Welcome back to the CCSP Bootcamp

Your instructors:

Michael J Shannon

and

Dave Robichaud

Class will begin at 11:00 A.M. Eastern Standard Time (EST)

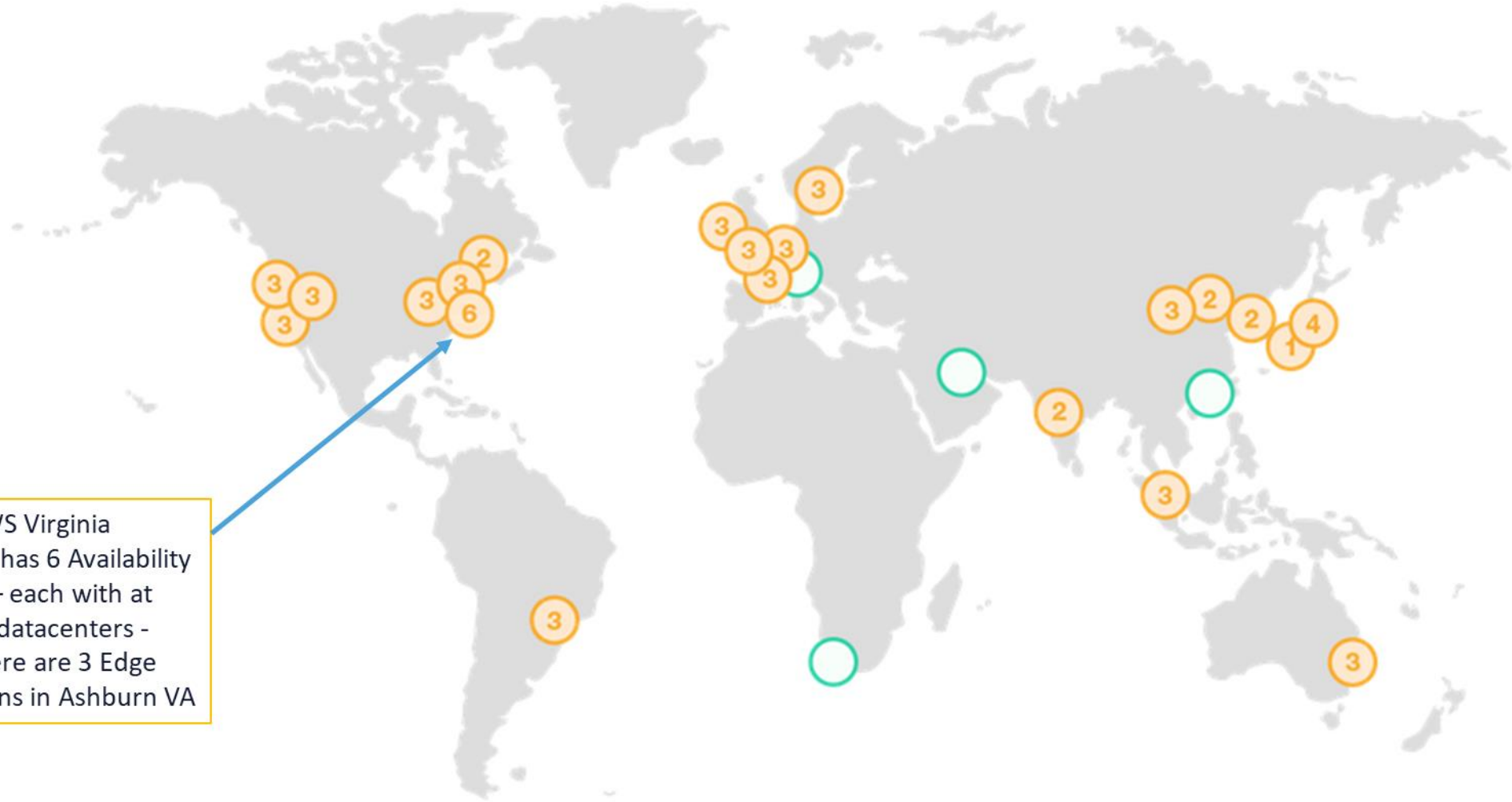
Domain 3

Cloud Platform and Infrastructure Security

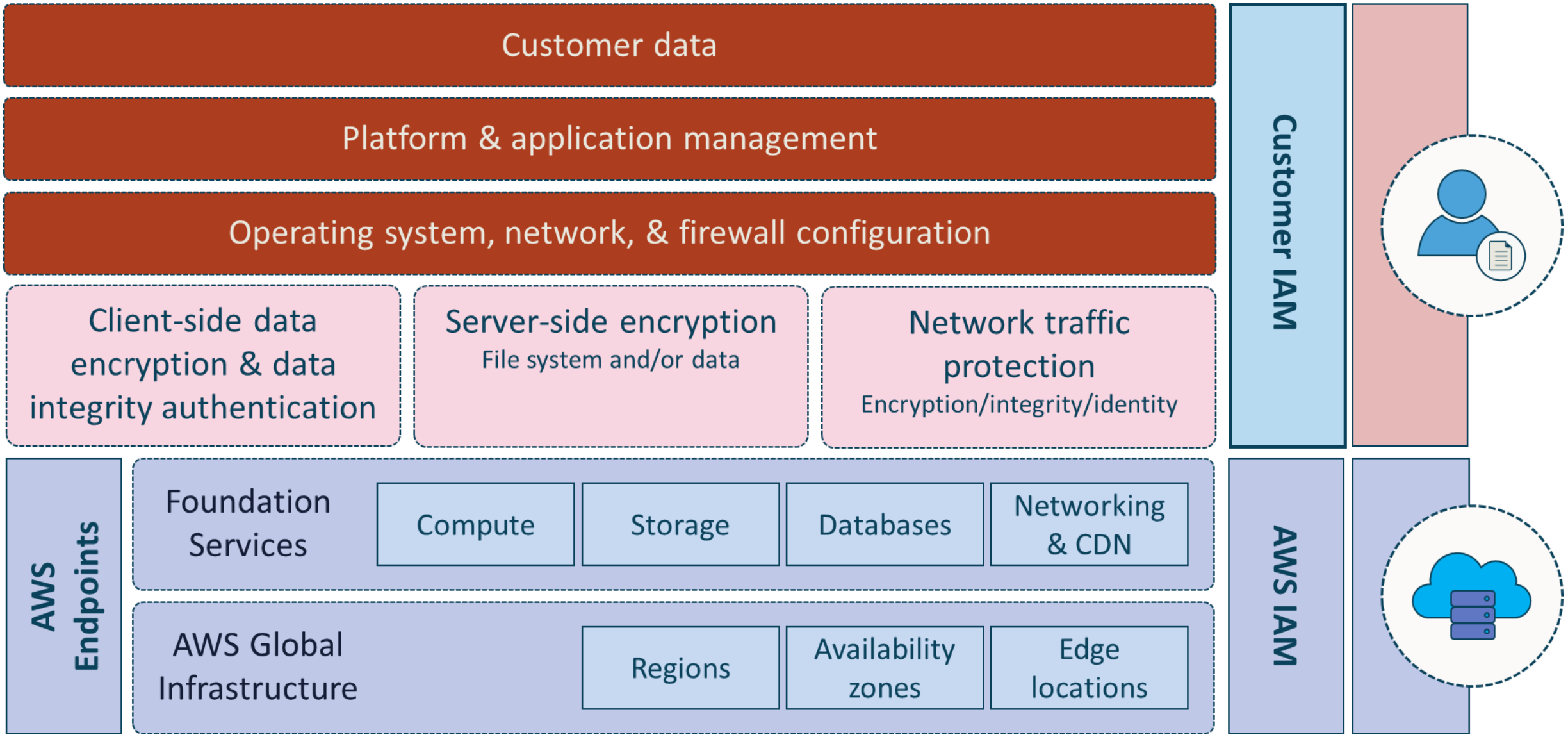
3.1 Comprehend Cloud Infrastructure Components

- Physical Environment
- Network and Communications
- Compute
- Virtualization
- Storage
- Management Plane

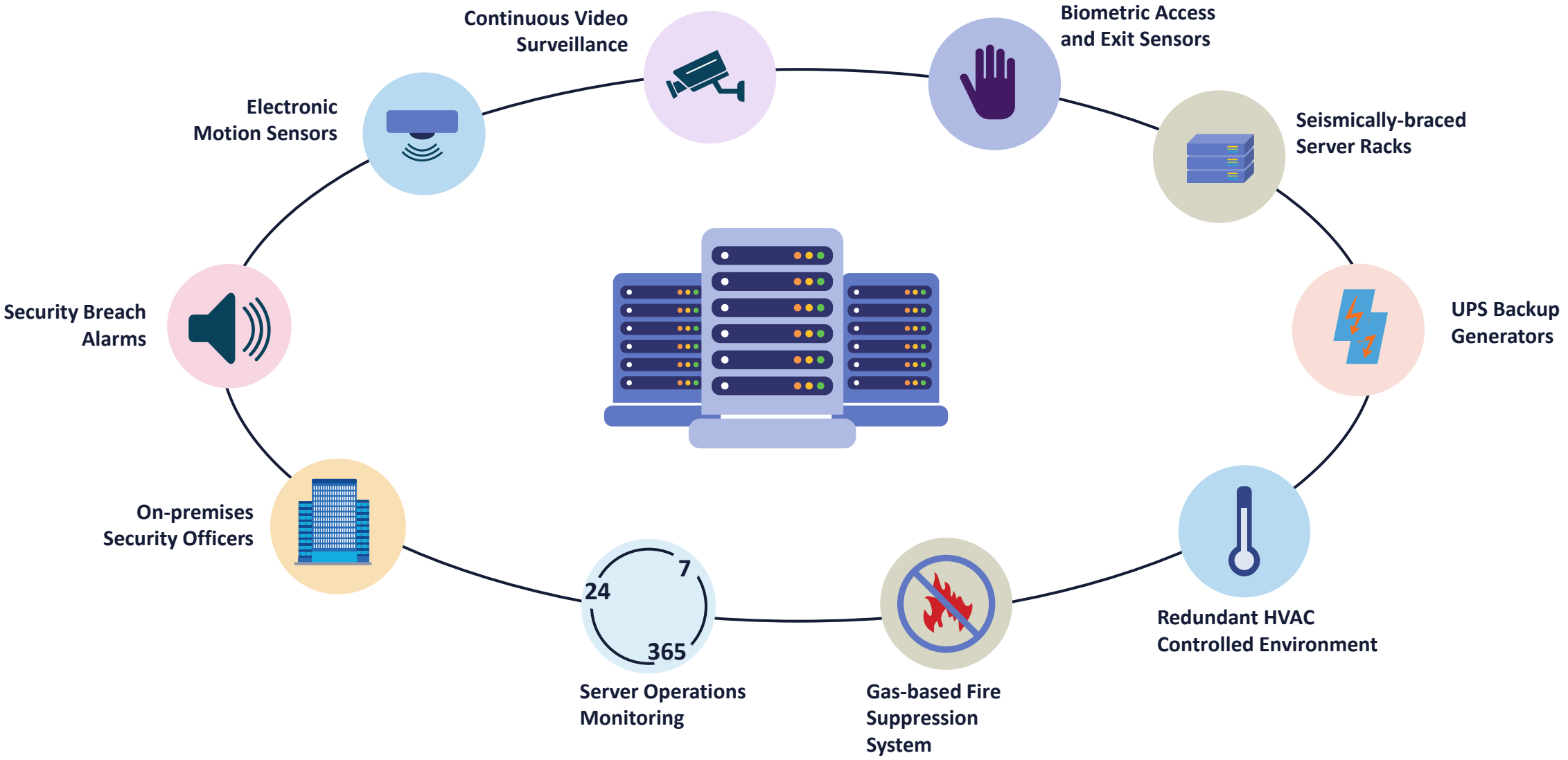
AWS Global Infrastructure



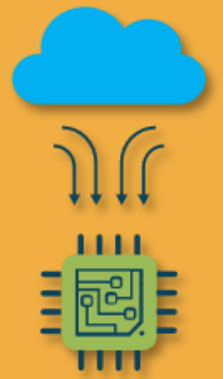
Cloud Service Provider Infrastructure



Cloud Datacenter Physical Security



Content Distribution (Delivery) Networks



CDN uses Edge Computing

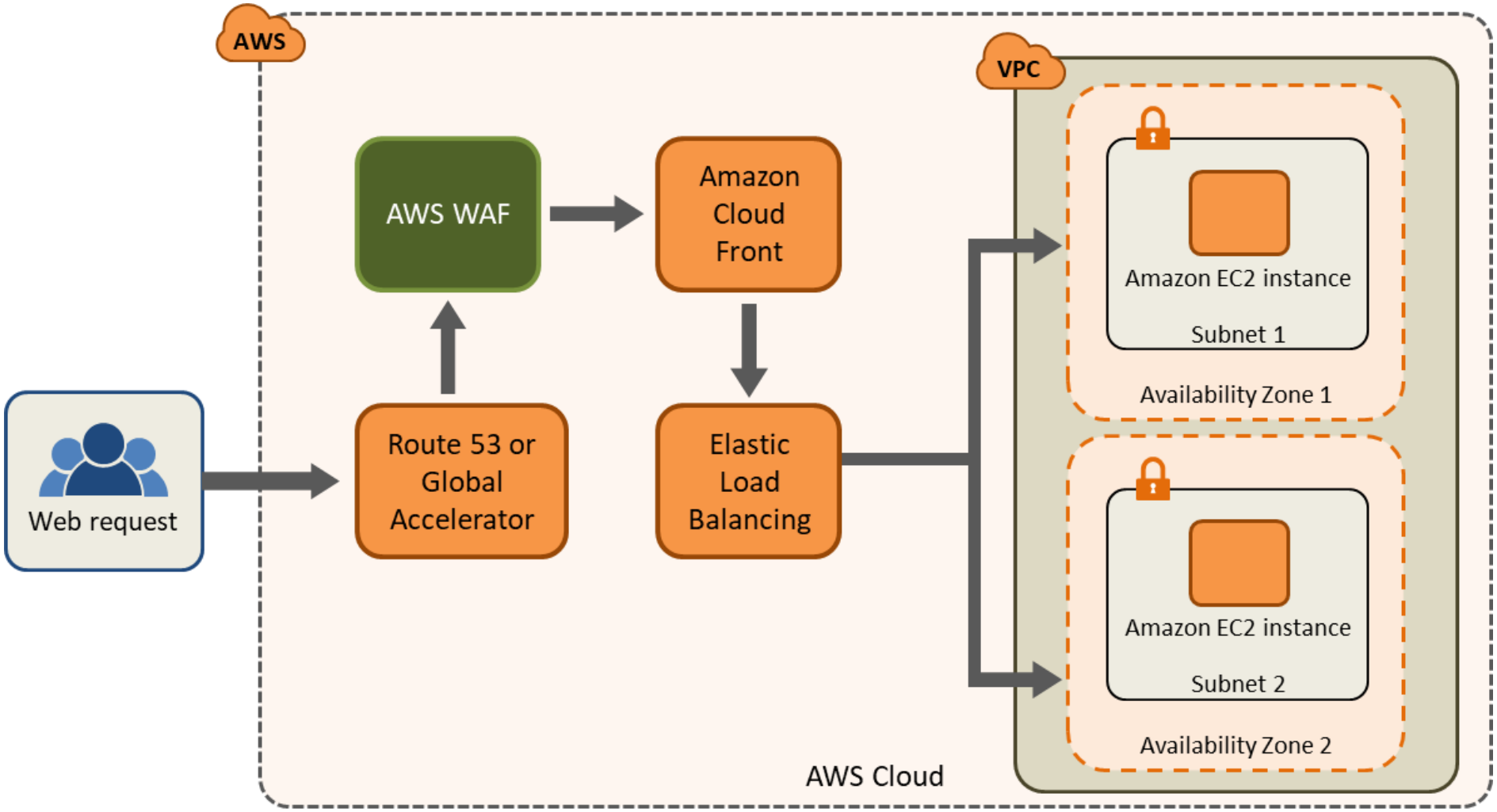
- A CDN is a highly-distributed platform of servers that reduces delays in loading web page content
- It reduces the physical distance between the server and the users around the world
- Without a CDN, origin servers would have to respond to every end user request, resulting in substantial traffic to the origin and subsequent load
- By responding to end user requests using modern edge computing and elastic caching, the CDN offloads traffic from content servers to metro edge locations
- Examples are Cloudflare, Akamai, Fastly, and AWS CloudFront

Content Distribution (Delivery) Networks

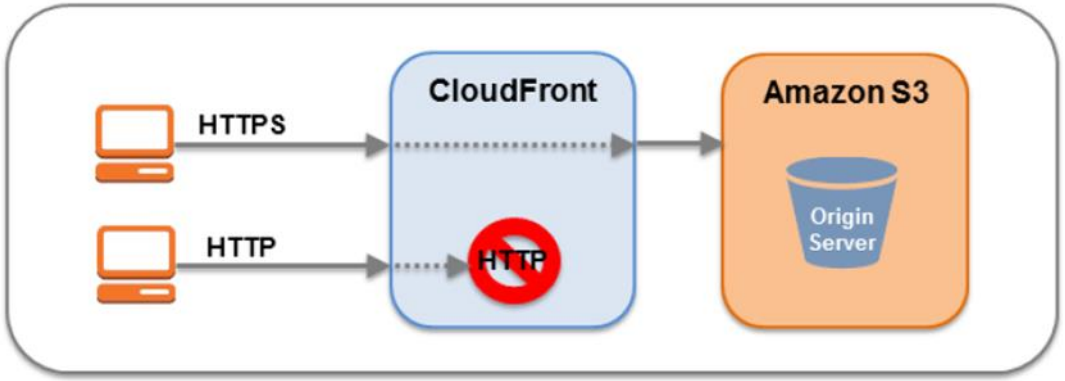
AWS CloudFront

- Amazon CloudFront is a fast CDN service like Akamai
- It securely delivers data, videos, applications, and APIs to customers at metro edge computing locations with low latency, high transfer speeds, and within a developer-friendly environment
- CloudFront is often integrated with AWS Redis ElastiCache at global provider partner locations and various service endpoints
- Functions seamlessly with Route 53, S3 object storage, Elastic Load Balancing, EC2 instances, WAF, and AWS Shield for DDoS protection

CloudFront at Amazon Web Services

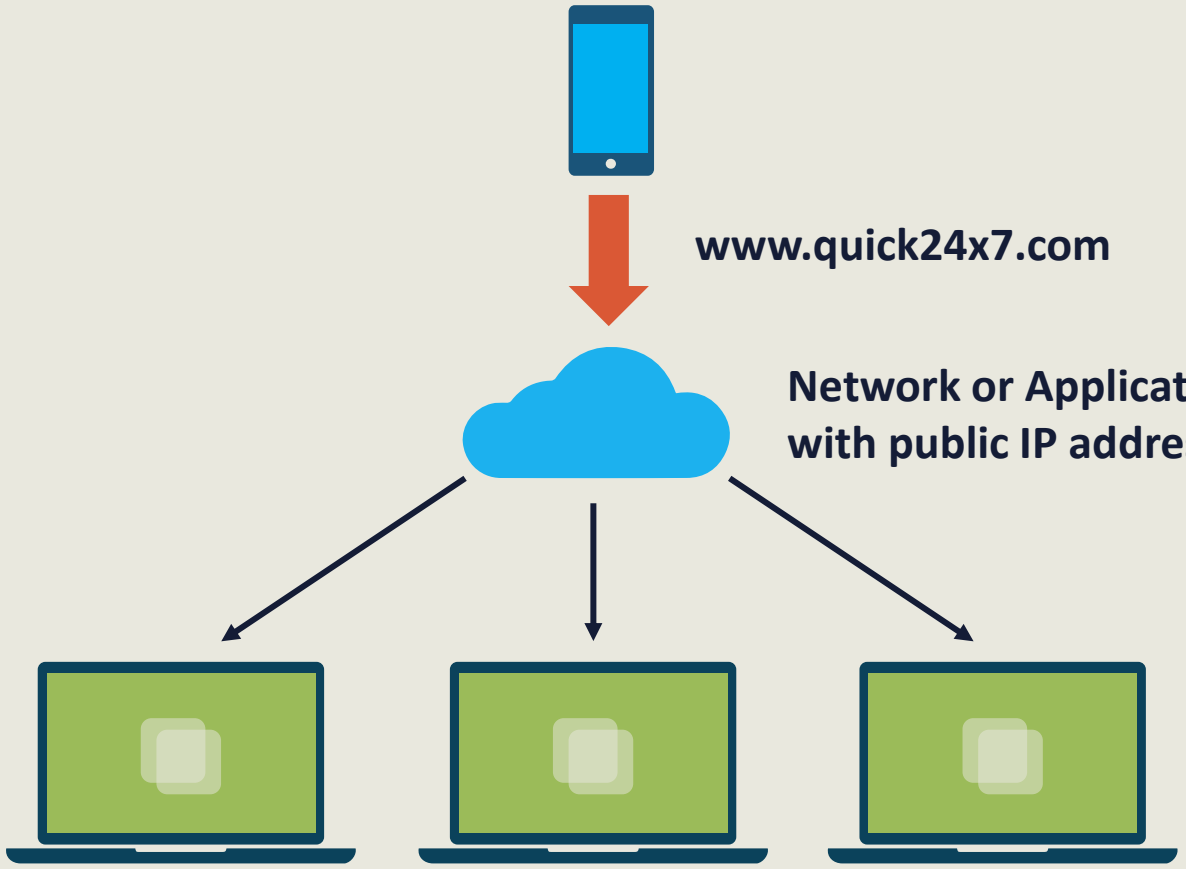


AWS CloudFront Security



- High-level data center physical security is in place
- **Uses TLSv1.1 and TLSv1.2** protocols for HTTPS connections between CloudFront and the custom origin web server
- Cipher suites use the **ECDHE** protocol on all connections
- **Private Content Feature** controls who can download content from CloudFront
- **Origin Access Identities** can control access to original copies of objects

CLOUD LOAD BALANCERS

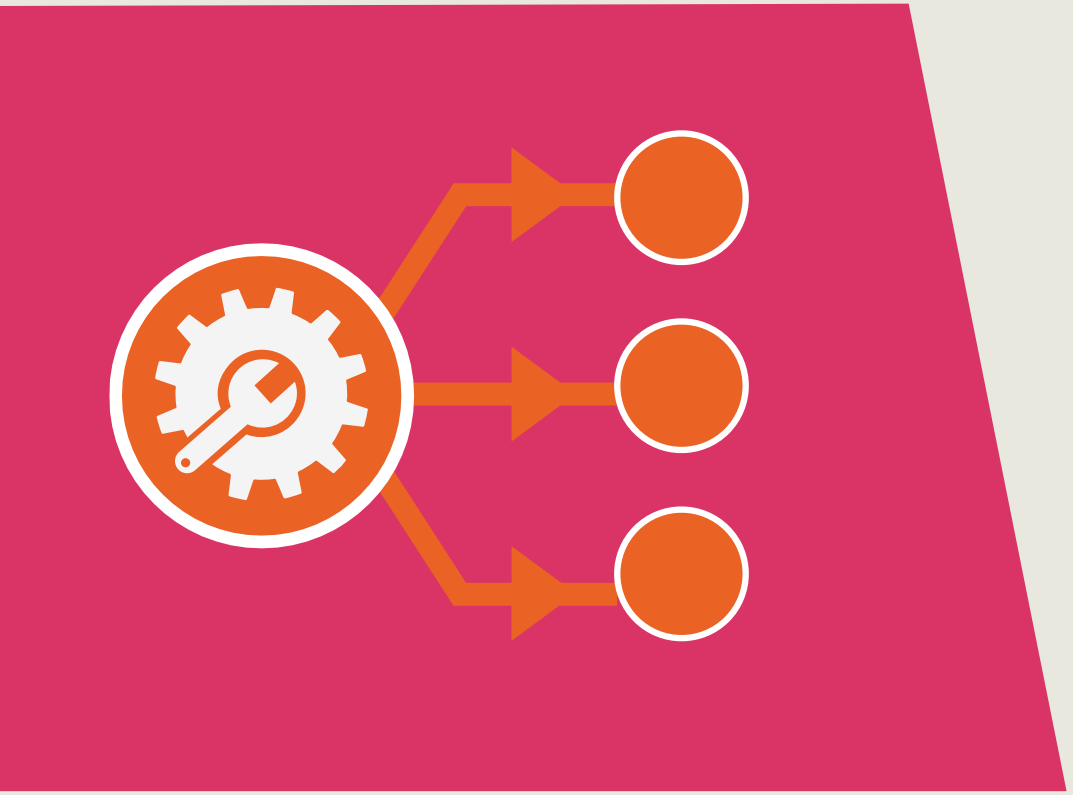


www.quick24x7.com

Network or Application Load balancer with public IP address

Backend virtual machines, containers, URLs to object storage, etc. – often Auto-scaling groups

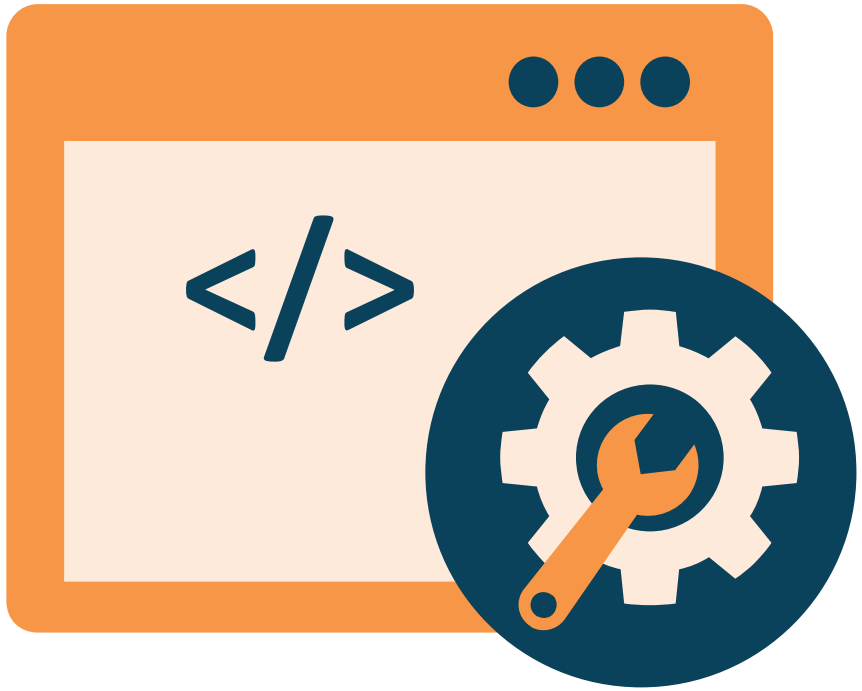
Secure Elastic LBs



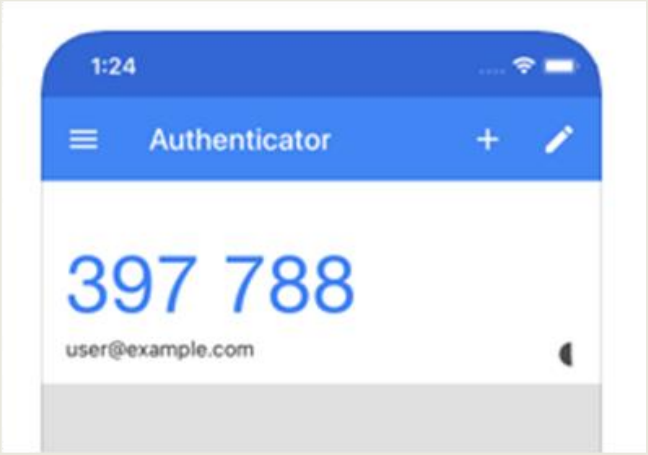
- Network (TCP, UDP, TLS) or Application (HTTPS/S) elastic load balancers are used at CSPs
- They can represent the virtual networks and resources to the public on the Internet
- Performs health checks on target instances
- Produces flow logs and DNS reports for visibility and Active Defense security
- Runs the TLS listener on Application LB to decrypt
- Can also have layer 3/4 and web application firewall (WebACL) applied

CSP Management Plane Protection

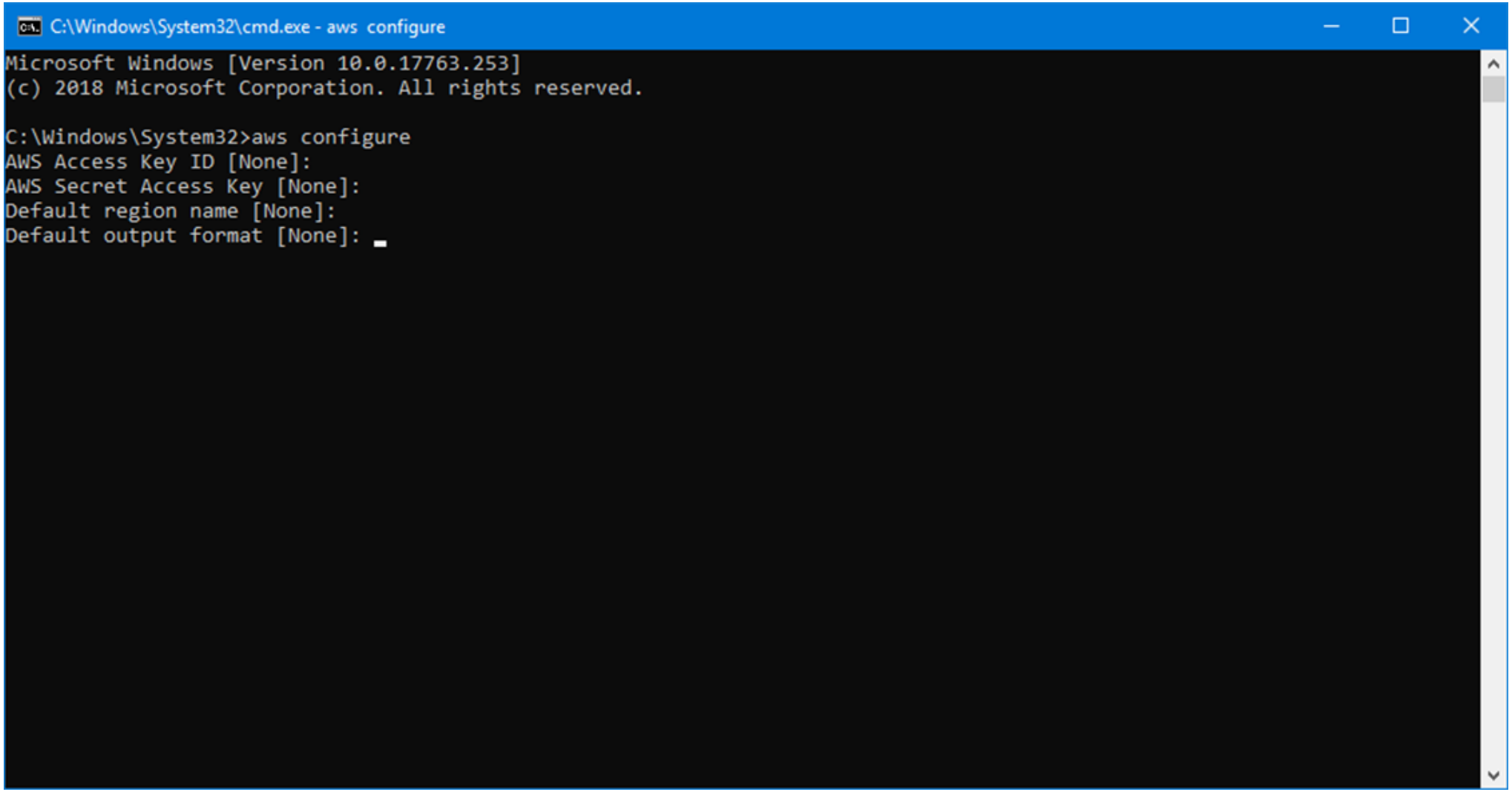
- All CSPs have systems management tools for managing the infrastructure using a graphical portals and IAM
- Can be used with IaaS and SaaS solutions
- Agent software is provided to install on Windows, Linux, and MacOS systems
- SSH2 sessions are setup initially then subsequent management sessions are protected with keys
- Managed services (AWS AppStream) can setup ad hoc management sessions when federated SSO using SAML 2.0 is used
- CLI, SDK, and other console-based access must be digitally signed



Use MFA on all Root and Service Accounts



Configuring CLI Access



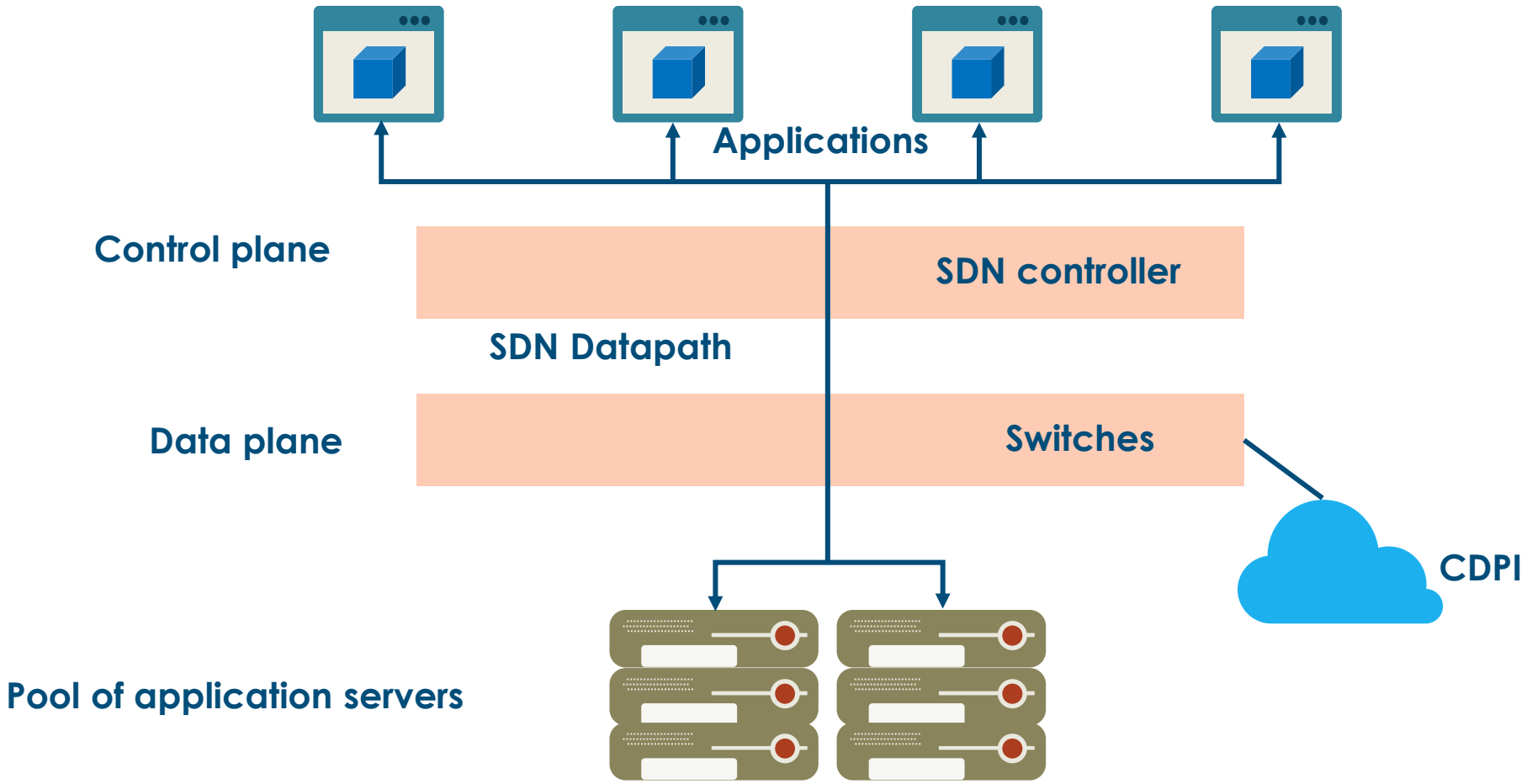
Managed Bastion Services

- Customers can instantiate self-hardened Windows and Linux servers in public subnets for SSH2 and RDP/TLS access to other systems for remote management
- CSPs prefer that customers use managed server-side solutions today where initial SSH2 handshakes are set up then used for subsequent management activities
- Strict least-privilege IAM must be employed

3.2 Design a Secure Data Center

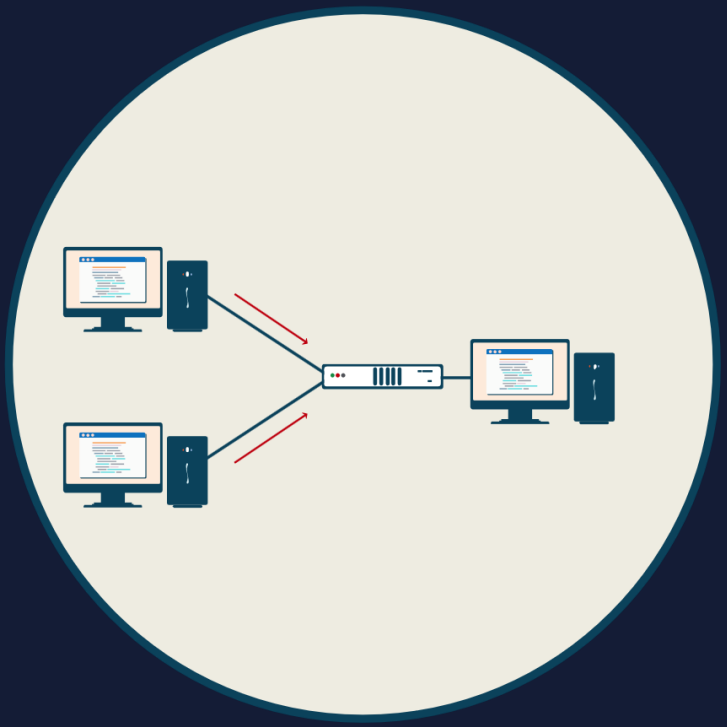
- Logical Design (e.g., tenant partitioning, access control)
- Physical Design (e.g., location, buy or build)
- Environmental Design (e.g., Heating, Ventilation and Air Conditioning (HVAC), multi-vendor pathway connectivity)

Software-defined Networking (SDN)

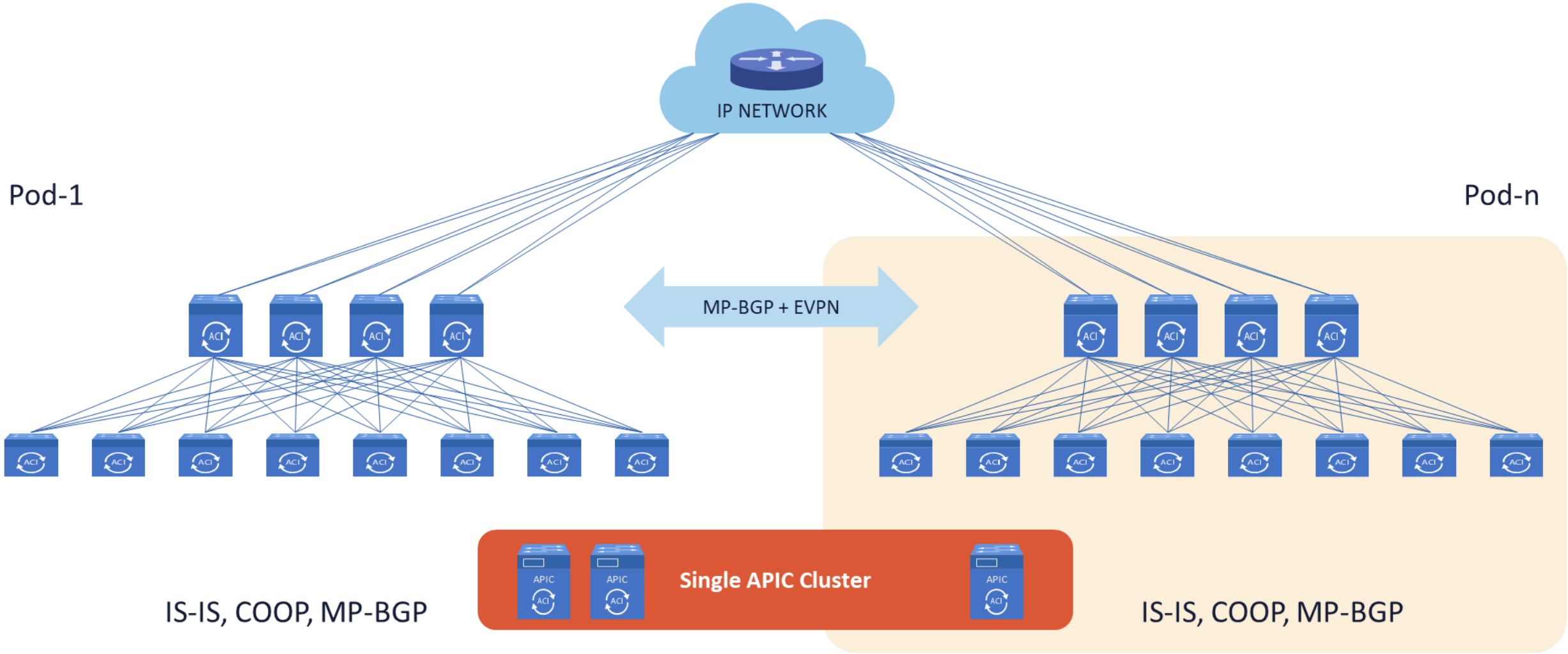


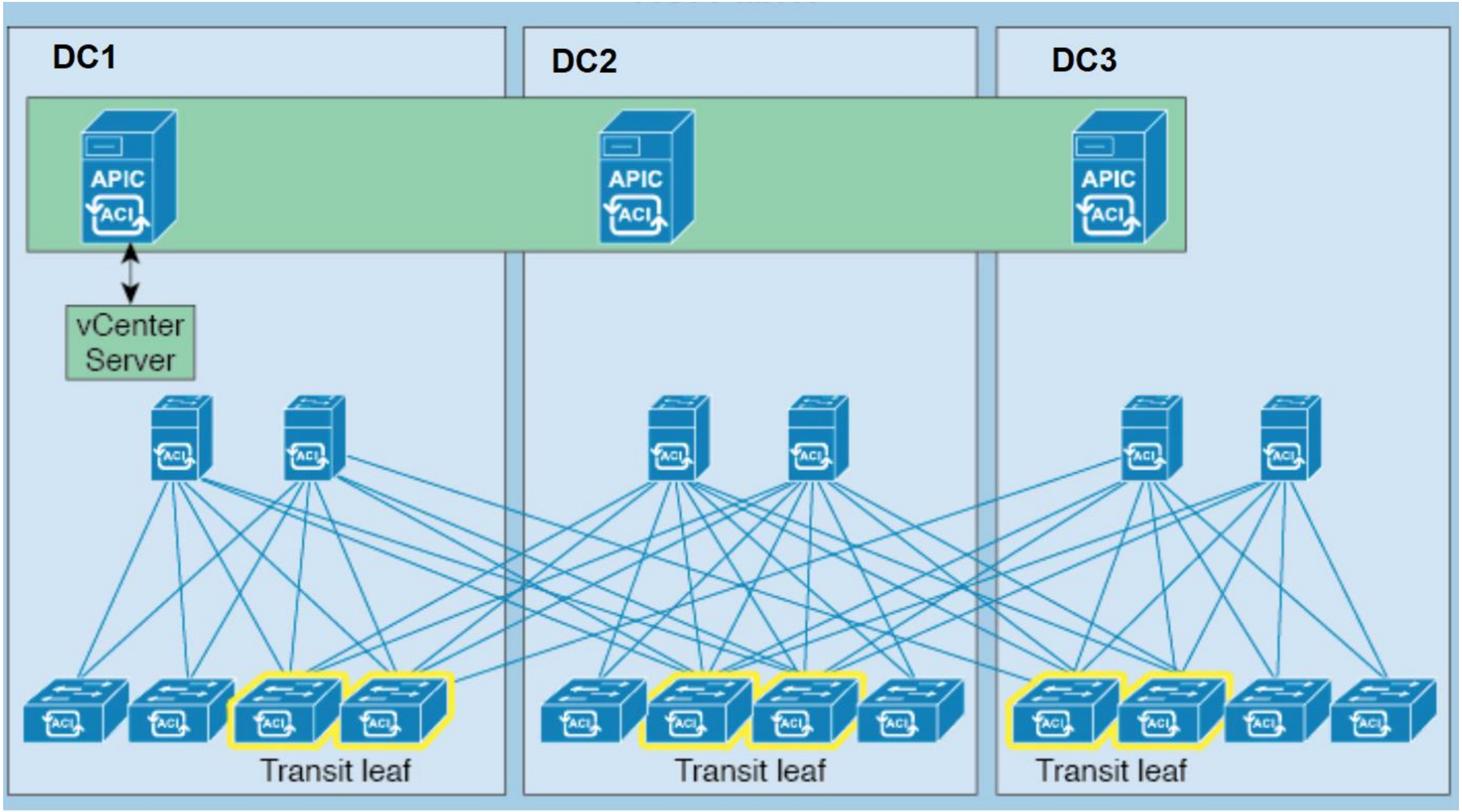
VXLAN

- VXLAN is technically an encapsulation protocol that offers data center connectivity using tunneling to stretch Layer 2 connections over an underlying Layer 3 network
- VXLAN solutions from a variety of vendors decouple the physical hardware from the network map in order to support virtualization
  - This uncoupling allows the data center network to be deployed programmatically
- It allows both Layer 2 and Layer 3 transport between VMs and bare-metal servers
- VXLAN supports the virtualization of the data center network while addressing the needs of multi-tenant data centers by offering the necessary scalable segmentation

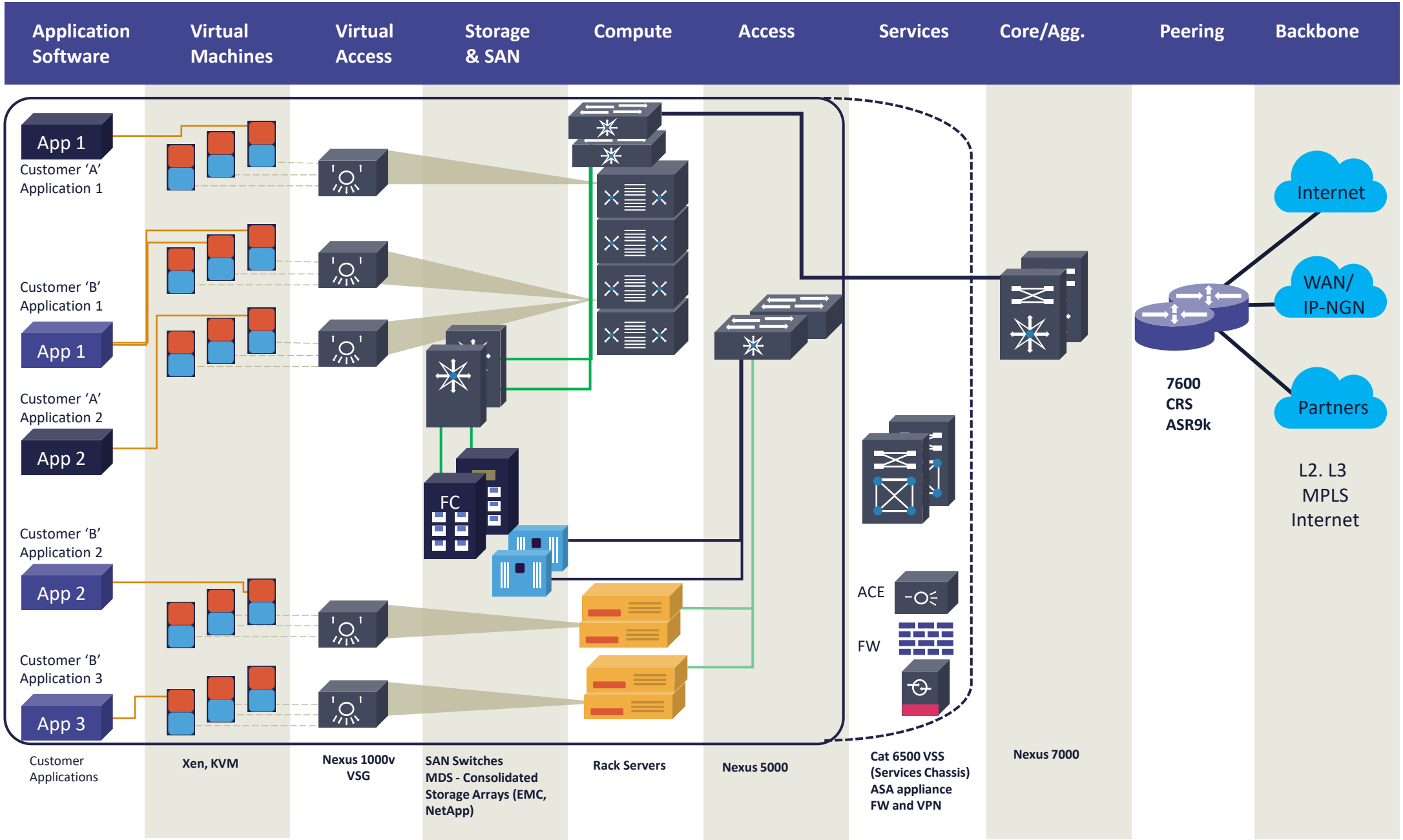


VXLAN


IP NETWORK
Pod-1
Pod-n
MP-BGP + EVPN
APIC
APIC
Single APIC Cluster
APIC
IS-IS, COOP, MP-BGP
IS-IS, COOP, MP-BGP



CSP Availability Zone


Application Software
Virtual Machines
Virtual Access
Storage & SAN
Compute
Access
Services
Core/Agg.
Peering
Backbone
App 1
Customer 'A' Application 1
Customer 'B' Application 1
App 1
Customer 'A' Application 2
App 2
Customer 'B' Application 2
App 2
Customer 'B' Application 3
App 3
FC
ACE
FW
Internet
WAN/ IP-NGN
Partners
7600 CRS ASR9k
L2. L3 MPLS Internet
Customer Applications
Xen, KVM
Nexus 1000v VSG
SAN Switches MDS - Consolidated Storage Arrays (EMC, NetApp)
Rack Servers
Nexus 5000
Cat 6500 VSS (Services Chassis) ASA appliance FW and VPN
Nexus 7000

Software-defined Security (SDS)

Used with Software-defined Networks

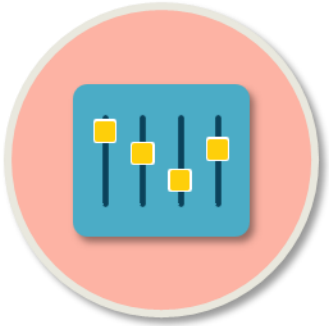
- Software-defined Security (SDS) is a model in which the information security is highly controlled often using virtualization
- The functionality of network security devices, such as next-gen firewalls, intrusion detection and prevention, identity and access controls, and network segmentation are removed from hardware devices to a software layer
- SDS exploits the software-defined networking (SDN) initiative to enhance network security
- The concept of software-defined security is envisioned to define IT infrastructure security services as a transition from hardware based to a software-defined solution

SDN and SDS

HOST

The host role is to transmit or receive data through the network

For the SDS, all security techniques are transferred to the controller

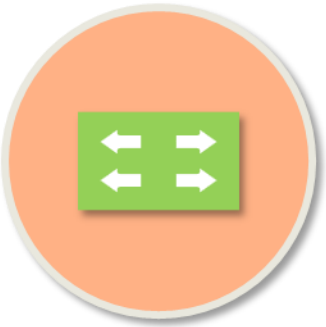


CONTROLLER

The controller is fully software-based

All security checks are done inside the controller, and it has total visibility of the traffic flows

It collects and processes information about the network



SWITCH

The switch checks with the controller to determine whether to accept or reject a request

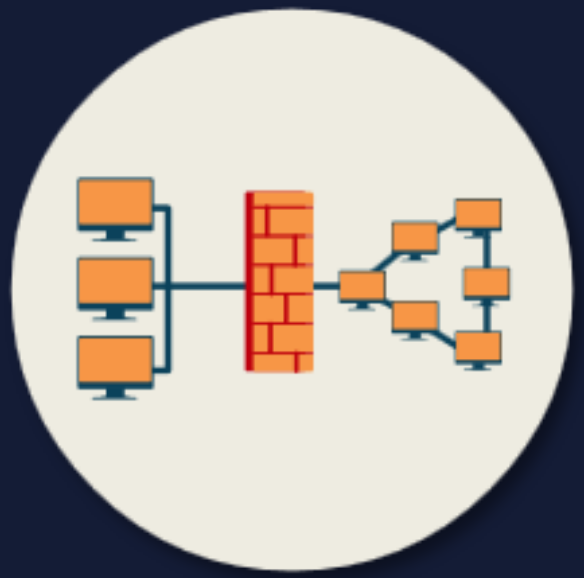
A reactive caching mechanism is adopted in SDN, which does make SDN switches vulnerable to a DoS attack

Advantages of SDS

- Offers resourceful and dynamic countermeasures to security attacks
- Separates security away from traditional hardware vulnerabilities
- Ability to dynamically configure existing network nodes allows for rapid attack mitigation from zero-day attacks
- Synchronized view of logical security policies exist within the SDN controller model (not tied to any server or specialized security device)
- Visibility of information provided from one source
- Integration with emerging technology to correlate events in a simpler way and respond more efficiently and intelligently to threats
- Enables centralized management of security, which is implemented, controlled, and managed by security software through the SDN controller
- Facilitates IoT & BYOD connectivity and security

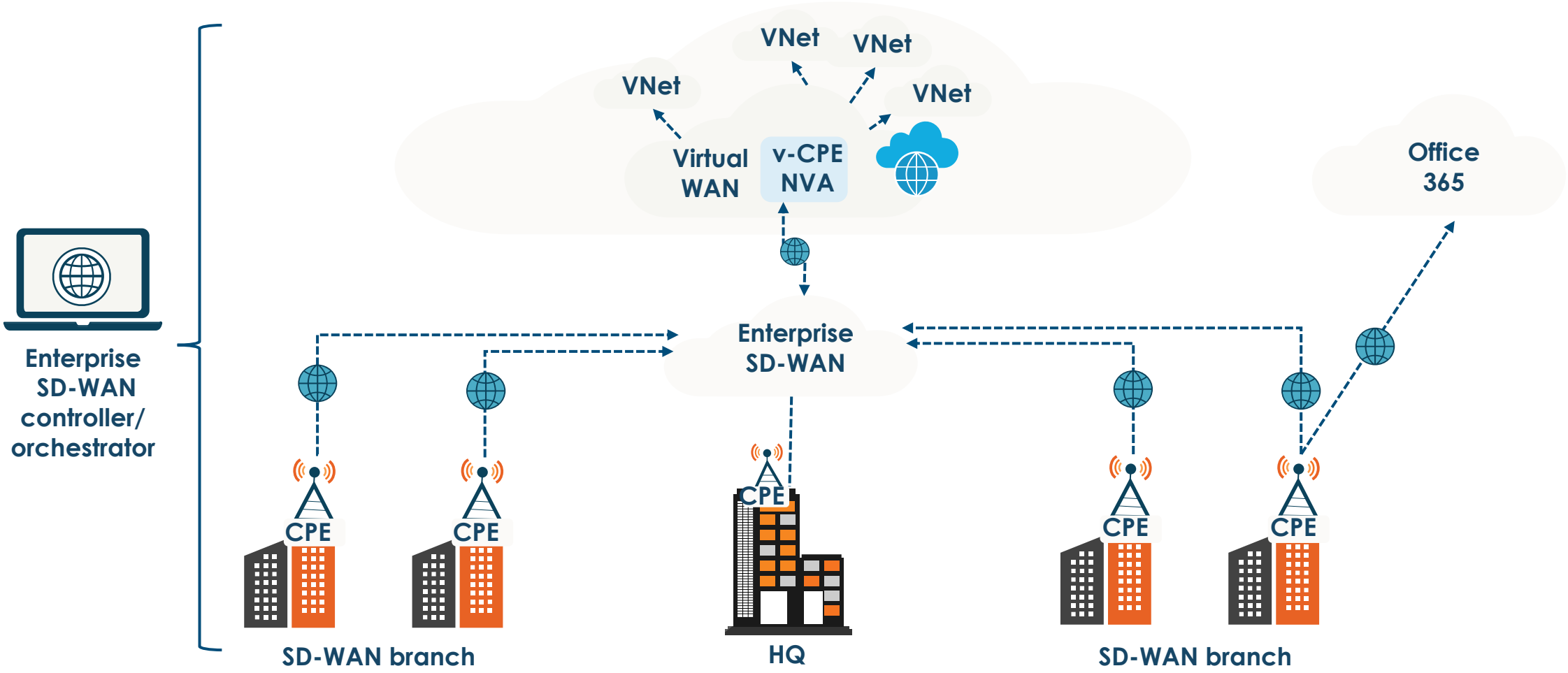
SD-WAN

Software-defined Wide Area Networks

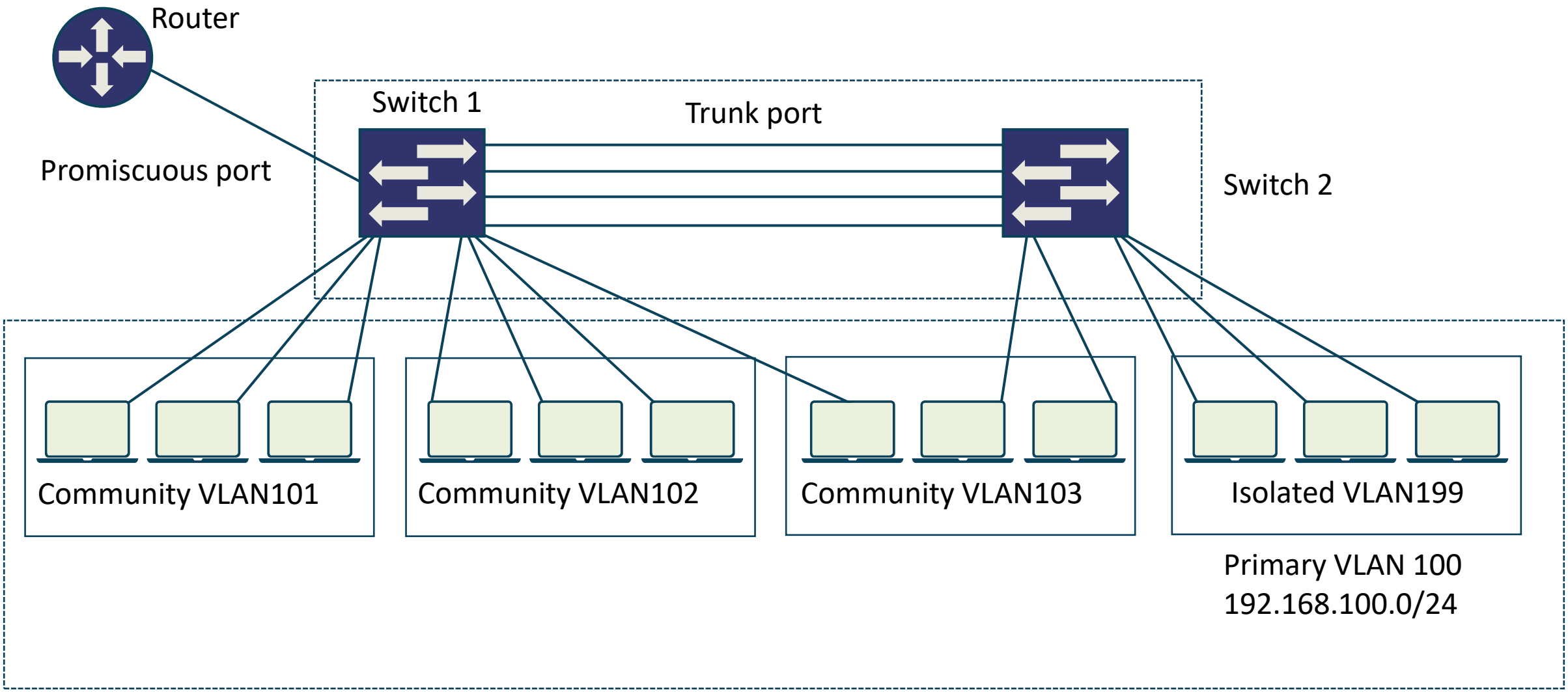


- Software Defined Wide Area Network is an SDN approach that raises network traffic management away from the hardware and premises to next-generation software in the cloud for superior agility, control, and visibility
- It is commonly used with Cloud Providers in metropolitan area solutions
- Incorporates a centralized control function with user-defined application and routing policies to deliver highly secure, robust, application-aware network traffic management

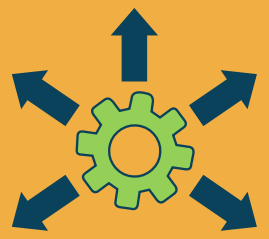
Microsoft Azure SD-WAN Solution



PVLANs for Segmentation and Containment



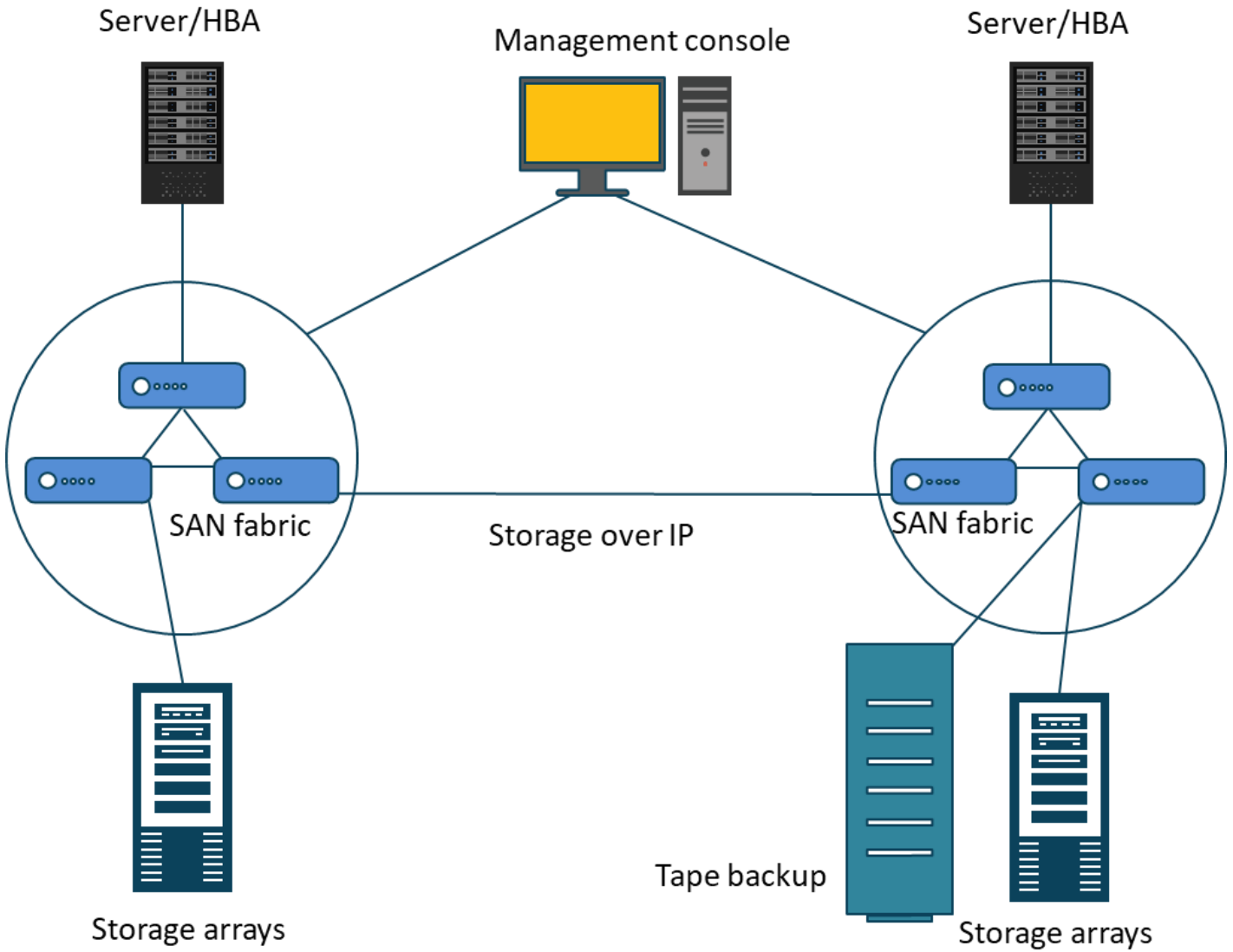
Securing Distributed Systems



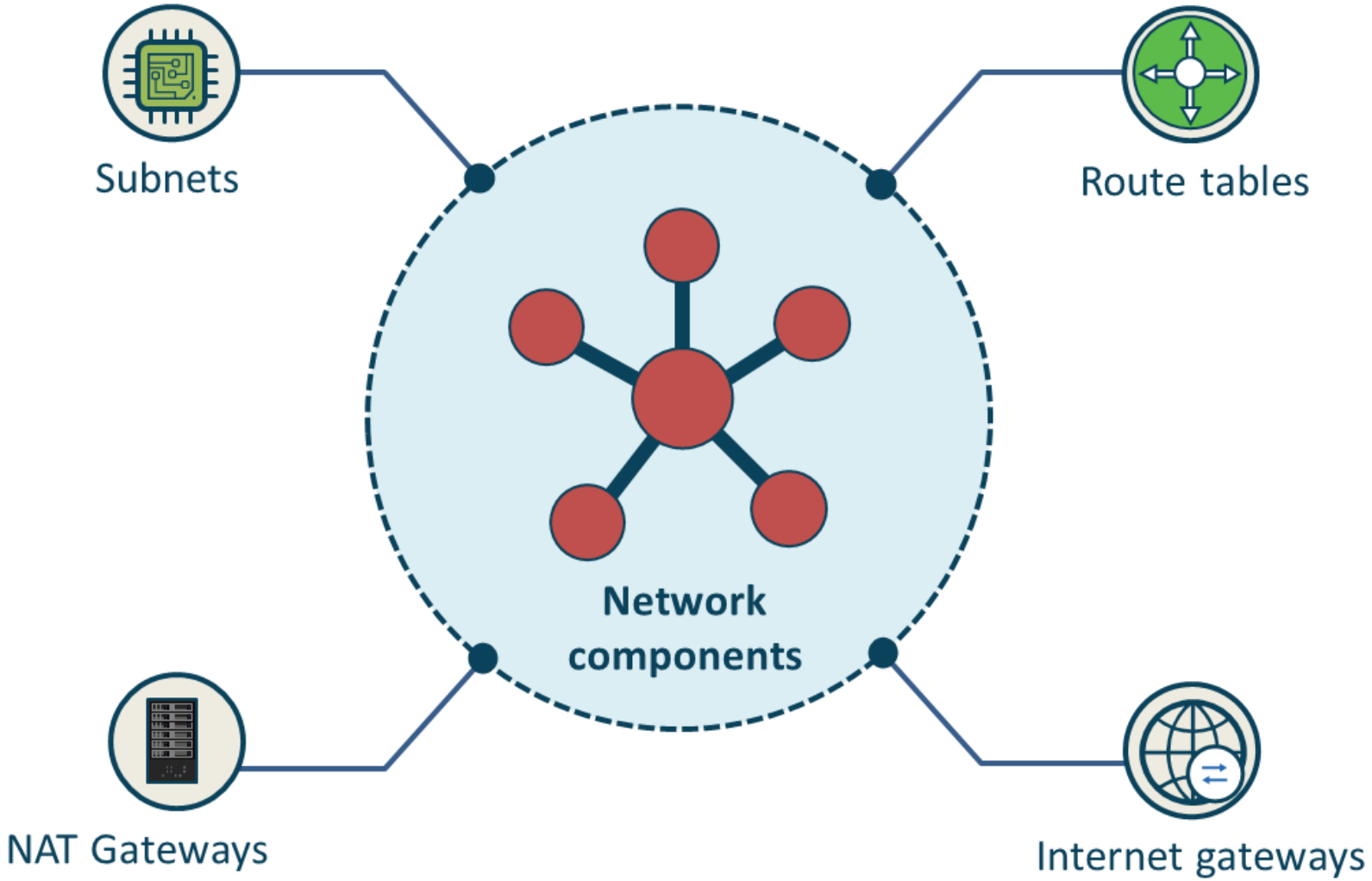
- A distributed system needs more security measures than centralized systems, as there are many users, differentiated data, multiple sites, and distributed control
- Security engineers must consider many permutations of failures and errors that can happen at any time, independently or in combination with other error conditions
- In distributed communication systems, there are several types of exploits:
  - Passive eavesdroppers that monitor messages and collect private information – information leakage
  - Active attackers that not only eavesdrop but further corrupt messages by inserting new data or modifying existing data
  - Distributed Denial of Service (DDoS) and botnets
  - Unauthorized access through poor access controls

Securing the Storage Area Network (SAN)

- For securing data in transit, consider IPsec AH for integrity and origin authentication
- 802.11AE (MACsec) can provide encryption and more on the SAN frames
- Use secure management protocols on console
- Harden all switches and servers
- Encrypt data at rest with AES-256-GCM

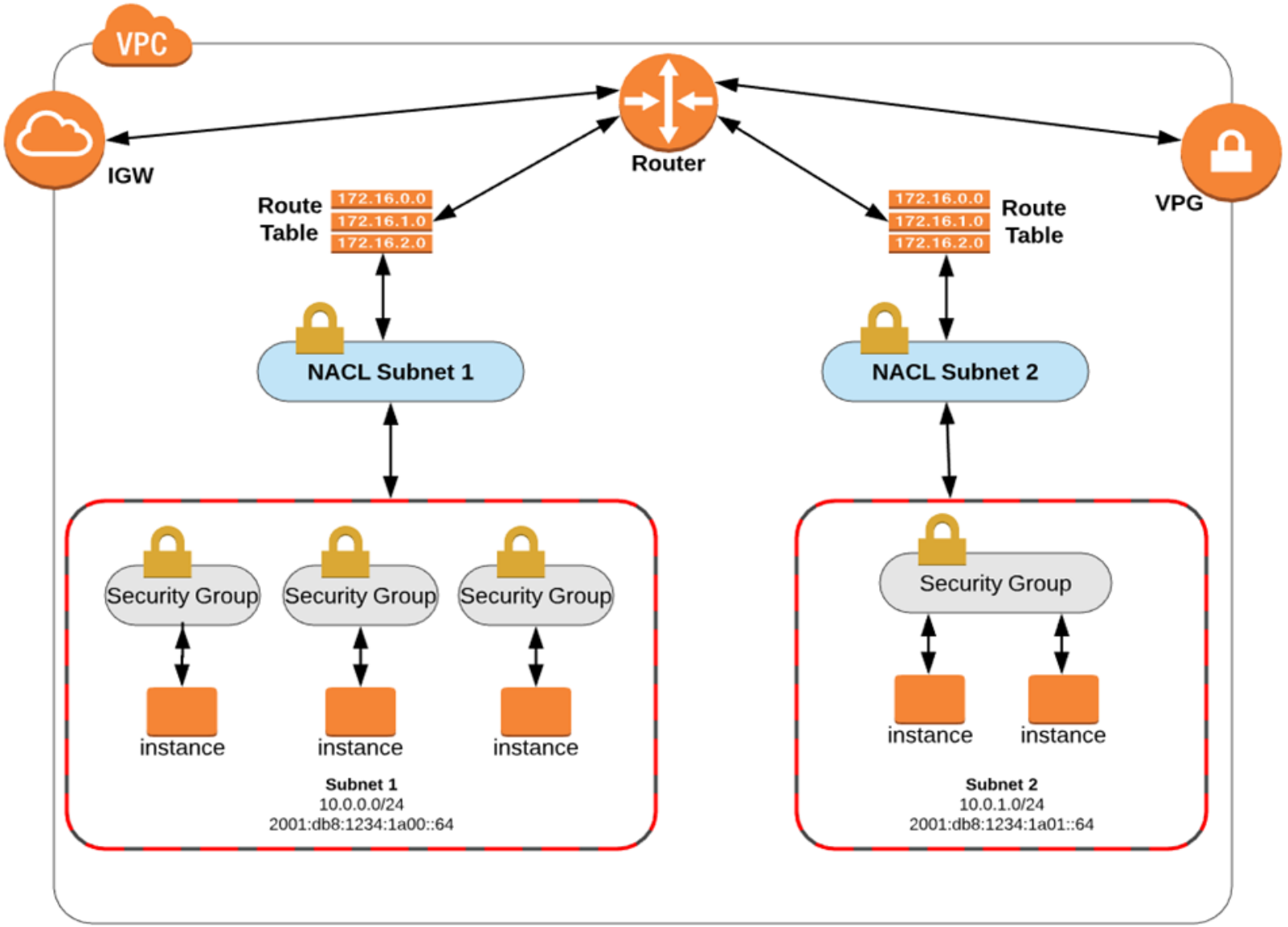


Networking Fundamentals

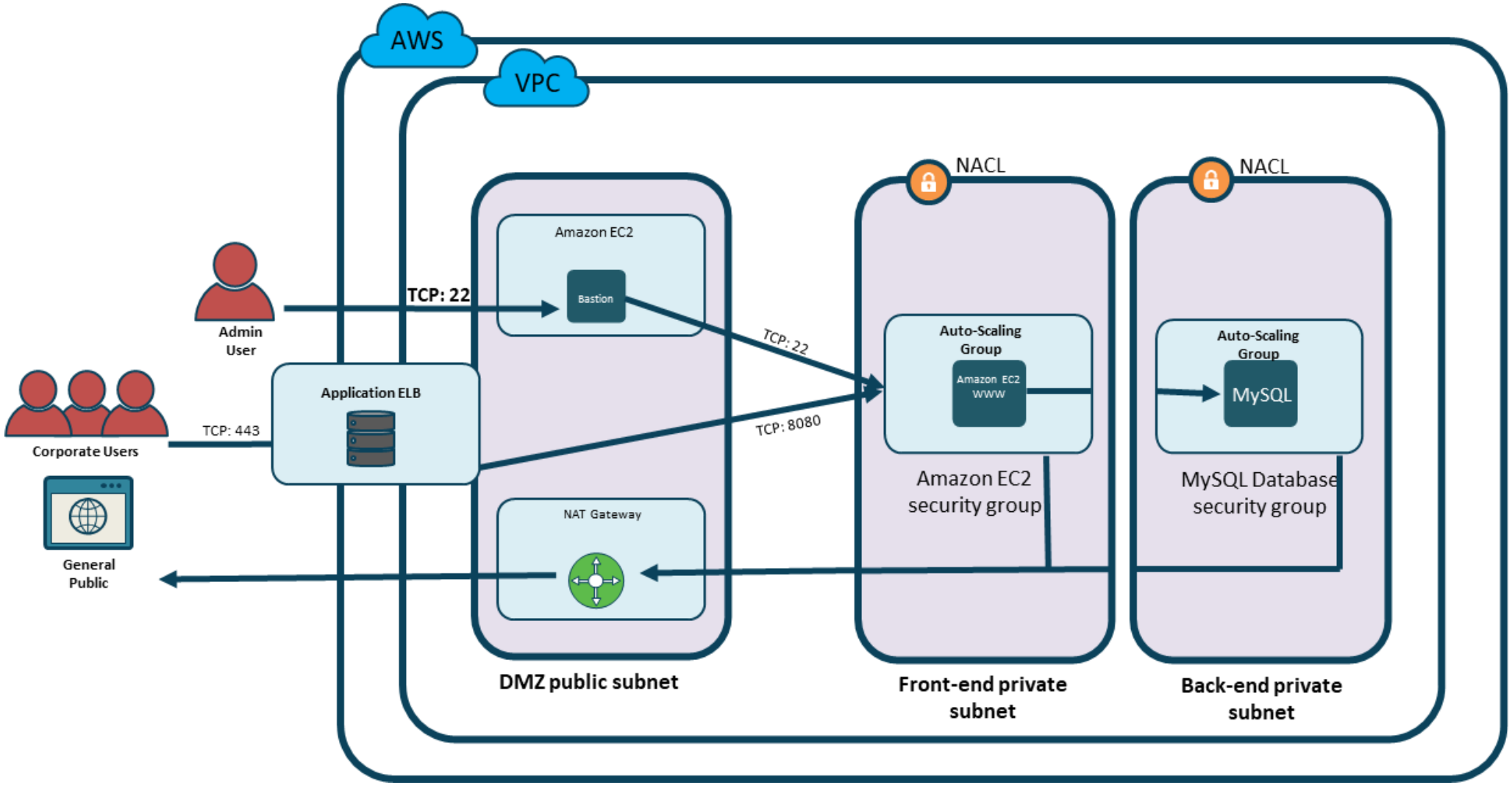


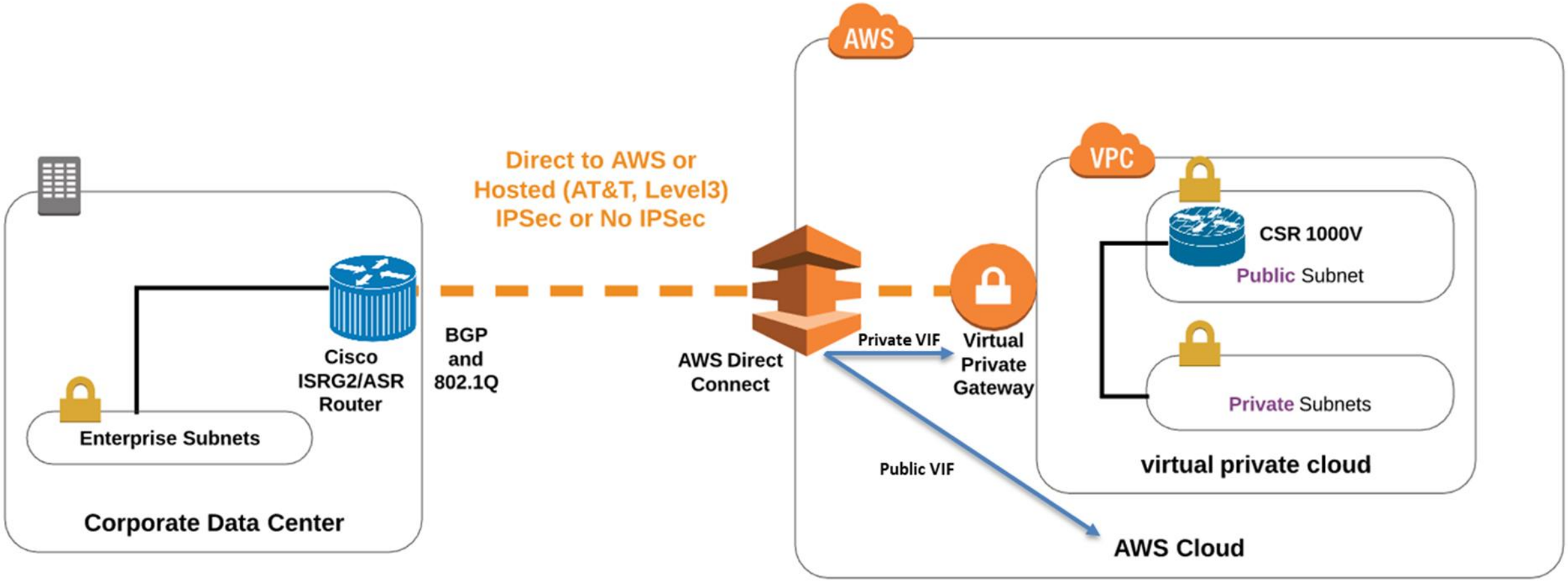
Networking Fundamentals

Customer Networking Begins with Design



Customer Networking Begins with Design

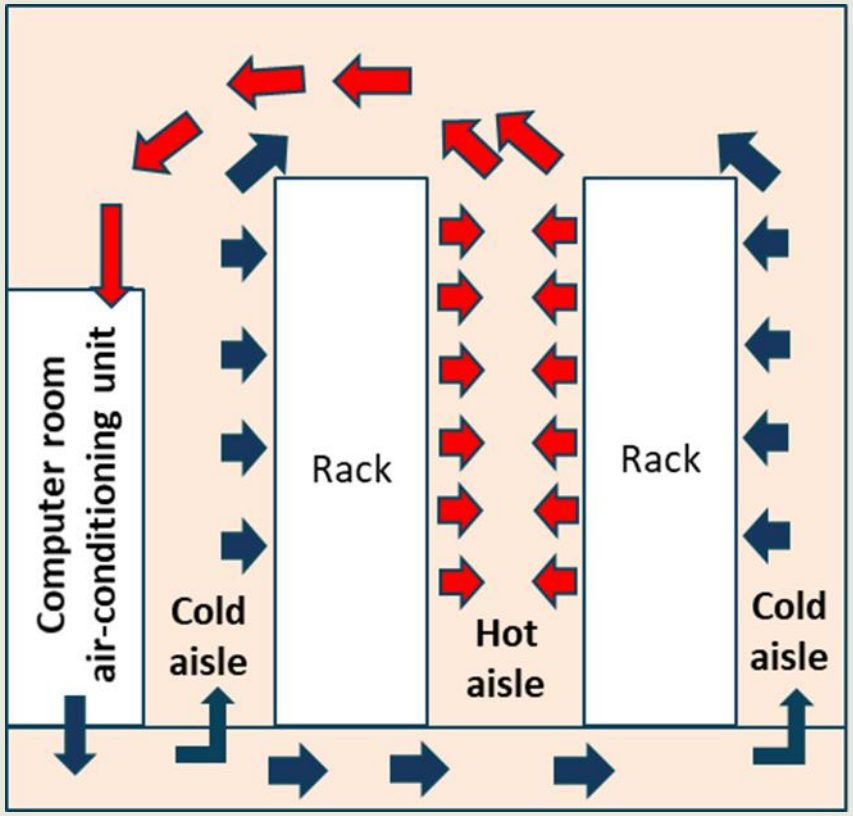




**AWS Direct Connect,
Azure ExpressRoute,
or Google Cloud
Interconnect**

HVAC Design Considerations

Include these industry HVAC guidance practices into your datacenter design

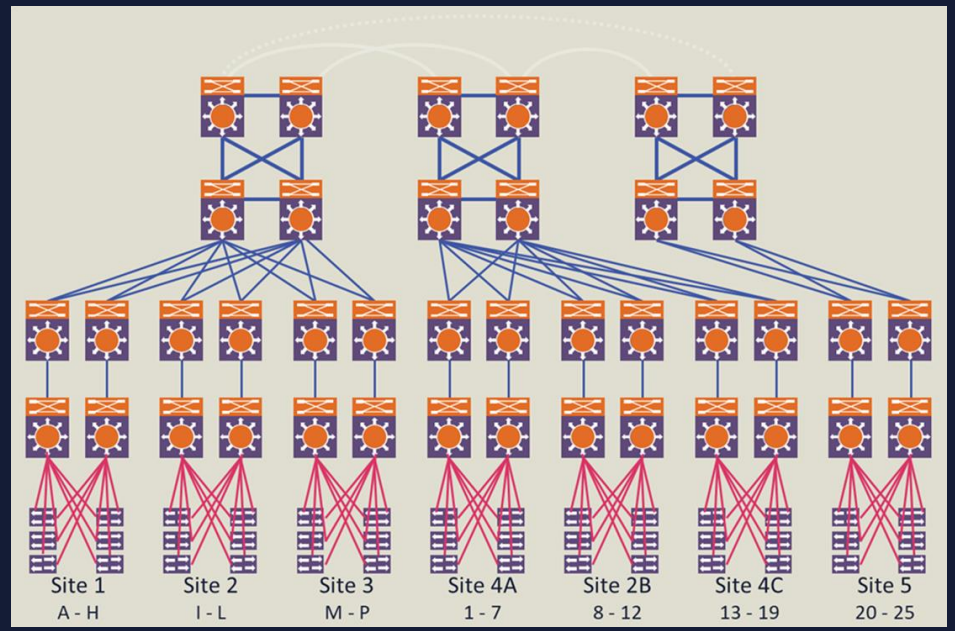


- Local climate will impact the HVAC design requirements
- Redundant HVAC systems should be part of the design
- HVAC systems should provide air management that separates the cool air from the heat exhaust of the servers
  - There are racks with built-in ventilation or alternating cold/hot aisles
  - The best design choice will depend on space and building design constraints
- Consider energy efficient systems when feasible
- Recommended temp: 72 to 76 degrees
- Recommended humidity: 40-60%
- Backup power supplies should be available to the HVAC system based on business impact analysis (BIA)
- The HVAC system should filter contaminants and dust

Adiabatic Coolers and Chillers

- Adiabatic cooling systems work similarly to dry cooling systems, but with the incorporation of pre-cooling pads
  - Running water over pre-cooling pads and drawing air through the pads depresses the ambient dry bulb of the incoming air
- The depressed dry bulb allows for greater system heat rejection - highly effective in hot, dry environments, while using less water than traditional evaporative units
- Adiabatic units also deliver the needed cooling capacity in a smaller footprint and/or lower fan motor horsepower than a completely dry cooler/condenser

Distribution Frames and Wiring Closets



- Gain visibility into all ethernet and fiber cable runs as well as the security of distribution frame (MDF rooms) rooms and closets
  - Under the floor
  - Above ceiling panels
  - In the walls
- Lock all doors to server rooms and frame rooms
- No window access or use security windows with wire mesh
- Use hardened management stations and environmental controls for temperature, fire, gas, and humidity

Server Rooms and Data Centers

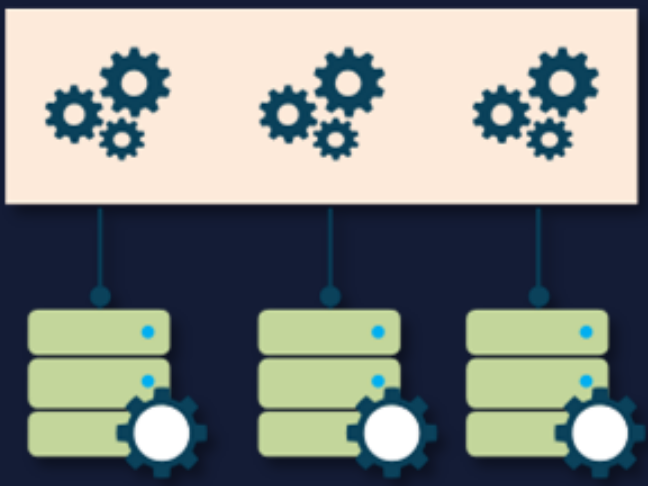
- Access control both at the perimeter and at room ingress points by professional security staff using video surveillance, intrusion detection systems, and more
- Authorized staff should pass biometric dual-factor authentication a minimum of two times to access data center floors
- Implement protective barriers
- **Have redundant and monitored support systems with secure KVM systems**
- Have visibility into high-security compartmentalized areas including all power conduits and water lines

Server Rooms and Datacenters

- When an employee no longer has a business need for data center privileges, access must be immediately revoked, even if they continue to be an employee
- Automatic fire detection and suppression equipment must be used
- The electrical power systems should be fully redundant and maintainable without impact to operations 24/7
- Uninterruptible power supply (UPS) units can provide back-up power for critical and essential loads in the facility in the event of an electrical failure
- Data centers often use generators to provide back-up power for the entire facility

Server Rooms and Data Centers

- Airgap is the physical separation of the control network and other networks
- Separate the highly secure networks from the unsecured networks with physical or logical compartmentalization
- Log and audit all devices and objects entering and exiting facility
- Stop malicious and privileged users from having individual access
- Work with facilities management to integrate blueprints and topological diagrams into IT services



Multi-vendor Pathway Connectivity

- Uninterrupted service and constant access are critical to the daily operation and productivity of the enterprise
- Since downtime leads directly to loss of income, datacenters must be designed for redundant, fail-safe reliability and availability
  - Datacenter reliability is also defined by the performance of the infrastructure
- Cabling and connectivity backed by a trustworthy vendor SLA with guaranteed error-free performance will help avoid poor data transmission in the datacenter
- **There should be redundant connectivity from multiple providers into the datacenter**
  - This will help prevent a single point of failure for network connectivity
  - The redundant paths should deliver the minimum expected connection speeds (10GB/100GB) for datacenter operations

3.3 Analyze Risks Associated with Cloud Infrastructure

- Risk Assessment and Analysis
- Cloud Vulnerabilities, Threats and Attacks
- Virtualization Risks
- Counter-measure Strategies

Defining Risk

- Inherent (total) risk
  - Risk the organization faces if safeguard is not implemented
- Residual risk
  - Risk that remains once safeguard is in place
- Residual = inherent risk - safeguards (controls)

Risk Assessment

	Event type								
	Accidental Leak	**Espionage**	**Financial fraud**	**Misuse**	**Opportunistic data theft**	**Physical theft**	**Product alteration**	**Sabotage**	**Violence**
Nonhostile									
Reckless insider	X			X			X		
Untrained/distracted insider	X			X			X		
Outward sympathizer	X			X					
Unknown (nonhostile or hostile)									
Supplier	X	X	X	X	X		X		
Partner	X	X	X	X	X		X		
Hostile									
Irrational individual	X			X		X		X	X
Thief		X	X		X	X			
Disgruntled insider	X	X	X	X	X	X	X	X	X
Activist		X		X	X	X	X	X	
Terrorist						X		X	X
Organized crime		X	X		X	X	X		
Competitor		X			X		X	X	
Nation state		X			X		X	X	

Tim Casey et al., "A Field Guide To Insider Threat," PDF file, https://www.nationalinsiderthreatsig.org (IT@Intel, Intel Corporation, October 2015), https://www.nationalinsiderthreatsig.org/itrmresources/Intel%20Insider%20Threat%20Field%20Guide.pdf.

Creating a Risk Register

- Risk Register is also called ledger or log
- Often represented as a scatter plot/table from a database
- Fulfills regulatory compliance
- Repository of identified risks, impact, scenarios, and potential responses

Identified Risks	Root Causes	Probability and Impact	Ranking	Categories	Priorities	Time and Cost Objectives	Potential Responses	Risk Owners	Assumptions

Risk Treatment

Also called risk handling or appetite

- Risk acceptance
  - Do not implement any safeguards
  - Justification in writing is often required
- Risk avoidance
  - Choose not to undertake actions that introduce risk
- Risk transference/sharing
  - Pass the risk to a third-party, such as an insurance company or a cloud service provider
- Risk mitigation
  - Implement safeguards that will eliminate or reduce risk exposure - risk may exist, but impact is reduced

Qualitative Risk Analysis

The most common method used in risk and security

- Descriptive approach using subjective opinions, history, and scenarios to determine risk levels
  - Expert judgement
  - Best practices
  - Experience
  - Intuition
- Often involves interviewing people (Delphi) regarding assets, known risks, known vulnerabilities, common threats, and historical impacts

Qualitative Heat Map

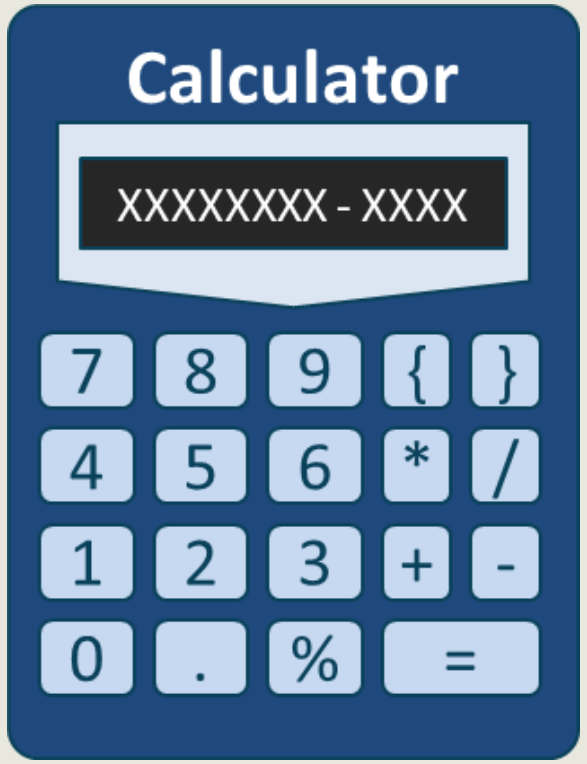
Likelihood			Impact				
			Negligible	Minor	Moderate	Critical	Disastrous
			1	2	3	4	5
	Frequent	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Occasional	3	Low	Medium	Medium	Medium	High
	Seldom	2	Low	Low	Medium	Medium	Medium
	Improbable	1	Low	Low	Low	Medium	Medium

Quantitative Risk Analysis

Rapidly gaining popularity due to FAIR analysis

- Scientific/mathematical approach to getting monetary and numeric results based on the following:
  - Asset values
  - Impact and magnitude
    - Severity of incident
  - Probability and likelihood of occurrence
    - Threat frequency
  - Costs and effectiveness of safeguards
  - Probabilities based on percentages and calibrated estimation

Classic Quantitative Analysis (Whitman)



- AV (asset value)
  - Value of the asset according to the organization
- EF (exposure factor)
  - Percentage of asset loss caused by identified threat
- SLE (single loss expectancy)
  - Potential loss if attack occurs
  - (Asset value * exposure factor)
- ARO (annualized rate of occurrence)
  - Estimated frequency the threat will occur within a single year
- ALE (annualized loss expectancy) = (SLE * ARO)

Classic Quantitative Analysis (Whitman)

Risk analysis						
Asset	**Threat**	**Asset value**	**Exposure factor**	**Single loss expectancy**	**Annualized rate of occurrence**	**Annualized loss expectancy**
SRV_1	Fire	$15000	100%	$15000	0.1	$1500
SRV_2	Fire	$20000	100%	$20000	0.1	$2000
SRV_1	Flood	$15000	100%	$15000	0.0001	$1.5
SRV_2	Flood	$20000	100%	$20000	0.0001	$2.0
SRV_1	Virus (no AV software)	$15000	10%	$1500	365	$547,500
SRV_1	Virus (with AV software)	$15000	10%	$1500	1	$1500

Cloud Vulnerabilities:

The Treacherous 12

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders

Cloud Vulnerabilities:
The Treacherous 12

7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues

AWS GuardDuty Findings

- Backdoor
  - Backdoor:EC2/C&CActivity - EC2 - VPC flow logs – high severity
- Behavior
  - Behavior:EC2/NetworkPortUnusual - EC2 - VPC flow logs – medium severity
- Credential Access
  - CredentialAccess:IAMUser/AnomalousBehavior – IAM – CloudTrail - medium
- Crypto Currency
  - CryptoCurrency:EC2/BitcoinTool.B!DNS - EC2 - DNS logs - high
- Defense Evasion
  - DefenseEvasion:IAMUser/AnomalousBehavior – IAM – CloudTrail - medium
- Discovery
  - Discovery:S3/MaliciousIPCaller – S3 - S3 CloudTrail data event - high
- Exfiltration
  - Exfiltration:IAMUser/AnomalousBehavior – IAM - CloudTrail - high
- Impact
  - Impact:EC2/AbusedDomainRequest.Reputation - EC2 - DNS logs - medium

AWS GuardDuty Findings

- Initial Access
  - InitialAccess:IAMUser/AnomalousBehavior – IAM – CloudTrail - medium
- Pen Test
  - PenTest:IAMUser/KaliLinux – IAM - CloudTrail - medium
- Persistence
  - Persistence:IAMUser/AnomalousBehavior – IAM – CloudTrail - medium
- Policy
  - Policy:S3/BucketPublicAccessGranted - S3 – CloudTrail - high
- Recon
  - Recon:EC2/PortProbeEMRUnprotectedPort - EC2 - VPC flow logs - high
- Stealth
  - Stealth:IAMUser/CloudTrailLoggingDisabled – IAM – CloudTrail - low
- Trojan
  - Trojan:EC2/DNSDataExfiltration - EC2 - DNS logs - high
- Unauthorized Access
  - UnauthorizedAccess:S3/TorIPCaller - S3 - S3 CloudTrail data event - high

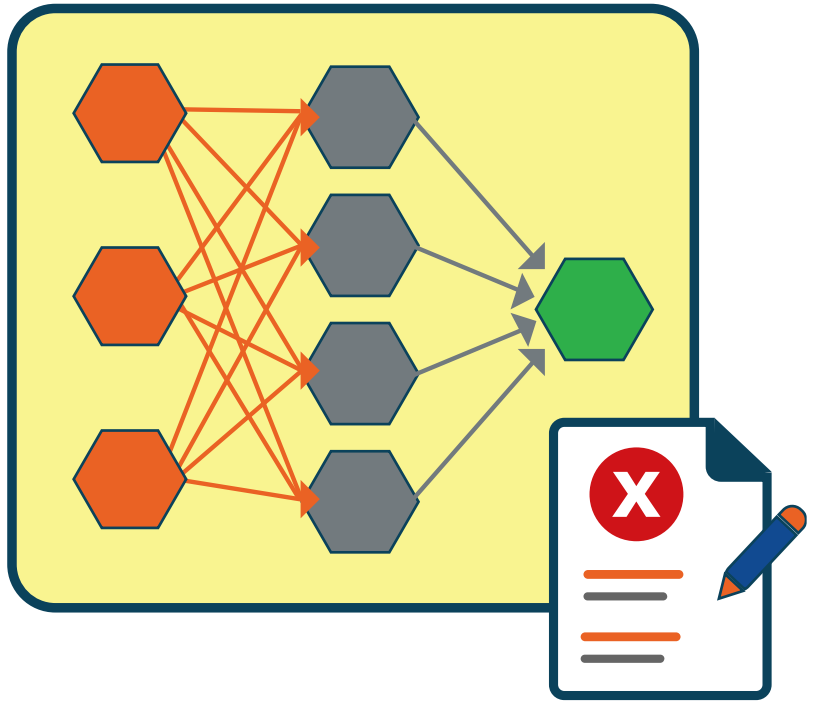
Virtualization Risks

- VM escape is a serious threat where a process running in the guest VM interacts directly with the host OS
- Hyperjacking happens when an attacker takes malicious control of the hypervisor that creates the VM host
  - Injecting a rogue under the original hypervisor
  - Taking full control of the initial Hypervisor
  - Running a rogue on top of the initial hypervisor
- VM sprawl happens when the number of VMs overtakes the administrator's ability to manage them and the available resources
  - Causes “Ghost” or “Shadow” IT vulnerability

Countermeasure Strategies

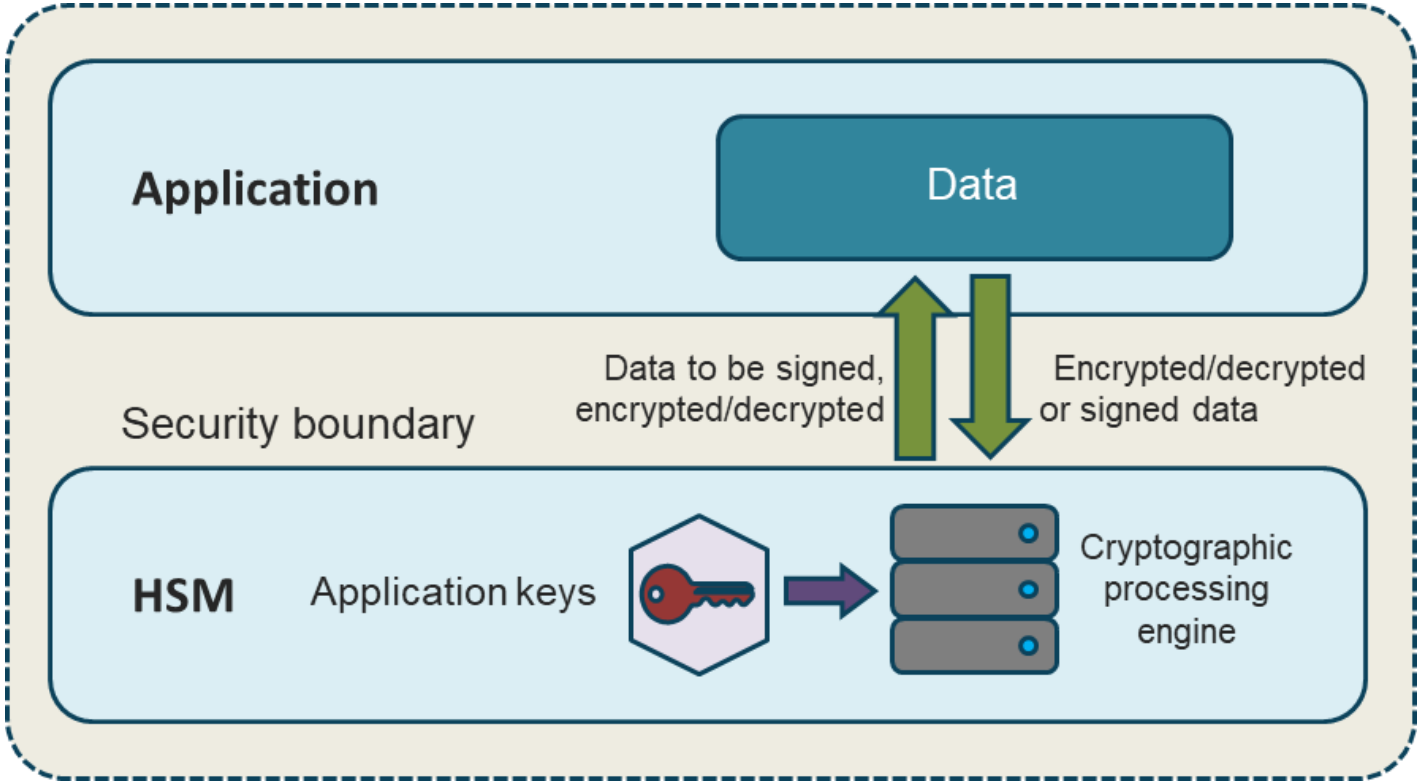
The Cloud Security Triad

- **Identity and access management** (IAM/IdM)
  - Cloud IAM or Federated SSO (token services)
- **Infrastructure security**
  - Network design and automated visibility
  - Firewalls (L3/4 stateless, stateful, and WAF)
  - Secure endpoints and policies
  - Secure management access (digitally signing, SSH2, TLS)
  - S2S and P2S VPN services
  - Managed Threat Management (GuardDuty)
- **Key Management Services (KMS)**
  - Client and server-side



Hardware Security Modules (HSM)

- **The underlying technology of Cloud KMS**
- Use tamper-proof, hardened devices
- Provide crypto processing
- Protect cryptographic functions
- Secure cryptographic keys
- Separate administration and security domains
- Apply key use policies
- Can be used in place of software crypto libraries

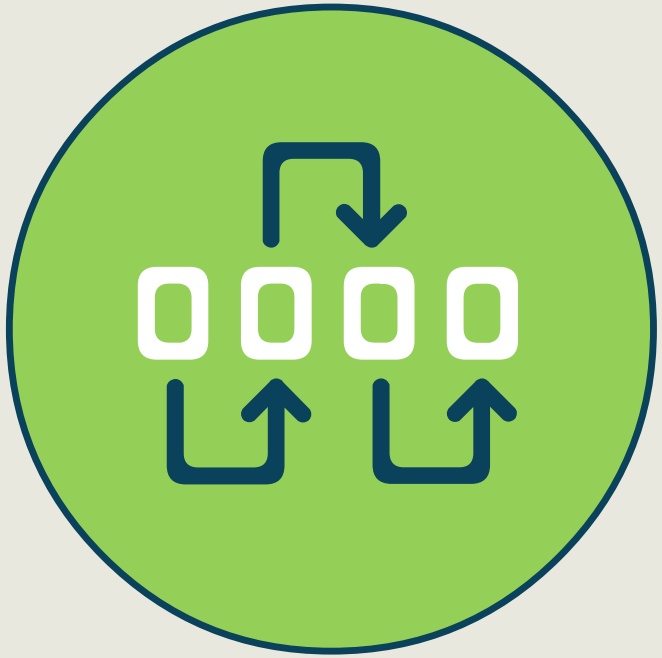


3.4 Design and Plan Security Controls

- Physical and Environmental Protection (e.g., on-premise)
- System and Communication Protection
- Virtualization Systems Protection
- Identification, Authentication and Authorization in Cloud Infrastructure
- Audit Mechanisms (e.g., log collection, packet capture)

Uptime Institute

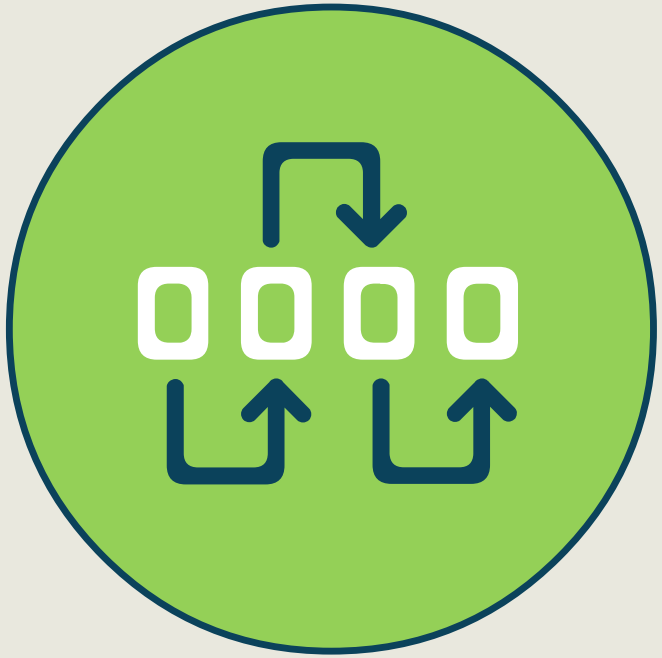
Standard bearer for digital Infrastructure performance whose Tier Standard has been used in thousands of sites in more than 100 countries



- **Tier 1**
  - The Basic Site Infrastructure
  - A simpler and less expensive solution with little or no redundancy - only dedicated space for IT systems, UPS for backup and line conditioning, cooling of critical equipment
  - Problematic personnel activity WILL cause downtime
  - **All 4 tiers have at least 4 hours of fuel for generators**
- **Tier 2**
  - Redundant Site Infrastructure Capacity Components has additional feature from Tier 1
    - Critical operation s do not have to be interrupted for scheduled maintenance or replacement
    - The WILL be downtime for any disconnection from power distribution and lines
    - Problematic personnel activity MAY cause downtime
    - Unplanned component failure or systems MAY cause downtime

Uptime Institute

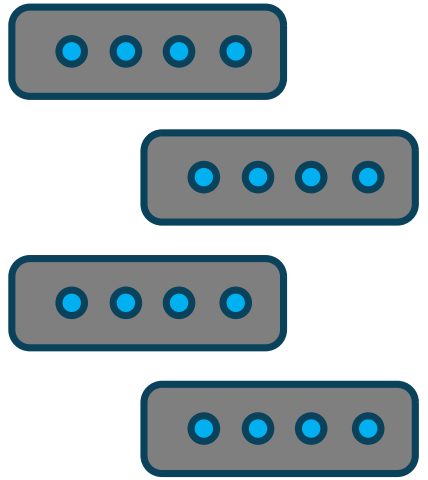
Standard bearer for digital Infrastructure performance whose Tier Standard has been used in thousands of sites in more than 100 countries



- **Tier 3**
  - Concurrently Maintainable Site Infrastructure
  - Dual power supplies for all systems
  - Critical operations can continue if a single component or power element is down for replacement or scheduled maintenance
  - Unplanned loss of component MAY cause downtime; unplanned loss of single system WILL cause downtime
- **Tier 4**
  - Fault-Tolerant Site Infrastructure – the optimal data center offering
  - Has features of other tiers included
  - Full redundancy of systems, power, cooling
  - Loss of a single element will NOT cause downtime
  - Fully automated visibility and response systems
  - Scheduled maintenance performed without downtime

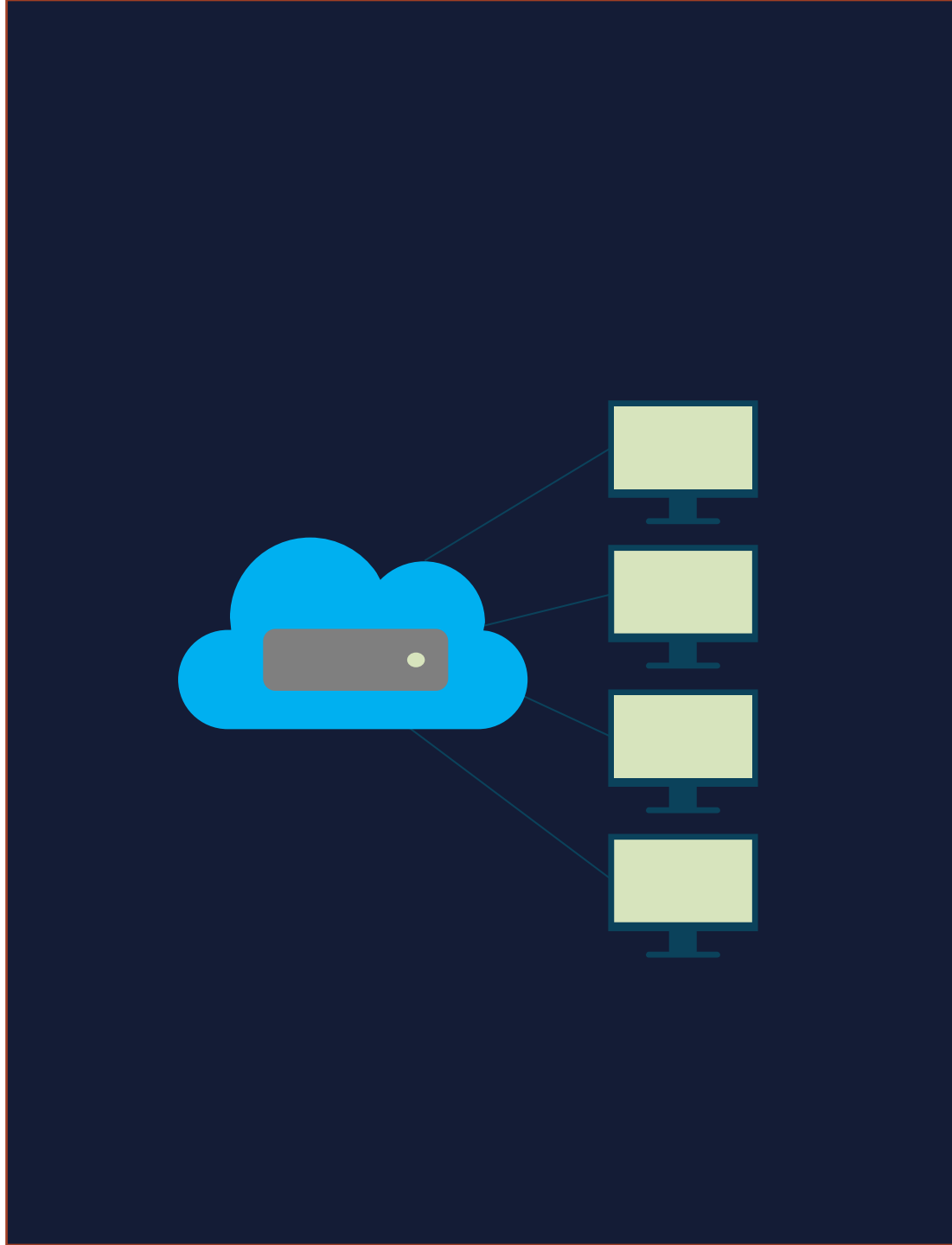
CSA BEST PRACTICES FOR MITIGATING RISKS IN VIRTUALIZED ENVIRONMENTS

- Risk #1 – VM Sprawl
- Risk #2 – Sensitive Data Within a VM
  - Passwords, personal data, bash profiles, bash history files, encryption keys, and license keys, also capture of corresponding data in images and snapshots
- Risk #3 – Security of Offline and Dormant VM
- Risk #4 – Security of Pre-Configured (Golden Image) VM / Active VMs
- Risk #5 – Lack of Visibility Into and Controls Over Virtual Networks
  - Hinders existing security policy enforcement in most organizations
  - Traffic over virtual networks may not be visible to security protection devices, such as network-based intrusion detection and prevention systems, on the physical network



VM Sprawl Mitigation

- Put effective policies, guidelines, and processes in place to govern and control VM lifecycle management
- Control the creation, storage, and use of VM images with a formal change management process and tools
- Keep a small number of known-good—and timely patched—images of a guest OS separately
- Use virtualization products with management solutions to examine, patch, and apply security configuration changes to VMs



Protecting Sensitive Data within a VM

- Encrypt data stored on virtual and cloud servers and release encryption/decryption keys only to authorized physical or virtual servers
- Develop policies to restrict storage of VM images and snapshots
- Ensure that backup and failover systems, including temporary upgrade/patch instances, are cleaned when deleting and wiping
- Use cryptographic checksum protection to detect unauthorized changes to VM images and snapshots
- Identify critical data files within the VM that may need a higher degree of monitoring

Securing Offline/Dormant VMs and Golden VM

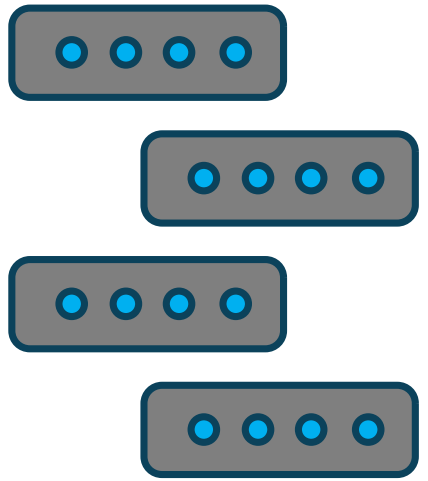
- Ensure proper hardening and protection of VM instances through VM guest hardening
- Augment VM operating systems with built-in security measures, leveraging third-party security technology, such as discovery and monitoring tools, to provide layered security controls
- Consider implementing an integrity checksum mechanism for all VM images
- Encrypt VM images to prevent unauthorized modification
- Implement strict controls and processes around access, creation, and deployment of VM images/instances

Gaining Visibility and Controls of Virtual Networks

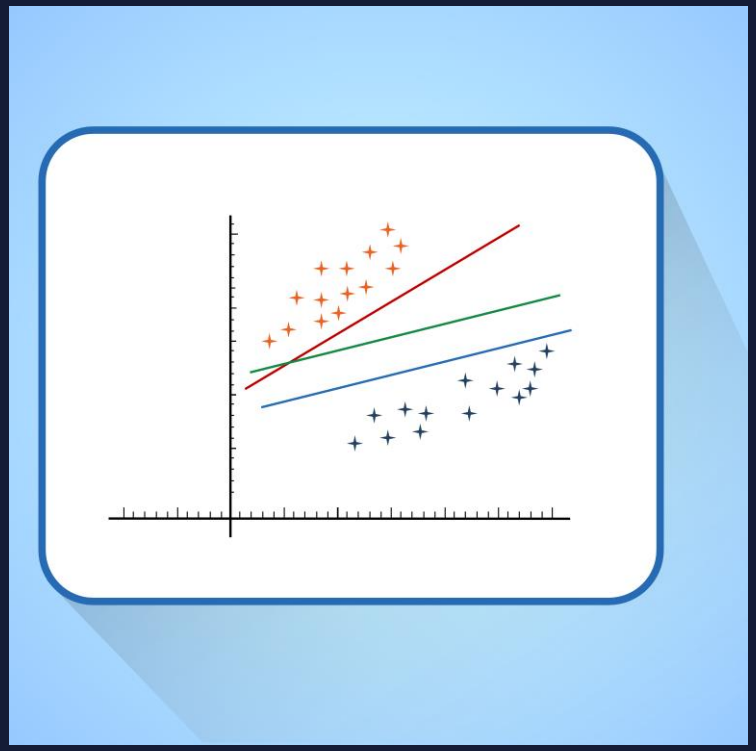
- Consider a hypervisor that can monitor each guest operating system (introspection) as it is running if separate tools are not installed to monitor communications between VMs
- Implement security technologies that span physical and virtual environments with a consistent policy management and enforcement framework
- Create consistent security policy and configuration across the physical/virtual network
- Use VM-specific security mechanisms embedded in hypervisor APIs to provide granular monitoring of traffic crossing VM control and data planes such as SDN/OpenFlow

CSA BEST PRACTICES FOR MITIGATING RISKS IN VIRTUALIZED ENVIRONMENTS

- Risk #6 – Resource Exhaustion
  - **Resource-intensive software tends to exhaust resources in a physical server when it is implemented in multiple VMs. For example, *anti-virus and other security software* interrupt every call to disk or memory in order to monitor and prevent security incidents such as hacking or viruses**
- Risk #7 – Hypervisor Security
- Risk #8 – Unauthorized Access to Hypervisor
- Risk #9 – Account or Service Hijacking Through the Self-Service Portal
  - A self-service portal is often used to delegate specific parts of virtual infrastructure provisioning and management to assigned self-service administrators
  - Generous use of self-service portals in cloud computing services will increase susceptibility to security risks, including account or service hijacking
- Risk #10 – Workload of Different Trust Levels Located on the Same Server
- Risk #11 – Risk Due to Cloud Service Provider API

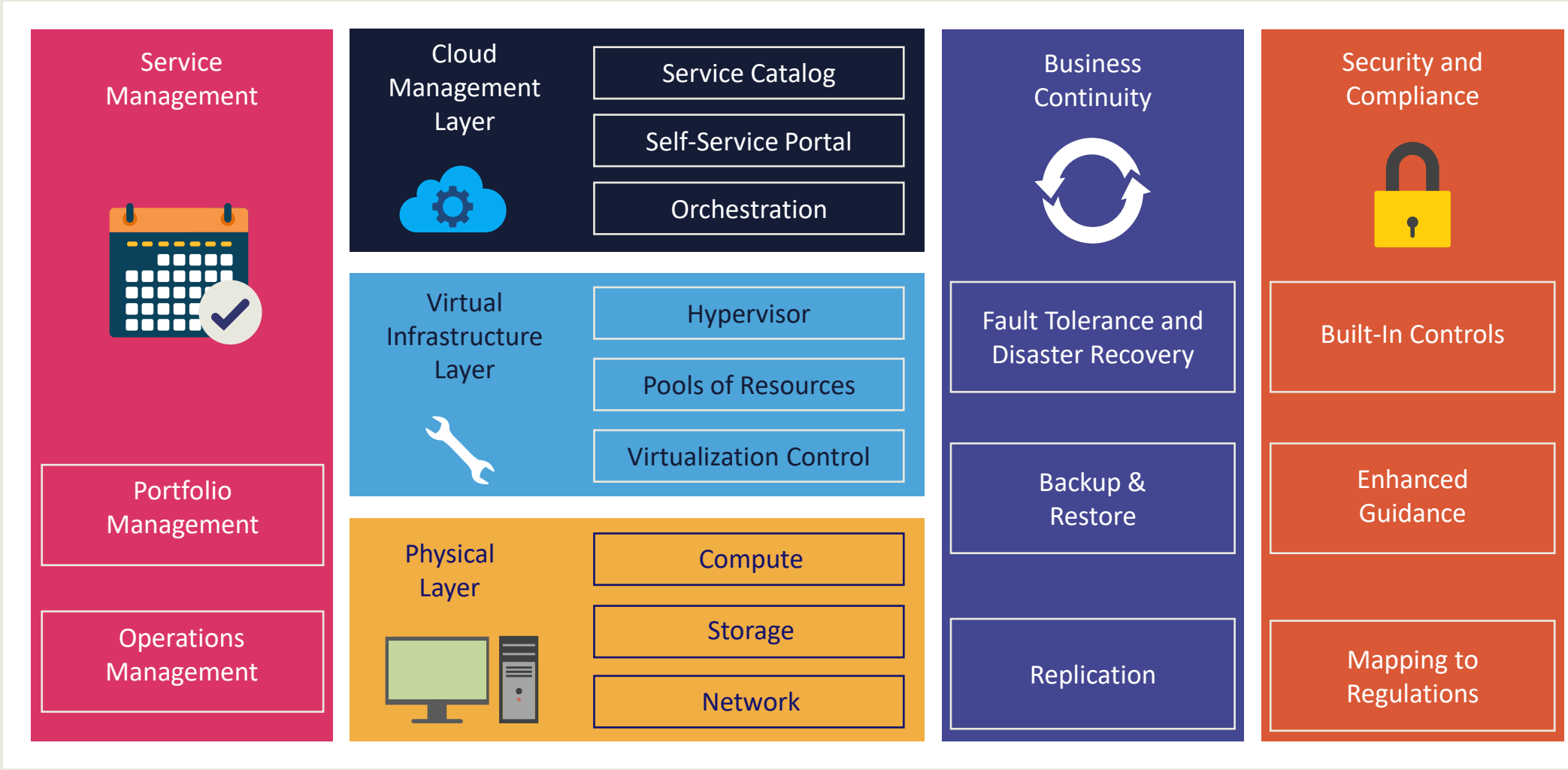


Mitigate Resource Exhaustion



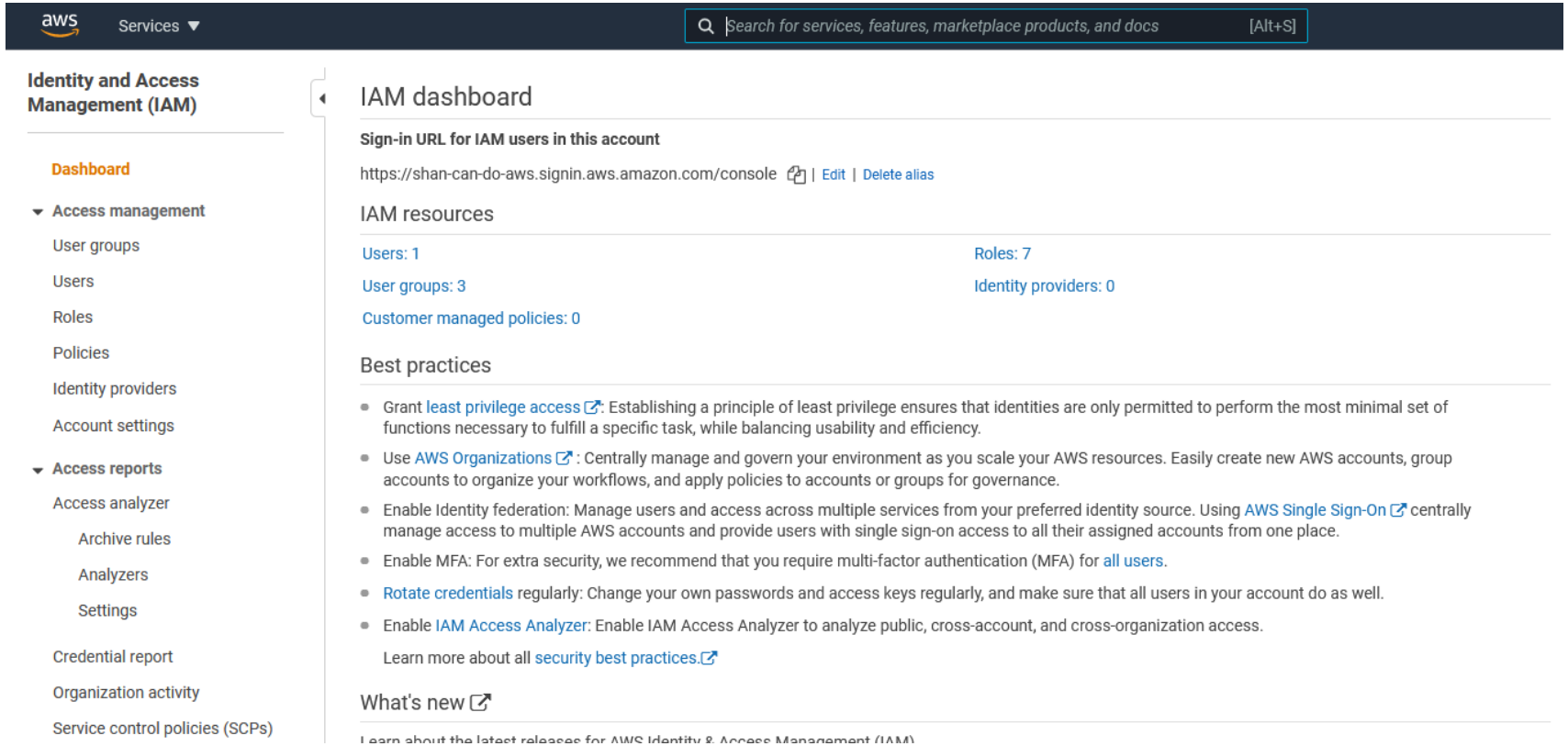
- Implement appropriate resource allocation and/or reservation policies based on classification of VMs based on sensitivity and/or risk level
- Use anti-virus and other security software that is virtualization-aware
- Implement mechanisms to minimize resource contention including staggering the scanning of VMs on the same physical server, using agentless deployment of anti-virus software, implementing distributed storage resources, and implementing a workload affinity policy
- Define and implement a standard operating procedure that detects VMs that are throttled due to resource exhaustion

VMWARE SECURITY DESIGN



Identification, Authentication and Authorization in Cloud Infrastructure

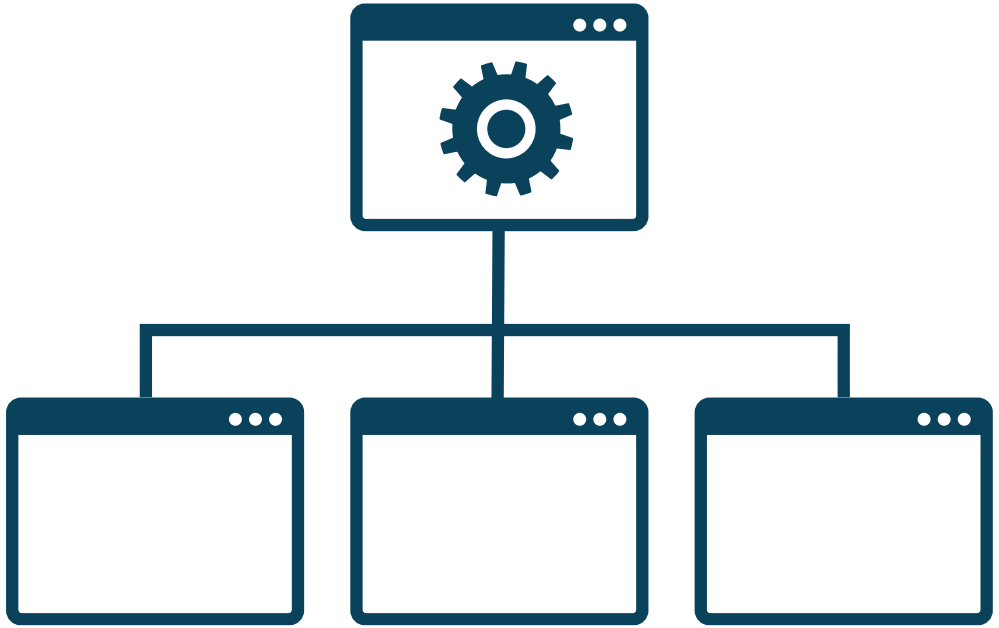
Demonstration: AWS IAM



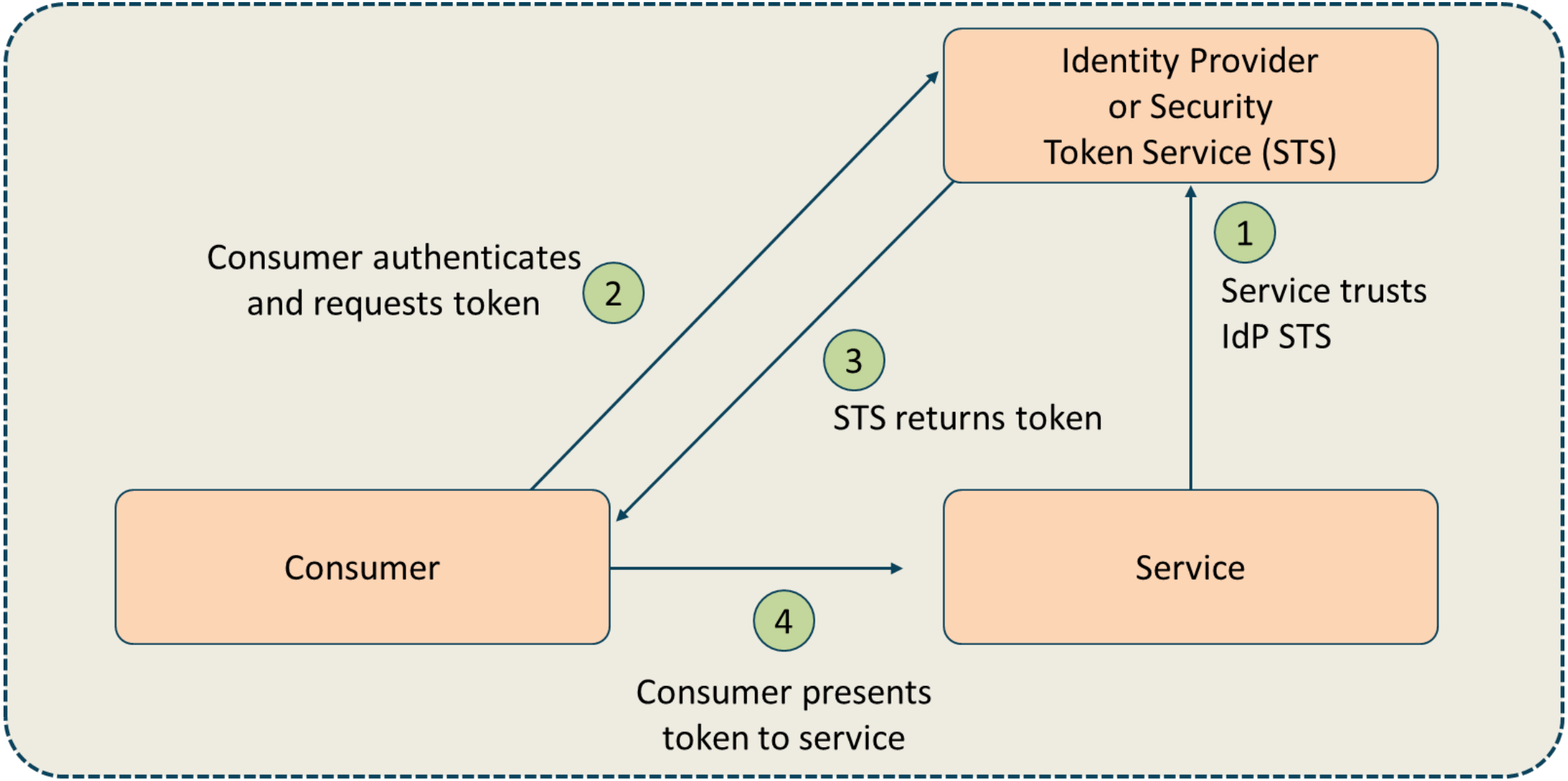
Federation Standards

For federated identity management

- Used to manage identities across different organizations
- Provides single sign-on for multiple organizations and service providers
- Web-of-trust model is where each member of the federation approves each other member
- The third-party identifier model relies on a trusted third-party
  - This is a popular model for the cloud as the identifier can be combined with other services like key management
  - Often outsourced to a Cloud Access Security Broker (CASB) or Managed Security Service Provider (MSSP)



Federated Identity Providers



SAML 2.0

- Security Assertion Markup Language
- SAML is an XML-based open-source SSO standard
- **SAML is used by many cloud SSO connections for thousands of large enterprises, government agencies, and service providers that communicate on the Internet**
- Key advantage of SAML is open-source interoperability
- Some large companies now require SAML for Internet SSO with SaaS applications and other external ISPs

SAML 2.0

Identity Provider

- The SAML identity provider declares the identity of the user along with additional metadata in an assertion
- Directory services like LDAP and Active Directory are common identity providers

Service Provider

- The service provider takes the assertion and passes the identity data to an application or service
- Common service providers are cloud services and social media sites

OAUTH

- **OAuth 2.0 is an open authorization framework that allows a third-party application to get limited access to an HTTP service**
- Developers use OAuth to publish and interact with protected data in a safe and secure manner
- Service provider developers can use OAuth to store protected data and give users secure delegated access
- OAuth is designed to work with HTTP and basically allows access tokens to be issued to third-party clients by an authorization server with the approval of the resource owner
- The third party then uses the access token to access the protected resources offered by the resource server

OpenID Connect (OIDC)

Often combined with OAUTH

- **OpenID Connect 1.0 is a basic identity layer on top of the OAuth 2.0 protocol**
- It verifies the end-user identity using an authorization server
- It can get basic profile information about the user with an interoperable REST-like methodology
- Supports web-based, mobile, and JavaScript clients
- OpenID is extensible as functionality can be added

Step-Up Authentication

- Ensures that users can access some resources with one set of credentials but will prompt them for more credentials when they request access to more sensitive resources, for example:
  - Users want seamless SSO access to certain assets, but organizations may want to further verify their identities before they grant access to anything more sensitive
  - Employees need occasional access to private data that would cause damage if exposed
  - You want to deploy a membership model that limits complete access to your site or service to paying users
- Step-up authentication enables you to provide easy access to one layer of resources and secure access to another layer of resources

Audit Mechanisms

Involves tools and techniques

- Various logs (system, application, firewall, etc.)
- Simple Network Management Protocol (SNMP) traps and informs
- NetFlow v5 and v9 collections
- **Security information and event management (SIEM) systems**
- **Security Orchestration, Automation, and Response (SOAR)**
- Next-Generation Intrusion Prevention System (NGIPS) alerts and logs
- Cloud-based ML and AI visibility/analysis

SIEM

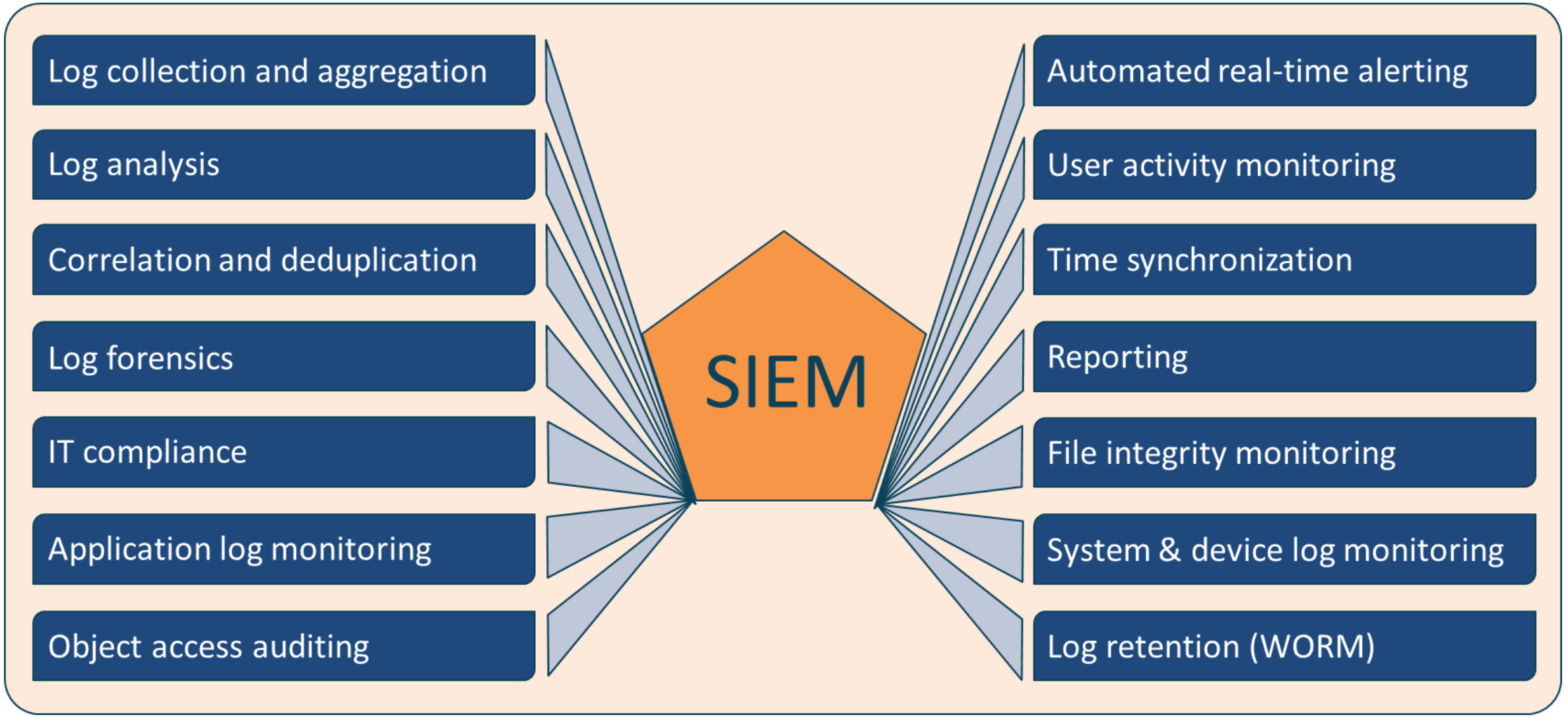
The term SIEM is a combination of security event management (SEM) and security information management (SIM)

Centralize the storage and analysis of logs and other security-related documentation to perform near real-time analysis

Can send filtered data to mining, big query, and data warehousing servers in a data center or at a cloud service provider

Allow security and network professionals to take countermeasures, perform rapid defensive actions, and handle incidents

SIEM


Log collection and aggregation
Log analysis
Correlation and deduplication
Log forensics
IT compliance
Application log monitoring
Object access auditing
SIEM
Automated real-time alerting
User activity monitoring
Time synchronization
Reporting
File integrity monitoring
System & device log monitoring
Log retention (WORM)

Automation and Orchestration

Automation

- IT automation involves generating a single task to run automatically without any human intervention
- Automation could involve sending alerts to a SIEM system, dynamically triggering a serverless function at a cloud provider, or adding a record to a database when a batch job is run
- Enterprises often automate both cloud-based and on-premise tasks

Orchestration

- Orchestration involves managing several or many automated tasks or processes
- As opposed to focusing on one task, orchestration combines all the individual tasks
- Orchestration occurs with various technologies, applications, containers, datasets, middleware, systems, and more

Security Orchestration, Automation, and Response (SOAR)

- SOAR is an assortment of software services and tools
- It allows organizations to simplify and aggregate security operations in three core areas
  - Threat and vulnerability management
  - Incident response
  - Security operations automation
- Security automation involves performing security related tasks without the need for human intervention
- Can be defensive detection, response, and remediation, or offensive vulnerability assessment and penetration testing
- You should automate if the process is routine, monotonous, and time-intensive

4 Key SOAR Elements

1. SIEM use cases, categories, and SIEM Rules are mapped to incident categories and these categories are then mapped to playbooks

2. Three types of playbooks: Manual playbooks (a series of manual tasks); Semi-Automated playbooks (a hybrid of automated and manual subtasks); and Fully-Automated playbooks (completely automated)

3. Four types of Automation

a. Defensive Automation (anything that tries to prevent the threat or risk)

b. Forensic Automation (anything that tries to retrieve additional evidence)

c. Offensive Automation (anything pro-active that tries to investigate an asset)

d. Deception Automation (anything that retrieves or adjusts deception tools)

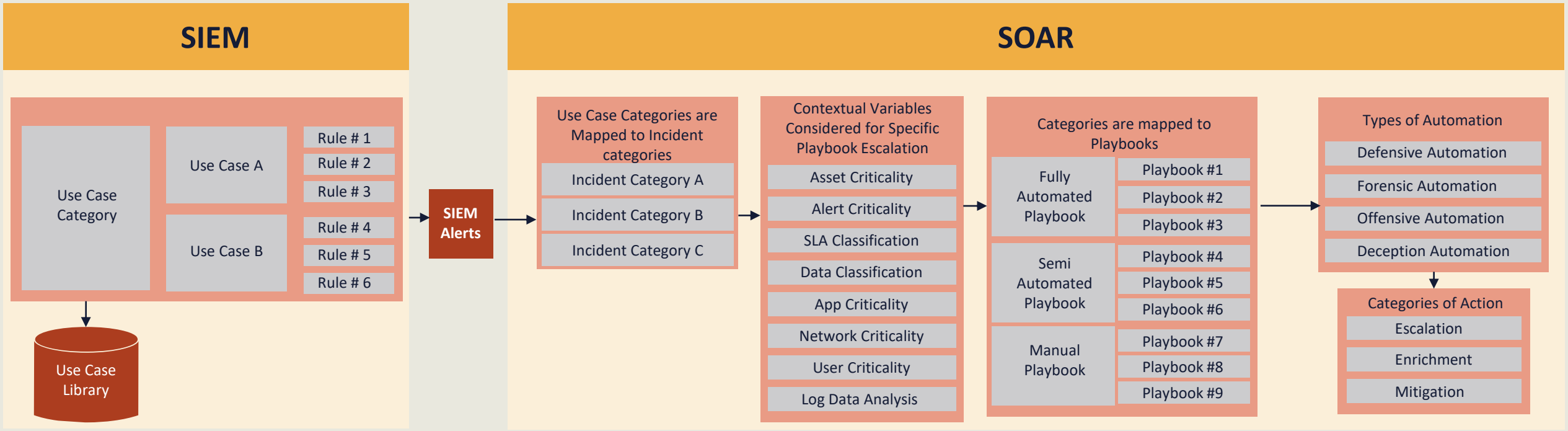
4. Three different categories of action

a. Enrichment (adding additional CMDB or environment data)

b. Escalation (e-mail, ticket escalation, SNS, chat/messaging communication)

c. Mitigation (the modification of device configuration)

SIEM AND SOAR

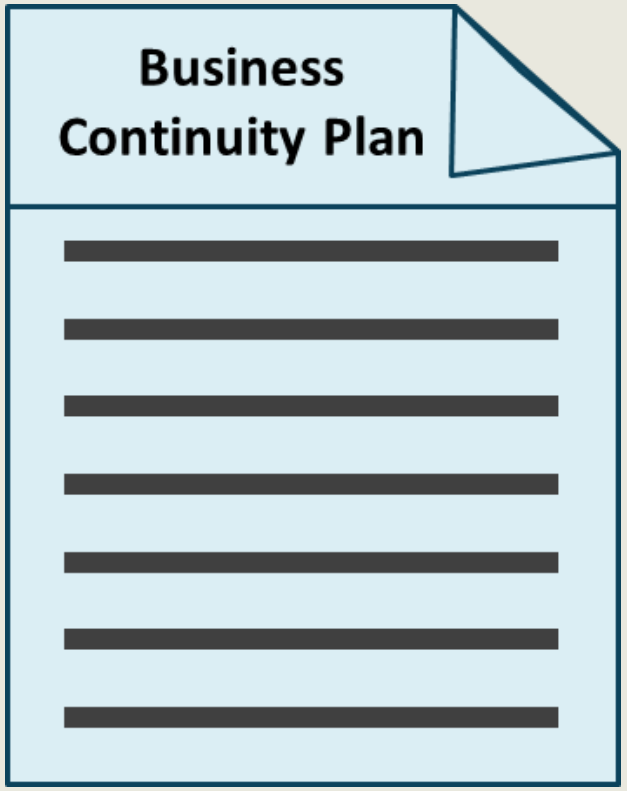


3.5 Plan Disaster Recovery (DR) and Business Continuity (BC)

- Risks Related to the Cloud Environment
- Business Requirements (e.g., Recovery Time Objective (RTO), Recovery Point Objective (RPO), Recovery Service Level (RSL))
- Business Continuity/Disaster Recovery Strategy
- Creation, Implementation and Testing of Plan

BCP/COOP

- Ensures business operates a pre-determined level when disaster strikes
  - Documents approved by executive management
- Outlines risk to business
  - Populates risk register/ledger
  - Requirements to mitigate incidents
- Identifies procedures needed to recover from a disaster
  - What is an acceptable amount of time?
  - How to reduce the impact of the disaster



NIST SP 800-34, Revision 1

BCP according to NIST

1. Develop a continuity planning policy statement
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training, and exercises
7. After-action report
8. Ensure plan maintenance

BCP from Ready.gov

Business impact analysis

- Develop questionnaire
- Conduct workshop to instruct business function and process managers how to complete BIA
- Receive complete BIA questionnaire forms
- Review BIA questionnaires
- Conduct follow-up interviews to validate information and fill any gaps

Recovery strategies

- Identify and document resource requirements based on BIAs
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities
- Explore recovery strategy options
- Select recovery strategies with management approval
- Implement strategies

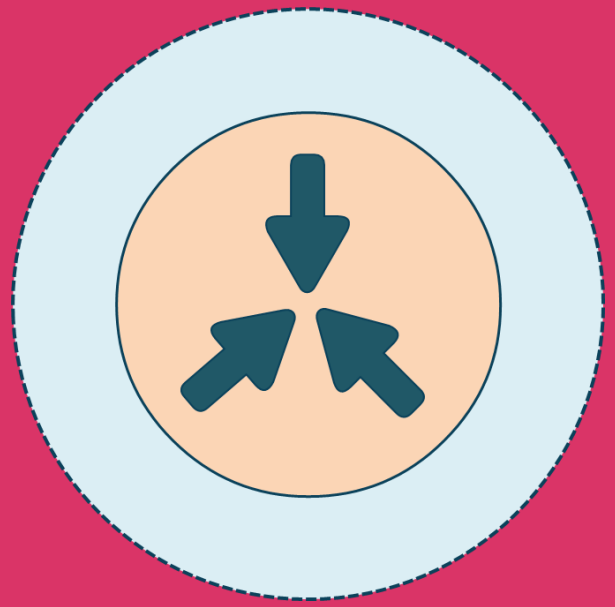
Plan development

- Develop plan framework
- Organize recovery teams
- Develop relocation plans
- Write business continuity and IT disaster recovery procedure
- Document manual workarounds
- Assemble plan
- Validate and gain management approval

Testing & exercises

- Develop testing, exercise, and maintenance requirements
- Conduct training for business continuity team
- Conduct orientation exercises
- Conduct testing and document test results
- Update BCP to incorporate lessons learned from testing and exercises

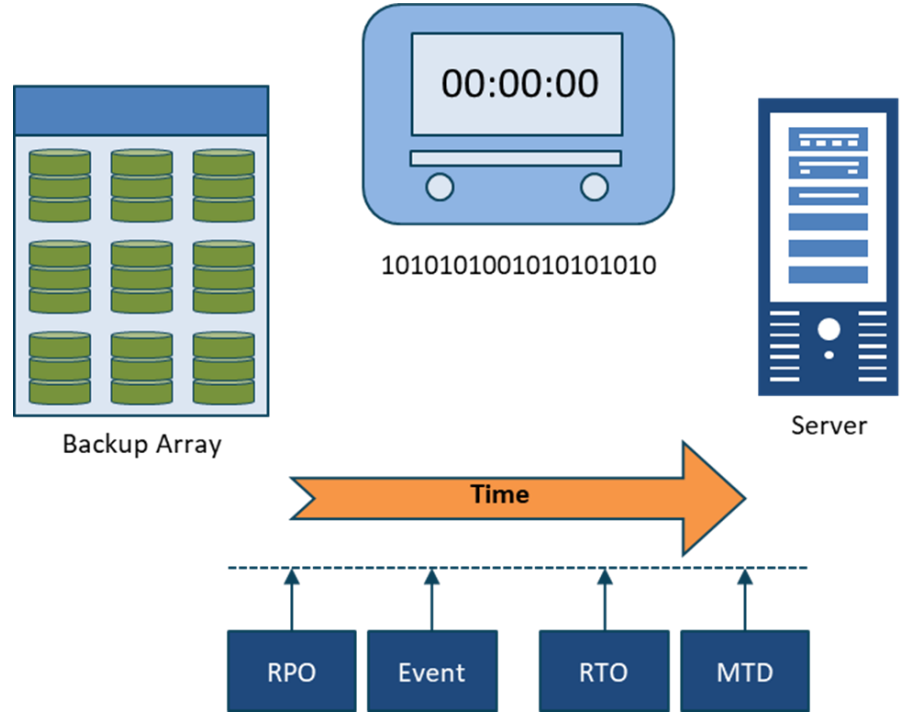
Business Impact Analysis



- The risk assessment aspect of the Business Continuity Plan (BCP) or (COOP)
- Identify critical functions to the business and prioritize them based on need for survival
- Identify the risks associated with the critical functions
- The probability of the risk occurring (likelihood)
- The impact the risk will have (magnitude)
- Identify how to eliminate the risk or reduce the risk

Recovery Time Objective (RTO)

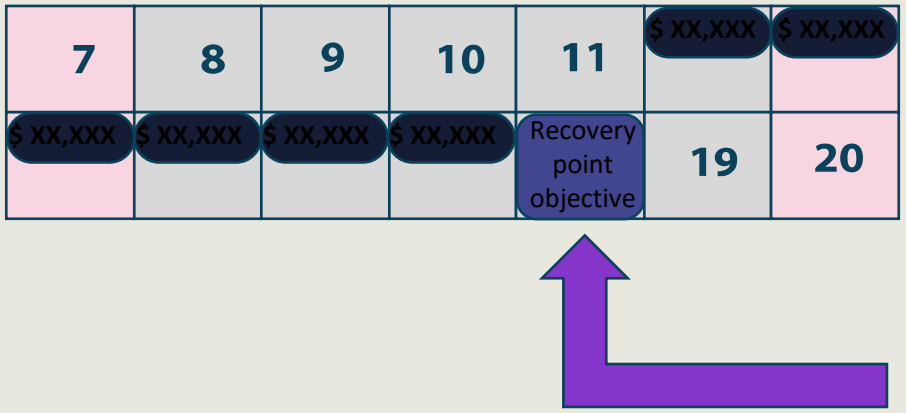
- The amount of time available to recover the resource, service, and function
- Must be equal to or less than Maximum Tolerable Downtime (MTD)
- Any solutions must be accomplished within this time frame, or it is considered loss
  - Add physical security
  - Add redundancy
  - Purchase insurance
  - Invest in backup generators
  - Invest in faster
  - Safeguard media off-site



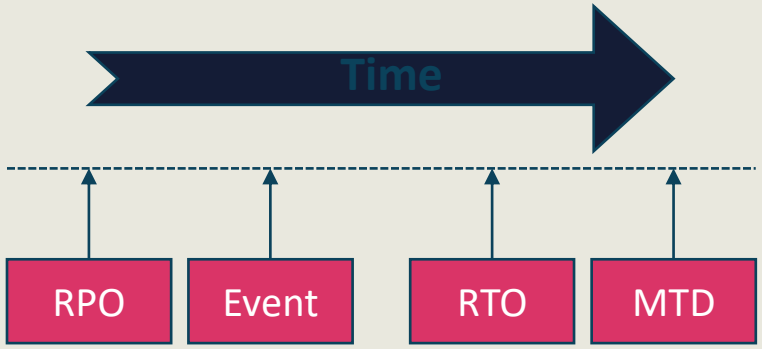
Recovery Point Objective (RPO)

The point in time, relative to a disaster, where the recovery process begins

- How much work can be lost if a disruption occurs?
- What impact will it have?
- How do we make sure we don't lose more than "X" information?



SUN	MON	TUE	WED	THU	FRI	SAT
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

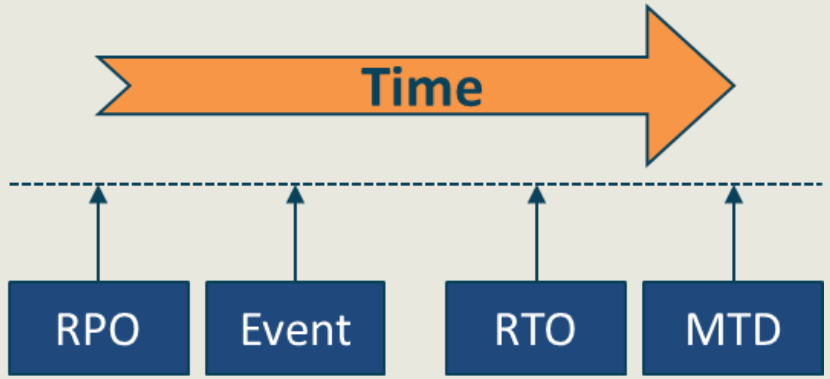


Maximum Tolerable Downtime (MTD)

Absolute maximum amount of time that a resource, service, or function can be unavailable before we start to experience a loss

Factors to consider include

- finances
- life/safety
- regulatory
- legal/contracts
- reputation, and
- property



Mean Time Between Failures (MTBF)

- A measure of how reliable a hardware system or component is
- For most devices, the measure is in thousands or tens of thousands of hours between failures
- For example, an SSD drive may have a mean time between failures of 10 years

Mean Time To Repair (MTTR)

- How long does it take to repair?
  - Measures time to fix
  - Average value predicted based on experience and documentation
  - (Total down time)/(number of breakdowns)

Disaster Recovery Planning (DRP)

- Ensuring that the company can recover to an established baseline of continuity after any kind of high-level incident
- The tasks and processes that will be conducted when a disaster or catastrophe strikes
- Incident can affect a single drive, an entire server, a VLAN, an area of the facility, an entire floor or building, or the entire site or campus

Disaster Recovery Planning (DRP)

- Outlines the technical aspects involved for restoration
  - Recovery sites: hot, warm, cold, mobile, cloud, shared
  - Order of restoration (most critical to least critical)
  - Backups, snapshots, and restores
  - Contact information
  - Communication plans
  - Chain of authority
  - Step-by-step instructions
  - Locations of documents, software, and keys

Disaster Recovery Site Strategies

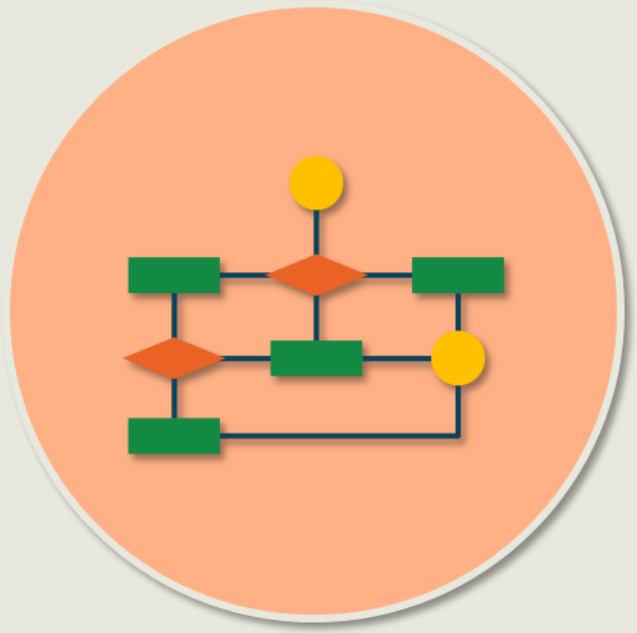
Recovery strategy	Recovery time	Advantages	Disadvantages
Commercial hot site	0 to 24 hours	• Fastest recovery time • Smoothest deployment, as facility, equipment, application software, data, and OS are installed and running • Easy to test when necessary • The optimal solution for recovering on-going operations	• The most expensive solutions often need to replicate all equipment and software, including on-going version and patch management issues • Continuous communication costs to duplicate data are very high • Terms of agreement may limit the duration of use especially if part of shared reciprocal agreement • Vendors will often prioritize only the larger customers in a real-world disaster scenario
Warm site	24 to 48 hours	• Moderately priced • A basic infrastructure is in place to support recovery operations – e.g., wireless network only • Allows for some degree of pre-staging of the necessary hardware, application software, OS software, data, and communications	• Not as easy to test • Recovery time is longer than with hot site and is dependent on the time to locate and restore applications • Facility equipment may not be exactly what is needed • Once the recovery begins delays may occur because of equipment, software, or staffing shortfalls
Cold site	72 plus hours	• Lowest cost solution • Basic infrastructure, power, air, and communication are in place and ready • Can rent the facility for a longer term at lower cost • Costs can be lowered even further using reciprocal agreements	• Longest recovery time • All equipment must be ordered, delivered, installed, and made operational • Worst solution for supporting on-going and mission-critical production operations
Cloud	0 to 24 hours	• Could be a lower cost hot/warm solution in the long run based on economy of scale and multitenancy of cloud provider • Data and applications available immediately • Location-independent • Easy to test	• Security may be an issue based on shared responsibility model • May not be feasible due to compliance and regulations • May not allow enough time for a daily cycle processing window

Test Disaster Recovery Plans

Read-through testing

- Read-through (plan review) is where the business continuity plan owner and business continuity team discuss the business continuity plan
- Look for missing elements and inconsistencies within the plan or with the organization
- A type of checklist test useful to train new members of a team, including the business function owner

Test Disaster Recovery Plans



Tabletop testing

- Participants gather in a room to execute documented plan activities in a stress-free environment
- Can use blueprints, topological diagrams, or computer models to effectively demonstrate whether team members know their duties in an emergency and if they need training
- Documentation errors, missing information, and inconsistencies across business continuity plans can be identified

Test Disaster Recovery Plans

Walkthrough testing

- Planned rehearsal of a possible incident designed to evaluate an organization's capability to manage that incident
- To provide an opportunity to improve the organization's future responses and enhance the relevant competences of those involved
- Often done on a limited basis or by scheduling each department or building separately for fire and active shooter drills

Test Disaster Recovery Plans

Simulation testing

- To determine if business continuity management procedures and resources work in a realistic situation, a simulation exercise is desirable
- May be the most elaborate test most entities ever conduct
- Uses established business continuity resources, such as the recovery site, backup equipment, services from recovery vendors, and transportation
- It can require sending teams to alternate sites to restart technology as well as business functions

Test Disaster Recovery Plans

Parallel testing

- A parallel test involves bringing the recovery site to a state of operational readiness, but maintaining operations at the primary site
- Staff are relocated, backup tapes are transferred, and operational readiness established in accordance with the disaster recovery plan while operations at the primary site continue normally
- May be the most comprehensive test most entities ever conduct

Test Disaster Recovery Plans

Full interruption testing

- Operations are completely shut down at the primary site to fully emulate the disaster
- Enterprise transfers to the recovery site in accordance with the disaster recovery plan
- A very thorough test, which is also expensive (may be cost-prohibitive)
- Has the capacity to cause a major disruption of operations if the test fails

Lessons Learned

From the After-action reporting

- Knowledge gained from the process of conducting the program, project, or task included in After-Action Report (AAR)
- Formal sessions usually held at the project close-out, near the completion of the initiative
- Recognized and documented at any point during the life cycle to:
  - share and use knowledge derived from an experience
  - endorse the recurrence of positive outcomes
  - prevent the recurrence of negative outcomes