

3. Access Control:

- **Purpose**: Ensure that only authorized users and devices can access network resources.
- **Implementation**: Use authentication methods such as strong passwords, multi-factor authentication (MFA), and certificates.
- **Benefits**: Prevent unauthorized access, enforce least privilege principle, and track user activities for auditing purposes.

4. Encryption:

- **Purpose**: Protect data confidentiality and integrity, especially over untrusted networks.
- **Implementation**: Utilize protocols like SSL/TLS for securing data in transit, and encrypt sensitive data at rest using strong algorithms.
- **Benefits**: Mitigate risks of eavesdropping, data tampering, and unauthorized access to sensitive information.

5. Network Monitoring and Logging:

- **Purpose**: Detect and respond to security incidents in real-time.
- **Implementation**: Deploy monitoring tools to analyze network traffic, detect anomalies, and generate alerts.
- **Benefits**: Early detection of threats, rapid incident response, and forensic analysis for post-incident investigations.

6. Regular Patch Management:

- **Purpose**: Address vulnerabilities in software and devices promptly.
- **Implementation**: Establish a process to regularly apply security patches and updates to all network components.
- **Benefits**: Minimize exposure to known vulnerabilities and reduce the risk of exploitation by attackers.

7. Redundancy and High Availability:

- **Purpose**: Ensure continuity of operations and resilience against failures or attacks.
- **Implementation**: Deploy redundant network paths, backup systems, and failover mechanisms.
- **Benefits**: Minimize downtime, maintain service availability during disruptions, and improve overall network reliability.

8. Secure Remote Access:

- **Purpose**: Enable secure access for remote users without compromising network security.
- **Implementation**: Use VPN (Virtual Private Network) technologies with strong encryption and access controls.
- **Benefits**: Securely extend the corporate network to remote locations or telecommuters, protecting data in transit.

9. Endpoint Security:

- **Purpose**: Protect devices (e.g., PCs, laptops, smartphones) connected to the network.
- **Implementation**: Install and maintain endpoint security solutions such as antivirus software, endpoint detection and response (EDR) tools, and mobile device management (MDM) systems.
- **Benefits**: Prevent malware infections, enforce security policies on endpoints, and detect/respond to suspicious activities.

10. User Awareness and Training:

- **Purpose**: Educate users about security best practices and potential threats.
- **Implementation**: Conduct regular security awareness training sessions, simulate phishing attacks, and provide guidelines for safe computing.
- **Benefits**: Enhance overall security posture by reducing human errors, improving incident reporting, and fostering a security-conscious culture.