Security Infrastructure

Objectives:

- 3.2 - Given a scenario, you must be able to apply security principles to secure enterprise architecture
- 4.5 - Given a scenario, you must be able to modify enterprise capabilities to enhance security

- **Security Infrastructure**
    - *Security Infrastructure*
        - Encompasses hardware, software, networks, data, and policies working cohesively for information asset safeguarding
    - Firewalls
        - Types
            - Web Application
            - Unified Threat Management
            - Next-generation
    - Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
        - Mechanisms
            - Identifying trends
            - Showcasing signatures
    - *Network Appliances*
        - *Specialized hardware or software for specific networking functions*
        - Functions
            - Load Balancing
            - Proxying

- Monitoring
- Security Enforcement

- *Port Security*
  - Restricting and controlling network access
  - *Basis*
    - Media Access Control (MAC) addresses
  - *Concepts*
    - 802.1x and EAP
- Securing Network Communications
  - Technologies
    - VPNs
    - IPSec
    - TLS
  - Objective
    - Create a secure backbone for communication
- Software-Defined Wide Area Networks (SD-WAN) and Secure Access Service Edge (SASE)
  - *SD-WAN*
    - Optimize WAN connections with software-defined principles
  - *SASE*
    - Cloud-based service integrating security and wide area networking
- Infrastructure Considerations
  - Aspects
    - Device placement, security zones, screen subnets, attack surfaces
  - Connectivity
    - Concerns and considerations

        - Device Attributes
            - Active vs. passive, inline vs. taps or monitors
        - Failure Mode Options
            - Fail-open or fail-closed for security devices
    - Selection of Infrastructure Controls
        - Choosing controls aligned with network needs
        - *Tailoring*
            - Ensuring robust security architecture

- **Ports and Protocols**
    - *Ports*
        - Logical communication endpoints on a computer or server
        - Classified as either
            - *Inbound*
                - Listening for connections
            - *Outbound*
                - Used to connect to a server
        - Example
            - SSH connection with an inbound port 22 and an outbound port on the client
    - Port Classification
        - *Well-Known Ports (0-1023)*
            - Assigned by IANA, commonly-used protocols
        - *Registered Ports (1024-49151)*
            - Vendor-specific, registered with IANA

- *Dynamic and Private Ports (49152-65535)*
  - Temporary outbound connections

- *Protocols*
  - Rules governing device communication and data exchange
  - Example
    - HTTPS (port 443) uses the HTTPS protocol for secure web communication
- Memorization Tips
  - Memorize for each port
    - Port number
    - Default protocol
    - Support for TCP or UDP
    - Basic description of the port or protocol
- List of Ports and Protocols
  - Port 21: FTP (File Transfer Protocol) - TCP
  - Port 22: SSH, SCP, SFTP - TCP
  - Port 23: Telnet - TCP
  - Port 25: SMTP (Simple Mail Transfer Protocol) - TCP
  - Port 53: DNS (Domain Name System) - TCP/UDP
  - Port 69: TFTP (Trivial File Transfer Protocol) - UDP
  - Port 80: HTTP (Hypertext Transfer Protocol) - TCP
  - Port 88: Kerberos - UDP
  - Port 110: POP3 (Post Office Protocol) - TCP
  - Port 119: NNTP (Network News Transfer Protocol) - TCP
  - Port 135: RPC (Remote Procedure Call) - TCP/UDP
  - Ports 137, 138, 139: NetBIOS - TCP/UDP
  - Port 143: IMAP (Internet Message Access Protocol) - TCP

- Port 161: SNMP (Simple Network Management Protocol) - UDP
- Port 162: SNMPTrap - UDP
- Port 389: LDAP (Lightweight Directory Access Protocol) - TCP
- Port 443: HTTPS (HTTP Secure) - TCP
- Port 445: SMB (Server Message Block) - TCP
- Ports 465, 587: SMTPS (SMTP Secure) - TCP
- Port 514: Syslog - UDP
- Port 636: LDAPS (LDAP Secure) - TCP
- Port 993: IMAPS (IMAP over SSL/TLS) - TCP
- Port 995: POP3S (POP3 over SSL/TLS) - TCP
- Port 1433: Microsoft SQL - TCP
- Ports 1645, 1646: RADIUS (Remote Authentication) - TCP
- Ports 1812, 1813: RADIUS UDP - UDP
- Port 3389: RDP (Remote Desktop Protocol) - TCP
- Port 6514: Syslog TLS - TCP

- Study Tips
  - Create flashcards with protocol, port, and connection details
  - Regularly test yourself to memorize ports and protocols
  - Understanding these is crucial for success in exams related to cybersecurity

- **Firewalls**
  - *Firewall*
    - A network security device or software that monitors and controls network traffic based on security rules
    - Protects networks from unauthorized access and potential threats

- *Screened Subnet (Dual-homed Host)*
  - Acts as a security barrier between external untrusted networks and internal trusted networks using a protected host with security measures like a packet-filtering firewall
- Types of Firewalls
  - *Packet Filtering Firewalls*
    - Inspect packet headers for IP addresses and port numbers
    - Limited in inspection, operates at Layer 4 (Transport Layer)
  - *Stateful Firewalls*
    - Track connections and requests, allowing return traffic for outbound requests
    - Operates at Layer 4, with improved awareness of connection state
  - *Proxy Firewalls*
    - Make connections on behalf of endpoints, enhancing security
    - Two Types of Proxy Firewalls
      - Session layer(Layer 5)
      - Application layer (Layer 7)
  - *Kernel Proxy Firewalls*
    - Minimal impact on network performance, full inspection of packets at every layer
    - Placed close to the system they protect
- Firewall Evolutions
  - *Next Generation Firewall (NGFW)*
    - *Application-aware*
      - distinguish between different types of traffic
    - Conduct deep packet inspection and use signature-based intrusion

protection

- Operate fast within minimal network performance impact
- Offer full-stack traffic visibility
- Can integrate with other security products
    - Can be a problem if organizations become reliant on a single vendor due to firewall configurations tailored to one product line

- *Unified Threat Management (UTM) Firewall*
    - Combines multiple security functions in a single device
    - Functions include firewall, intrusion prevention, antivirus, and more
    - Reduces the number of devices
    - Are a single point of failure
    - UTMs use separate individual engine
        - NGFW uses a single engine
- *Web Application Firewall (WAF)*
    - Focuses on inspecting HTTP traffic
    - Prevents common web application attacks like cross-site scripting and SQL injections
    - Can be placed
        - In-line (live attack prevention)
            - Device sits between the network firewall and the web servers
        - Out of band (detection)
            - Device receives a mirrored copy of web server traffic

- Layer based Firewalls
    - *Layer 4 Firewall*
        - Operates at the transport layer

        - Filters traffic based on port numbers and protocol data
    - *Layer 7 Firewall*
        - Operates at the application layer
        - Inspects, filters, and controls traffic based on content and data characteristics

- **Configuring Firewalls**
    - Firewalls and Access Control Lists (ACLs)
        - *Firewalls*
            - Dedicated devices for using Access Control Lists (ACLs) to protect networks
        - *Access Control Lists (ACLs)*
            - Essential for securing networks from unwanted traffic
            - Consist of permit and deny statements, often based on port numbers
            - Rule sets placed on firewalls, routers, and network infrastructure devices
            - Control the flow of traffic into and out of networks
            - May define quality of service levels inside networks but are primarily used for network security in firewalls
    - Configuring ACLs
        - A web-based interface or a text-based command line interface can be used
        - The order of ACL rules specifies the order of actions taken on traffic (top-down)
        - The first matching rule is executed, and no other ACLs are checked
        - Place the most specific rules at the top and generic rules at the bottom
        - Some devices support implied deny functions, while others require a "deny all" rule at the end
        - Actions taken by network devices should be logged, including deny actions

- ACL Rules
  - Made up of some key pieces of information including
    - Type of traffic
    - Source of traffic
    - Destination of traffic
    - Action to be taken against the traffic
- Firewall Types
  - *Hardware-Based Firewall*
    - A dedicated network security device that filters and controls network traffic at the hardware level
    - Commonly used to protect an entire network or subnet by implementing ACLs and rules
  - *Software-Based Firewall*
    - A firewall that runs as a software application on individual devices, such as workstations
    - Utilizes ACLs and rules to manage incoming and outgoing traffic, providing security at the software level on a per-device basis
- Key Takeaway
  - Firewalls use ACLs to control network traffic, ensuring security by specifying permitted and denied actions
  - Proper ACL configuration and rule order are crucial for effective network protection

- **IDS and IPS**
    - Key difference
        - IDS - Logs and alerts
        - IPS - Logs, alerts, and takes action
    - *Intrusion Detection Systems (IDS)*
        - Logs or alerts that it found something suspicious or malicious
        - Three Types of Intrusion Detection Systems (IDS)
            - *Network-based IDS (NIDS)*
                - Monitors the traffic coming in and out of a network
            - *Host-based IDS (HIDS)*
                - Looks at suspicious network traffic going to or from a single or endpoint
            - *Wireless IDS (WIDS)*
                - Detects attempts to cause a denial of a service on a wireless network
        - Intrusion detection systems operate either using signature-based or anomaly-based detection algorithms
            - *Signature-based IDS*
                - Analyzes traffic based on defined signatures and can only recognize attacks based on previously identified attacks in its database
                    - *Pattern-matching*
                        - Specific pattern of steps
                        - NIDS, WIDS
                    - *Stateful-matching*
                        - Known system baseline

- HIDS
- *Anomaly-based IDS*
  - Analyzes traffic and compares it to a normal baseline of traffic to determine whether a threat is occurring
  - Five Types of Anomaly-based Detection Systems
    - Statistical
    - Protocol
    - Traffic
    - Rule or Heuristic
    - Application-based

- *Intrusion Prevention Systems (IPS)*
  - Logs, alerts, and takes action when it finds something suspicious or malicious
  - Scans traffic to look for malicious activity and takes action to stop it

- **Network Appliances**
  - *Network Appliance*
    - A dedicated hardware device with pre-installed software for specific networking services
  - Different Types of Network Appliances
    - *Load Balancers*
      - Distribute network/application traffic across multiple servers
      - Enhance server efficiency and prevent overload
      - Ensure redundancy and reliability
      - Perform continuous health checks
      - Application Delivery Controllers (ADCs) offer advanced functionality
      - Essential for high-demand environments and high-traffic websites

- *Proxy Servers*
  - Act as intermediaries between clients and servers
  - Provide content caching, requests filtering, and login management
  - Enhance request speed and reduce bandwidth usage
  - Add a security layer and enforce network utilization policies
  - Protect against DDoS attacks
  - Facilitate load balancing and user authentication
  - Handle data encryption and ensure compliance with data sovereignty laws
- *Sensors*
  - Monitor, detect, and analyze network traffic and data flow
  - Identify unusual activities, security breaches, and performance issues
  - Provide real-time insights for proactive network management
  - Aid in performance monitoring and alerting
  - Act as the first line of defense against cyber threats
- *Jump Servers/Jump Box*
  - Secure gateways for system administrators to access devices in different security zones
  - Control access and reduce the attack surface area
  - Offer protection against downtime and data breaches
  - Simplify logging and auditing
  - Speed up incident response during cyber-attacks
  - Streamline system management and maintenance
  - Host essential tools and scripts
  - Monitor system health for performance and security

- **Port Security**
  - *Port Security*
    - A network switch feature that restricts device access to specific ports based on MAC addresses
    - Enhances network security by preventing unauthorized devices from connecting
  - *Network Switches*
    - Networking devices that operate at Layer 2 of the OSI model
    - Use MAC addresses for traffic switching decisions through transparent bridging
    - Efficiently prevent collisions, operate in full duplex mode
    - Remember connected devices based on MAC addresses
    - Broadcast traffic only to intended receivers, increasing security
  - *CAM Table (Content Addressable Memory)*
    - Stores MAC addresses associated with switch ports
    - Vulnerable to MAC flooding attacks, which can cause the switch to fail open
  - Port Security Implementation
    - Associate specific MAC addresses with interfaces
    - Prevent unauthorized devices from connecting
    - Can use Sticky MACs for easier setup
    - Susceptible to MAC spoofing attacks
  - *802.1x Authentication*
    - Provides port-based authentication for wired and wireless networks
    - Requires three roles
      - Supplicant
      - Authenticator
      - Authentication server
    - Utilizes RADIUS or TACACS+ for actual authentication

        - Prevents rogue device access
    - RADIUS vs. TACACS+
        - RADIUS is cross-platform, while TACACS+ is Cisco proprietary
        - TACACS+ is slower but offers additional security and independently handles authentication, authorization, and accounting
        - TACACS+ supports all network protocols, whereas RADIUS lacks support for some
    - *EAP (Extensible Authentication Protocol)*
        - A framework for various authentication methods
        - Has different variants which have their own features
            - *EAP-MD5*
                - Uses simple passwords and the challenge handshake authentication process to provide remote access authentication
                - One-way authentication process
                - Doesn't provide mutual authentication
            - *EAP-TLS*
                - Uses public key infrastructure with a digital certificate which is installed on both the client and the server
                - Uses mutual authentication
            - *EAP-TTLS*
                - REquires a digital certificate on the server, but not on the client
                - The client uses a password for authentication
            - *EAP-FAST*
                - Uses protected access credential, instead of a certificate, to establish mutual authentication
            - *PEAP*
                - Supports mutual authentication using server certificates and

Active Directory databases to authenticate a password from the client

- *EAP-LEAP*
  - Cisco proprietary and limited to Cisco devices

- Integration for Network Security
  - Combining port security, 802.1X, and EAP enhances network security
  - Ensures only authenticated and authorized devices can access sensitive resources

- **Securing Network Communications**
  - *Virtual Private Networks (VPNs)*
    - Extend private networks across public networks
    - Allow remote users to securely connect to an organization's network
    - Can be configured as site-to-site, client-to-site, or clientless VPNs
      - *Site-to-Site VPN*
        - Connects two sites cost-effectively
        - Replaces expensive leased lines
        - Utilizes a VPN tunnel over the public internet
        - Encrypts and secures data between sites
        - Slower, but more secure
      - *Client-to-Site VPN*
        - Connects a single host (e.g., laptop) to the central office
        - Ideal for remote user access to the central network
        - Options for full tunnel and split tunnel configurations
      - *Clientless VPN*
        - Uses a web browser to establish secure, remote-access VPN
        - No need for dedicated software or hardware client

        - Utilizes HTTPS and TLS protocols for secure connections to websites
    - In addition to site-to-site and client-to-site VPNs, we have to decide whether we are going to use a full tunnel or split tunnel VPN configuration
        - *Full Tunnel VPN*
            - Encrypts and routes all network requests through the VPN
            - Provides high security, clients fully part of central network
            - Limits access to local resources
            - Suitable for remote access to central resources
        - *Split Tunnel VPN*
            - Divides traffic, routing some through the VPN, some directly to the internet
            - Enhances performance by bypassing VPN for non-central traffic
            - Less secure; potential exposure to attackers
            - Recommended for better performance but requires caution on untrusted networks
- *Transport Layer Security (TLS)*
    - Provides encryption and security for data in transit
    - Used for secure connections in web browsers (HTTPS)
    - Uses Transmission Control Protocol (TCP) for secure connections between a client and a server
        - may slow down the connection
    - *Datagram Transport Layer Security (DTLS)*
        - A faster User Datagram Protocol-based (UDP-based) alternative
        - Ensures end-user security and protects against eavesdropping in clientless VPN connections

- Ensures confidentiality, integrity, and authentication of data

- *Internet Protocol Security (IPSec)*
  - A secure protocol suite for IP communication
  - Provides confidentiality, integrity, authentication, and anti-replay protection
  - Used for both site-to-site and client-to-site VPNs
  - Five key steps in establishing an IPSec VPN
    - Request to start the Internet Key Exchange (IKE)
      - PC1 initiates traffic to PC2, triggering IPSec tunnel creation by RTR1
    - Authentication - IKE Phase 1
      - RTR1 and RTR2 negotiate security associations for the IPSec IKE Phase 1 (ISAKMP) tunnel
    - Negotiation - IKE Phase 2
      - IKE Phase 2 establishes a tunnel within the tunnel
    - Data transfer
      - Data transfer between PC1 and PC2 takes place securely
    - Tunnel termination
      - Tunnel torn down including the deletion of IPSec security associations
  - IPSec Tunneling Modes (Data transfer)
    - *Transport Mode*
      - Uses original IP header
      - Suitable for client-to-site VPNs
      - Avoids potential fragmentation issues from MTU constraints
        - *MTU (Maximum Transmission Unit)*
          - set by default at 1500 bytes and may cause

fragmentation and other VPN problems

- Does not increase packet size
- *Tunneling Mode*
  - Adds a new header to encapsulate the entire packet
  - Ideal for site-to-site VPNs
  - May increase packet size and require jumbo frames
  - Provides confidentiality for both payload and header
- *Authentication Header (AH)*
  - Offers connectionless data integrity and data origin authentication for IP datagrams using cryptographic hashes as identification information
- *Encapsulating Security Payload (ESP)*
  - Provides confidentiality, integrity, and encryption
  - Provides replay protection
  - Encrypts the packet's payload

- Considerations
  - Balance between security and performance when choosing VPN tunnel type
  - Use full tunnel VPNs for higher security but reduced local access
  - Use split tunnel VPNs for better performance but potentially lower security
  - Ensure proper MTU settings when using tunneling mode in site-to-site VPNs
  - AH for integrity and ESP for encryption in IPSec, but both can be used together for comprehensive security

- **SD-WAN and SASE**
  - *SD-WAN (Software-Defined Wide Area Network)*
    - A virtualized approach to managing and optimizing wide area network connections

- Purpose
  - Efficiently routes traffic between remote sites, data centers, and cloud environments
- Benefits
  - Increased agility, security, and efficiency for geographically distributed workforces
- Control
  - Software-based architecture with control extracted from underlying hardware
- Transport Services
  - Allows the use of various transport services
    - MPLS
    - Cellular
    - Microwave links
    - Broadband internet
- Centralized Control
  - Utilizes centralized control function for intelligent traffic routing
- Traditional WAN vs. SD-WAN
  - *Traditional WANs*
    - Cannot efficiently integrate cloud services
  - *SD-WAN*
    - Enables dynamic and efficient routing, improving visibility, performance, and manageability
- Use Cases
  - Ideal for enterprises with multiple branch offices moving towards cloud-based services

        - IaaS
        - PaaS
        - SaaS
- *SASE (Secure Access Service Edge)*
    - A network architecture combining network security and WAN capabilities in a single cloud-based service
    - Purpose
        - Addresses challenges of securing and connecting users and data across distributed locations
    - Key Technology
        - Utilizes software-defined networking (SDN) for security and networking services from the cloud
    - Components
        - Firewalls
        - VPNs
        - Zero-trust network access
        - Cloud Access Security Brokers (CASBs)
    - Policy and Management
        - Delivered through a common set of policy and management platforms
    - Cloud Providers
        - Major cloud providers offer services aligned with SASE
        - Examples:
            - AWS VPC
            - Azure Virtual WAN
            - Azure ExpressRoutes
            - Google Cloud Interconnect

        - Google Cloud VPN
    - Alignment
        - These cloud services offer secure, flexible, and global networking capabilities, aligning with SASE principles
- Importance
    - As cyber threats evolve and organizations become more geographically dispersed, understanding and implementing SD-WAN and SASE are crucial for enhanced security and successful migration to cloud-based environments

- **Infrastructure Considerations**
    - Device Placement
        - Proper placement of routers, switches, and access points is crucial
        - Correct placement ensures
            - Optimal data flow,
            - Minimizes latency
            - Enhances security
        - Routers at the network's edge help filter traffic efficiently
        - Strategic placement of access points ensures coverage and reduces interference
        - Switches should be located for easy connection to network segments
    - Security Zones and Screened Subnets
        - *Security Zones*
            - Isolate devices with similar security requirements
        - *Screened Subnets*
            - Act as buffer zones between internal and external networks
            - Hosts public-facing services, protecting core internal networks
            - Use the term "screened subnet" instead of "DMZ" for modern

configurations

- *Attack Surface*
  - Refers to points where unauthorized access or data extraction can occur
  - A larger attack surface increases the risk of vulnerabilities
  - Identify and mitigate vulnerabilities to reduce the attack surface
  - Regularly assess and minimize the attack surface for network security
- Connectivity Methods
  - Choose connectivity methods that influence network performance, reliability, and security
  - Wired (e.g., Ethernet) offers stability and speed but restricts mobility
  - Wireless (e.g., Wi-Fi) provides flexibility but may suffer from interference and security issues
  - Consider factors like scalability, speed, security, and budget constraints when choosing connectivity methods
- Device Attributes
  - Consider whether devices are active or passive, and if they are inline or tapped
  - Active devices (e.g., intrusion prevention systems)
    - monitor and act on network traffic.
  - Passive devices (e.g., intrusion detection systems)
    - observe and report without altering traffic
  - Inline devices are in the path of network traffic
  - Taps and monitors capture data without disruption
  - Align device choices with network goals and challenges

- Failure Mode
  - Choose between "fail-open" and "fail-closed" modes to handle device failures
  - *Fail-open*
    - Allows traffic to pass during a failure, maintaining connectivity but reducing security
  - *Fail-closed*
    - Blocks all traffic during a failure, prioritizing security over connectivity
  - The choice depends on the organization's security policy and the criticality of the network segment

- **Selecting Infrastructure Controls**
  - *Control*
    - A protective measure put in place to reduce potential risks and safeguard an organization’s assets
  - Key Principles
    - *Least Privilege*
      - Users and systems should have only necessary access rights to reduce the attack surface
    - *Defense in Depth*
      - Utilize multiple layers of security to ensure robust protection even if one control fails
    - *Risk-based Approach*
      - Prioritize controls based on potential risks and vulnerabilities specific to the infrastructure
    - *Lifecycle Management*
      - Regularly review, update, and retire controls to adapt to the evolving

threat landscape

- *Open Design Principle*
  - Ensure transparency and accountability through rigorous testing and scrutiny of controls

- Methodology
  - Assess Current State
    - Understand existing infrastructure, vulnerabilities, and current controls
  - Gap Analysis
    - Identify discrepancies between current and desired security postures
  - Set Clear Objectives
    - Define specific goals for adding new controls (data protection, uptime, compliance, etc.)
  - Benchmarking
    - Compare your organization's processes and security metrics with industry best practices
  - Cost-Benefit Analysis
    - Evaluate the balance between desired security level and required resources
  - Stakeholder Involvement
    - Engage relevant stakeholders to ensure controls align with business operations
  - Monitoring and Feedback Loops
    - Continuously revisit control selection to adapt to evolving threats
- Best Practices
  - Conduct Risk Assessment
    - Regularly assess threats and vulnerabilities specific to your organization,

and update it with significant changes

- Align with Frameworks
  - Utilize established frameworks (e.g., NIST, ISO) to ensure comprehensive and tested methodologies
- Customize Frameworks
  - Tailor framework controls to your organization's unique risk profile and business operations
- Stakeholder Engagement and Training
  - Engage all relevant stakeholders in the decision-making process, and conduct regular training to keep the workforce updated on security controls and threats