1.0 Security Architecture

1.1 Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.

- **Services**
  - Load balancer
  - Intrusion detection system (IDS)/network intrusion detection system (NIDS)/wireless intrusion detection system (WIDS)
  - Intrusion prevention system (IPS)/network intrusion prevention system (NIPS)/wireless intrusion prevention system (WIPS)
  - Web application firewall (WAF)
  - Network access control (NAC)
  - Virtual private network (VPN)
  - Domain Name System Security Extensions (DNSSEC)
  - Firewall/unified threat management (UTM)/next-generation firewall (NGFW)
  - Network address translation (NAT) gateway
  - Internet gateway
  - Forward/transparent proxy
  - Reverse proxy
  - Distributed denial-of-service (DDoS) protection
  - Routers
  - Mail security
  - Application programming interface (API) gateway/Extensible Markup Language (XML) gateway
  - Traffic mirroring
    - Switched port analyzer (SPAN) ports
    - Port mirroring
    - Virtual private cloud (VPC)
    - Network tap
  - Sensors
    - Security information and event management (SIEM)
    - File integrity monitoring (FIM)
    - Simple Network Management Protocol (SNMP) traps
    - NetFlow
    - Data loss prevention (DLP)
    - Antivirus
- **Segmentation**
  - Microsegmentation
  - Local area network (LAN)/virtual local area network (VLAN)
  - Jump box
  - Screened subnet
  - Data zones
  - Staging environments
  - Guest environments
  - VPC/virtual network (VNET)
  - Availability zone
  - NAC lists
  - Policies/security groups
  - Regions
  - Access control lists (ACLs)
  - Peer-to-peer
  - Air gap
- **Deperimeterization/zero trust**
  - Cloud
  - Remote work
  - Mobile
  - Outsourcing and contracting
  - Wireless/radio frequency (RF) networks
- **Merging of networks from various organizations**
  - Peering
  - Cloud to on premises
  - Data sensitivity levels
  - Mergers and acquisitions
  - Cross-domain
  - Federation
  - Directory services
- **Software-defined networking (SDN)**
  - Open SDN
  - Hybrid SDN
  - SDN overlay

1.2 Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.

- **Scalability**
  - Vertically
  - Horizontally
- **Resiliency**
  - High availability
  - Diversity/heterogeneity
  - Course of action orchestration
  - Distributed allocation
  - Redundancy
  - Replication
  - Clustering
- **Automation**
  - Autoscaling
  - Security Orchestration, Automation, and Response (SOAR)
  - Bootstrapping
- **Performance**
- **Containerization**
- **Virtualization**
- **Content delivery network**
- **Caching**

1.3 Given a scenario, integrate software applications securely into an enterprise architecture.

- **Baseline and templates**
  - Secure design patterns/ types of web technologies
    - Storage design patterns
  - Container APIs
  - Secure coding standards
  - Application vetting processes
  - API management
  - Middleware
- **Software assurance**
  - Sandboxing/development environment
  - Validating third-party libraries
  - Defined DevOps pipeline
  - Code signing
  - Interactive application security testing (IAST) vs. dynamic application security testing (DAST) vs. static application security testing (SAST)
- **Considerations of integrating enterprise applications**
  - Customer relationship management (CRM)
  - Enterprise resource planning (ERP)
  - Configuration management database (CMDB)
  - Content management system (CMS)
  - Integration enablers
    - Directory services
    - Domain name system (DNS)
    - Service-oriented architecture (SOA)
    - Enterprise service bus (ESB)
- **Integrating security into development life cycle**
  - Formal methods
  - Requirements
  - Fielding
  - Insertions and upgrades
  - Disposal and reuse
  - Testing
    - Regression
    - Unit testing
    - Integration testing
  - Development approaches
    - SecDevOps
    - Agile
    - Waterfall
    - Spiral
    - Versioning
    - Continuous integration/ continuous delivery (CI/CD) pipelines
  - Best practices
    - Open Web Application Security Project (OWASP)
    - Proper Hypertext Transfer Protocol (HTTP) headers

1.4 Given a scenario, implement data security techniques for securing enterprise architecture.

- **Data loss prevention**
  - Blocking use of external media
  - Print blocking
  - Remote Desktop Protocol (RDP) blocking
  - Clipboard privacy controls
  - Restricted virtual desktop infrastructure (VDI) implementation
  - Data classification blocking
- **Data loss detection**
  - Watermarking
  - Digital rights management (DRM)
  - Network traffic decryption/ deep packet inspection
  - Network traffic analysis
- **Data classification, labeling, and tagging**
  - Metadata/attributes
- **Obfuscation**
  - Tokenization
  - Scrubbing
  - Masking
- **Anonymization**
- **Encrypted vs. unencrypted**
- **Data life cycle**
  - Create
  - Use
  - Share
  - Store
  - Archive
  - Destroy
- **Data inventory and mapping**
- **Data integrity management**
- **Data storage, backup, and recovery**
  - Redundant array of inexpensive disks (RAID)

1.5 Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.

- **Credential management**
  - Password repository application
    - End-user password storage
    - On premises vs. cloud repository
  - Hardware key manager
  - Privileged access management
- **Password policies**
  - Complexity
  - Length
  - Character classes
  - History
  - Maximum/minimum age
  - Auditing
  - Reversable encryption
- **Federation**
  - Transitive trust
  - OpenID
  - Security Assertion Markup Language (SAML)
  - Shibboleth
- **Access control**
  - Mandatory access control (MAC)
  - Discretionary access control (DAC)
  - Role-based access control
  - Rule-based access control
  - Attribute-based access control
- **Protocols**
  - Remote Authentication Dial-in User Server (RADIUS)
  - Terminal Access Controller Access Control System (TACACS)
  - Diameter
  - Lightweight Directory Access Protocol (LDAP)
  - Kerberos
  - OAuth
  - 802.1X
  - Extensible Authentication Protocol (EAP)
- **Multifactor authentication (MFA)**
  - Two-factor authentication (2FA)
  - 2-Step Verification
  - In-band
  - Out-of-band
- **One-time password (OTP)**
  - HMAC-based one-time password (HOTP)
  - Time-based one-time password (TOTP)
- **Hardware root of trust**
- **Single sign-on (SSO)**
- **JavaScript Object Notation (JSON) web token (JWT)**
- **Attestation and identity proofing**

1.6 Given a set of requirements, implement secure cloud and virtualization solutions.

- **Virtualization strategies**
  - Type 1 vs. Type 2 hypervisors
  - Containers
  - Emulation
  - Application virtualization
  - VDI
- **Provisioning and deprovisioning**
- **Middleware**
- **Metadata and tags**
- **Deployment models and considerations**
  - Business directives
    - Cost
    - Scalability
    - Resources
    - Location
    - Data protection
  - Cloud deployment models
    - Private
    - Public
    - Hybrid
    - Community
- **Hosting models**
  - Multitenant
  - Single-tenant
- **Service models**
  - Software as a service (SaaS)
  - Platform as a service (PaaS)
  - Infrastructure as a service (IaaS)
- **Cloud provider limitations**
  - Internet Protocol (IP) address scheme
  - VPC peering
- **Extending appropriate on-premises controls**
- **Storage models**
  - Object storage/file-based storage
  - Database storage
  - Block storage
  - Blob storage
  - Key-value pairs

1.7 Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.

- **Privacy and confidentiality requirements**
- **Integrity requirements**
- **Non-repudiation**
- **Compliance and policy requirements**
- **Common cryptography use cases**
  - Data at rest
  - Data in transit
  - Data in process/data in use
  - Protection of web services
  - Embedded systems
  - Key escrow/management
  - Mobile security
  - Secure authentication
  - Smart card
- **Common PKI use cases**
  - Web services
  - Email
  - Code signing
  - Federation
  - Trust models
  - VPN
  - Enterprise and security automation/orchestration

1.8 Explain the impact of emerging technologies on enterprise security and privacy.

- **Artificial intelligence**
- **Machine learning**
- **Quantum computing**
- **Blockchain**
- **Homomorphic encryption**
  - Private information retrieval
  - Secure function evaluation
  - Private function evaluation
- **Secure multiparty computation**
- **Distributed consensus**
- **Big Data**
- **Virtual/augmented reality**
- **3-D printing**
- **Passwordless authentication**
- **Nano technology**
- **Deep learning**
  - Natural language processing
  - Deep fakes
- **Biometric impersonation**