CompTIA Security+ Exam SY0-701

Lesson 6

Secure Cloud Network Architecture

Lesson 6

Topic 6A

Cloud Infrastructure

Cloud Deployment Models

- Public (or multi-tenant)
- Private
  - Hosted Private
- Community
- Hybrid Cloud

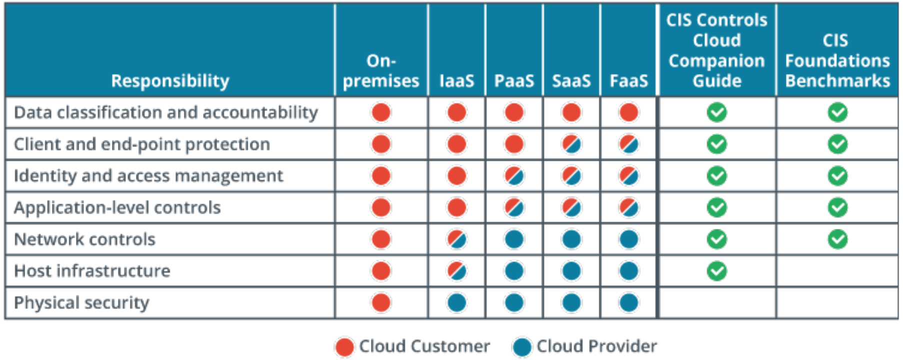
Cloud Deployment Models

- Security Considerations
- Single-tenant architecture
- Multi-tenant architecture
- Hybrid architecture
- Serverless architecture

Cloud Service Models

- Models
  - Software as a Service
  - Platform as a Service
  - Infrastructure as a Service
- Third-Party Vendors

Responsibility Matrix



Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS	CIS Controls Cloud Companion Guide	CIS Foundations Benchmarks
Data classification and accountability	🔴	🔴	🔴	🔴	🔴	✓	✓
Client and end-point protection	🔴	🔴	🔴	🔴🔵	🔴🔵	✓	✓
Identity and access management	🔴	🔴	🔴🔵	🔴🔵	🔴🔵	✓	✓
Application-level controls	🔴	🔴	🔴🔵	🔴🔵	🔴🔵	✓	✓
Network controls	🔴	🔴🔵	🔵	🔵	🔵	✓	✓
Host infrastructure	🔴	🔴🔵	🔵	🔵	🔵	✓	
Physical security	🔴	🔵	🔵	🔵	🔵		

🔴 Cloud Customer 🔵 Cloud Provider

Responsibility model

- Describes the balance of responsibility between a customer and a cloud service provider

Responsibility Matrix

- Cloud Service Provider
  - Physical security of the infrastructure
  - Securing computer, storage, and network equipment
  - Securing foundational elements of networking, such as DDoS protection
  - Cloud storage backup and recovery
  - Security of cloud infrastructure resource isolation among tenants
  - Tenant resource identity and access control
  - Security, monitoring, and incident response for the infrastructure
  - Securing and managing the datacenters located in multiple geographic regions

Responsibility Matrix

- Cloud Service Customer
  - User identity management
  - Configuring the geographic location for storing data and running services
  - User and service access controls to cloud resources
  - Data and application security configuration
  - Protection of operating systems, when deployed
  - Use and configuration of encryption, especially the protection of keys

Centralized and Decentralized Computing

- Centralized computing architecture
  - All data processing and storage is performed in a single location
  - All users and devices rely on the central server/authority
- Decentralized computing architecture
  - Data processing and storage distributed across multiple locations or devices
  - Increasingly important design trend impacting modern infrastructures

Centralized and Decentralized Computing

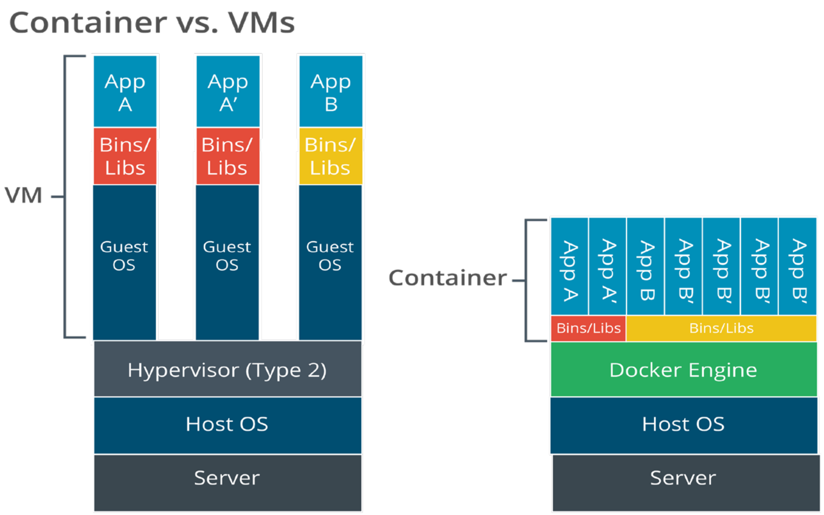
- Decentralized computing examples
  - Blockchain
  - Peer-to-peer (P2P)
  - Content Delivery Networks (CDNs)
  - Internet of Things (IoT)
  - Distributed databases
  - TOR (The Onion Router)

Resilient Architecture Concepts

- Replication
- High Availability Across Zones
  - Local replication
  - Regional replication
  - Geo-redundant storage (GRS)

Application Virtualization and Container Virtualization

- Application virtualization
- Containerization
- Container versus virtual machine



Comparison of VMs versus containers.

Cloud Architecture

- Virtual Private Cloud (VPC)
  - A cloud computing model in which the cloud provider manages the infrastructure and automatically allocates resources as needed, charging only for the actual usage of the application
- Serverless Computing
  - A private network segment made available to a single cloud consumer on a public cloud
- Microservices
  - An architectural approach to building software applications as a collection of small and independent services focusing on a specific business capability

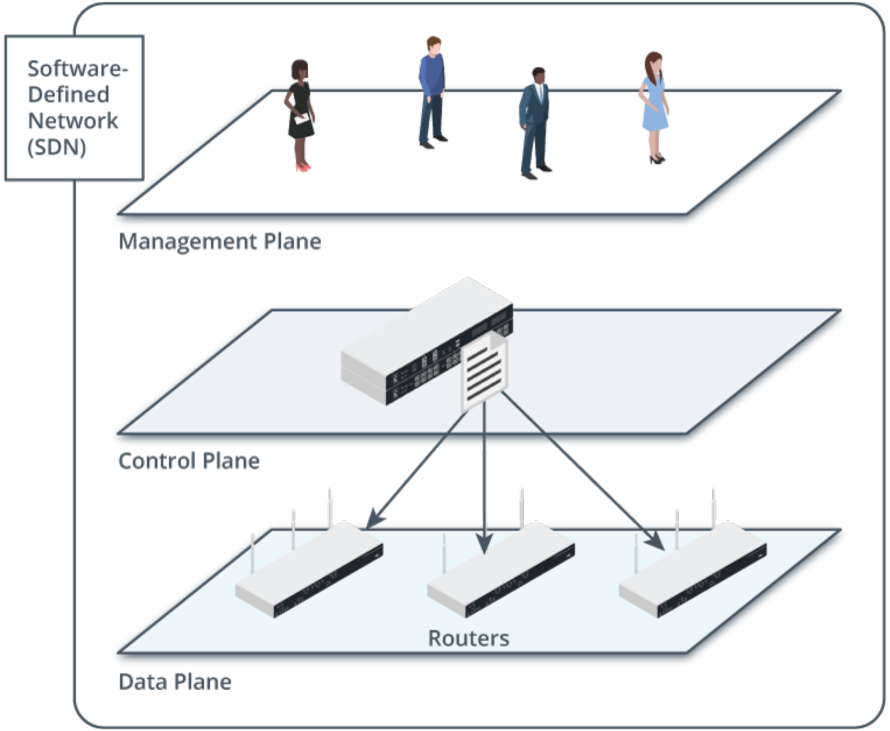
Cloud Automation Technologies

- Infrastructure as Code (IaC)
- Responsiveness
  - Load Balancing
  - Edge Computing
  - Auto-Scaling

Software Defined Networking

- Network functions are divided into three “planes”
- Control plane
    - Decisions about how traffic should be prioritized, secured, and where it should be switched
- Data plane
    - Handles the switching and routing of traffic and imposition of security access controls
- Management plane
    - Monitors traffic conditions and network status

Software Defined Networking



Data plane devices managed by a control plane device and monitored by a management plane. (Images © 123RF.com.)

- SDN is an important part of the latest automation and orchestration technologies
- SDN architecture reduces complexity of enforcing security policy
- Enables fully automated deployment (or provisioning) of network links, appliances, and servers

Cloud Architecture Features

- Considerations for Cloud Infrastructure
- Cost
- Scalability
- Resilience
- Ease of deployment
- Ease of recovery
- SLA and ISA
- Power
- Compute

Cloud Security Considerations

- Considerations for Cloud Infrastructure Security
- Data protection
- Patching
- Secure Communication
  - Software-Defined Wide Area Network (SD-WAN)
- Secure Access
  - Secure Access Service Edge (SASE)

Review Activity: Cloud Infrastructure

- Cloud Deployment Models
- Cloud Services Models
- Responsibility Matrix
- Centralized and Decentralized Computing
- Resilient Architecture Concepts
- Application Virtualization and Container Virtualization
- Cloud Architecture
- Cloud Automation Technologies
- Software Defined Networking
- Cloud Architecture Features
- Cloud Security Considerations

Lab Activity

- Assisted Lab: Using Containers
- Assisted Lab: Using Virtualization

Lesson 6

Topic 6B

Embedded Systems and Zero Trust Architecture

Embedded Systems

- Specialized computers
- Many consumer and commercial use cases.
- Some examples:
  - Home appliances
  - Smartphones and tablets
  - Automotive systems
  - Industrial automation
  - Medical devices
  - Aerospace and defense
- Real-Time Operating Systems

Industrial Control Systems

- Industrial control systems (ICSs)
  - Human-machine interfaces (HMIs)
  - Data historian
  - Programmable Logic Controller (PLC)
  - Supervisory Control and Data Acquisition (SCADA)
- ICS/SCADA Applications
  - Energy
  - Industrial
  - Fabrication and manufacturing
  - Logistics
  - Facilities

Internet of Things

- Network of physical devices, vehicles, appliances, and other objects embedded with sensors, software, and connectivity, enabling them to collect and exchange data

- The significantly decreased cost of IoT sensors and devices over the past few years has made them more affordable and accessible to businesses and consumers

- Advances in connectivity technology, such as 5G and low-power wireless networks, have made connecting and managing large numbers of IoT devices easier and more efficient

Internet of Things

- Security Risks Associated with IoT
- Many IoT devices have limited processing power and memory
  - Difficult to implement stringent security controls
- Rushed to market
  - Lacking or misrepresented security capability
  - “Un-patchable”
- Lack of standards in design of IoT devices
- Collect and transmit sensitive information

Internet of Things

- Best Practice Guidance for IoT
- The Internet of Things Security Foundation (IoTSF)
  - https://iotsecurityfoundation.org
- Industrial Internet Consortium (IIC) Security Framework
  - https://www.iiconsortium.org/iisf/
- Cloud Security Alliance (CSA) IoT Security Controls Framework
  - https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework
- European Telecommunications Standards Institute (ETSI) IoT Security Standards
  - https://www.etsi.org/technologies/consumer-iot-security

Deperimeterization and Zero Trust

- Deperimeterization
  - Shifts focus from defending the network boundaries to protecting individual resources
- Zero Trust
  - “Never trust, always verify”

Deperimeterization and Zero Trust

- Trends Driving Deperimeterization
- Cloud
- Remote Work
- Mobile
- Outsourcing & Contracting
- Wireless Networks

Deperimeterization and Zero Trust

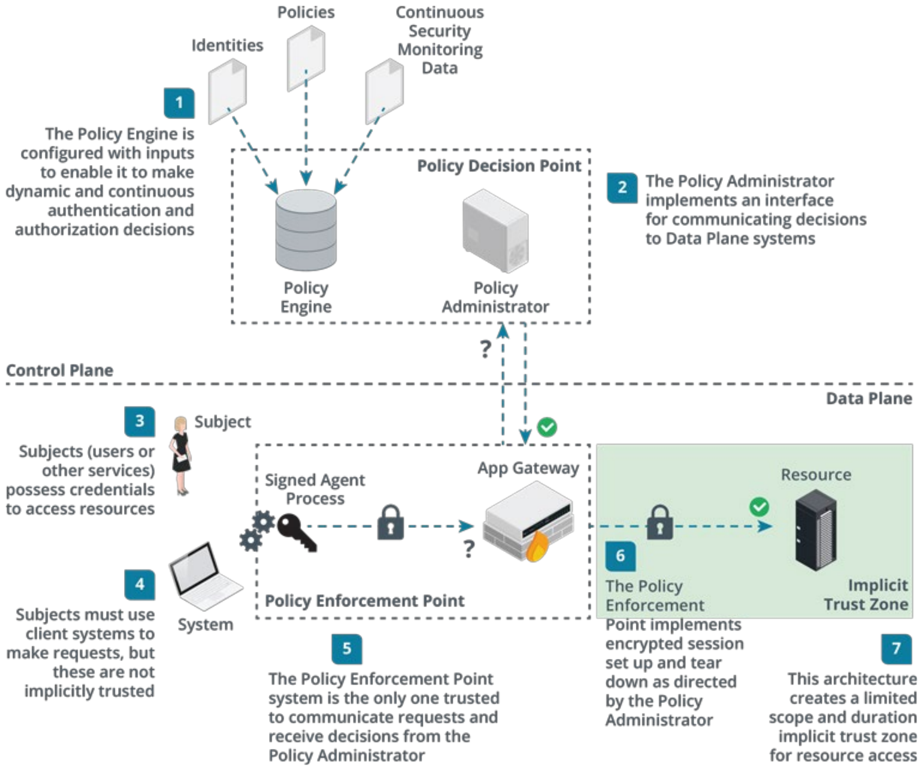
- The Key Benefits of a Zero Trust Architecture
- Greater security
- Better access controls
- Improved governance and compliance
- Increased granularity

Deperimeterization and Zero Trust

- Essential Components of a Zero Trust Architecture
- Network and endpoint security
- Identity and access management (IAM
- Policy-based enforcement
- Cloud security
- Network visibility
- Network segmentation
- Data protection
- Threat detection and prevention

Zero Trust Security Concepts

- Assumes that all devices, users, and services are not inherently trusted, regardless of whether inside or outside a network's perimeter



1 The Policy Engine is configured with inputs to enable it to make dynamic and continuous authentication and authorization decisions

2 The Policy Administrator implements an interface for communicating decisions to Data Plane systems

3 Subjects (users or other services) possess credentials to access resources

4 Subjects must use client systems to make requests, but these are not implicitly trusted

5 The Policy Enforcement Point system is the only one trusted to communicate requests and receive decisions from the Policy Administrator

6 The Policy Enforcement Point implements encrypted session set up and tear down as directed by the Policy Administrator

7 This architecture creates a limited scope and duration implicit trust zone for resource access

Components in NIST's zero trust architecture framework.

Review Activity: Embedded Systems and Zero Trust Architecture

- Embedded Systems
- Industrial Control Systems
- Internet of Things
- Deperimeterization and Zero Trust

CompTIA Security+ Exam SY0-701

Lesson 6

Summary