Domain 7 Infrastructure and Networking

Foundational Infrastructure Security Techniques:

- **Secure architecture:** properly segregating resources and networks.
- **Secure deployment and configuration:** hardening all cloud infrastructure components, including virtual machines (VMs), containers, storage, and networking.
- **Guardrails** are **preventative** and reactive controls that either block an undesired outcome (e.g., block use of regions, public object storage, or specific cloud services that aren't approved) or auto-remediate/correct a policy violation + logging and monitoring. **Amazon Web Service (AWS)** / **Microsoft Azure Policies** : enforce security policies.
- Customers can focus on securing what they consume and deploy on that infrastructure.
- **Single-region deployment :** vulnerable to regional outages.
- **Multi-region resiliency:** running parallel deployments of the application across multiple regions within the same cloud provider's network. = additional costs.(need to synchronize data across regions.)
- **Multi-provider resiliency:** hardest cloud resiliency / safeguard the application from a scenario in which an entire cloud provider goes down. / technological differences between cloud providers.

Cloud Network Fundamentals:

- Cloud networks : SDNs.
- Network administrators can dynamically configure and manage network resources through software. / SDN **can be used on any network** but **is the default on all IaaS providers.**
- Customers are not managing individual network components, such as routers, switches, and their access control lists (ACLs).
- Security groups most often apply to resources (e.g., instances), while ACLs apply to subnets /networks.
- **Load Balancer Service:** Is a service rather than a device. / Spreads traffic over multiple VMs running web servers. A foundation for other security services, such as Web Application Firewalls (**WAF**) and distributed denial-of-service **(DDOS) attack protection**.

Cloud Network Security & Secure Architectures:

- **Preventative Security Measures**:
  - **CSP Firewalls:** expl: Amazon Network Firewall / Azure Firewall : simplified management for both. **Limitations:** customization and advanced features.

    - **Virtual Appliances:** greater flexibility and control over firewall rules and configurations.
    - **WAFs** : protect web-facing applications from common exploits like SQL injection, cross-site scripting (XSS).
- **Detective Security Measures:**
    - **Flow Logs and DNS Logs*

Infrastructure as Code:

- Create complete infrastructure architectures : **Infrastructure-as-Code (IaC)**. The enabler for this is the API of the cloud management plane.
- Using machine-readable configuration files, rather than employing physical hardware configuration or interactive configuration tools". / dominant model for deploying cloud resources / deployed using continuous implementation/continuous delivery (CI/CD) automated pipelines. / Security scanning for misconfigurations can occur in the pipeline.
- Benefits : **Automated Compliance Checks** (every time infrastructure is provisioned or modified.) / **Consistent Security Posture** / **Rapid Rollback** (fixing update problems).
- Most cloud providers have native IaC tools / open-source products for IaC exist.

Software-Defined Perimeter & ZT Network Access:

- **Software Defined Perimeter (SDP):**
- Establishes a secure, "dark" network that is invisible to unauthorized users and devices.
- **Blackout approach**: Network is inaccessible by default.
- Users and devices **must authenticate** + **be authorized** before they can access the SDP-protected resources.
- **Identity-centric controls** + **Micro-segmentation.**
- How it works:
    - The **SDP Client** software opens a connection to the **SDP controller** (policy decision point (PDP) where access decision is taken.)
    - The network can be outside the control of the enterprise operating the SDP.
    - **SDP Gateway** : provides **authorized users and devices** with temporary access to protected processes and services. / monitoring, logging, and reporting on these connections.
    - **Invisible** to unauthorized users and devices.
- **Zero Trust Network Access (ZTNA)**:
- Replaces traditional VPNs with a more granular, application-specific access control model.
- Users are verified and authorized based on identity, device, location, and other contextual factors. / Access is provided to specific applications. Can be cloud-hosted (ZTNA-as-a-Service **(ZTNAaaS)**) or **on-premises**

Secure Access Service Edge:

- SASE is an emerging cybersecurity concept.
- Designed to address the challenges of securing endpoint devices and access to applications and data in a cloud-first.
- Centrally controlled endpoint agents and a global network of points of presence where security functions are executed.
- Common terms in this category include Firewalls, Next-Generation Firewalls, Proxies, Secure Web Gateways, Data Leakage Prevention (DLP) tools, and Cloud Access Security Brokers (CASB). They can filter traffic on IP addresses and ports, Web URLs, content inspection, user attributes, user behavior, threat intelligence, and more.