Welcome to the Security+ Bootcamp

Your instructor:

Michael J Shannon

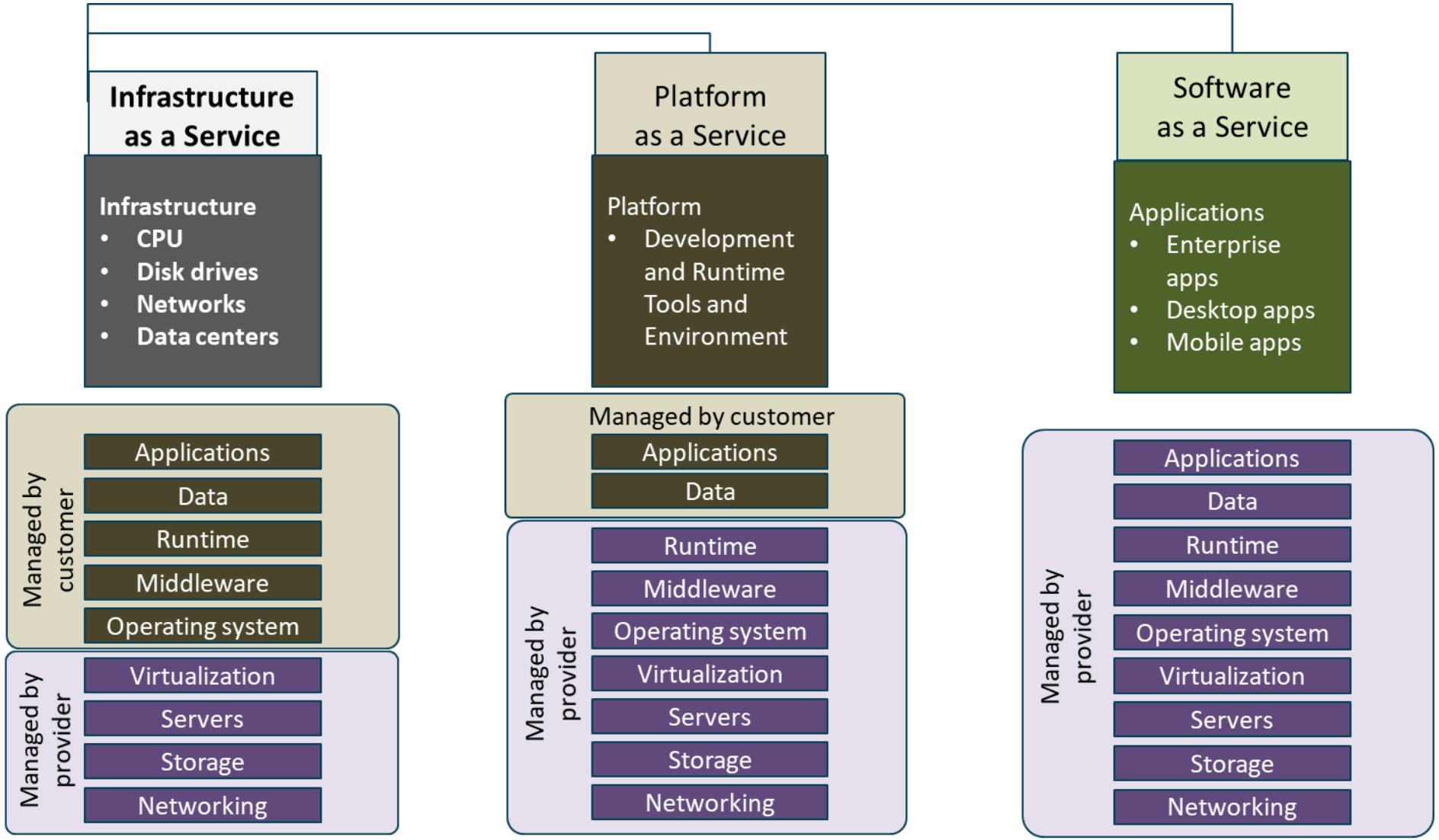
CISSP #42221 / #524169,
CCNP-Security, PCNSE7,
Security+, GIAC GSEC,
OpenFAIR, and
ITIL 4 Managing Professional

Class will begin at 10:00 A.M. Central Standard Time (CST)

Cloud Computing Value Propositions

- Cost savings and resource pooling
- Rapid elasticity and agility
- On-demand service with broad access
- Measured services with visibility
- Security and shared responsibility

Cloud Computing Service Types

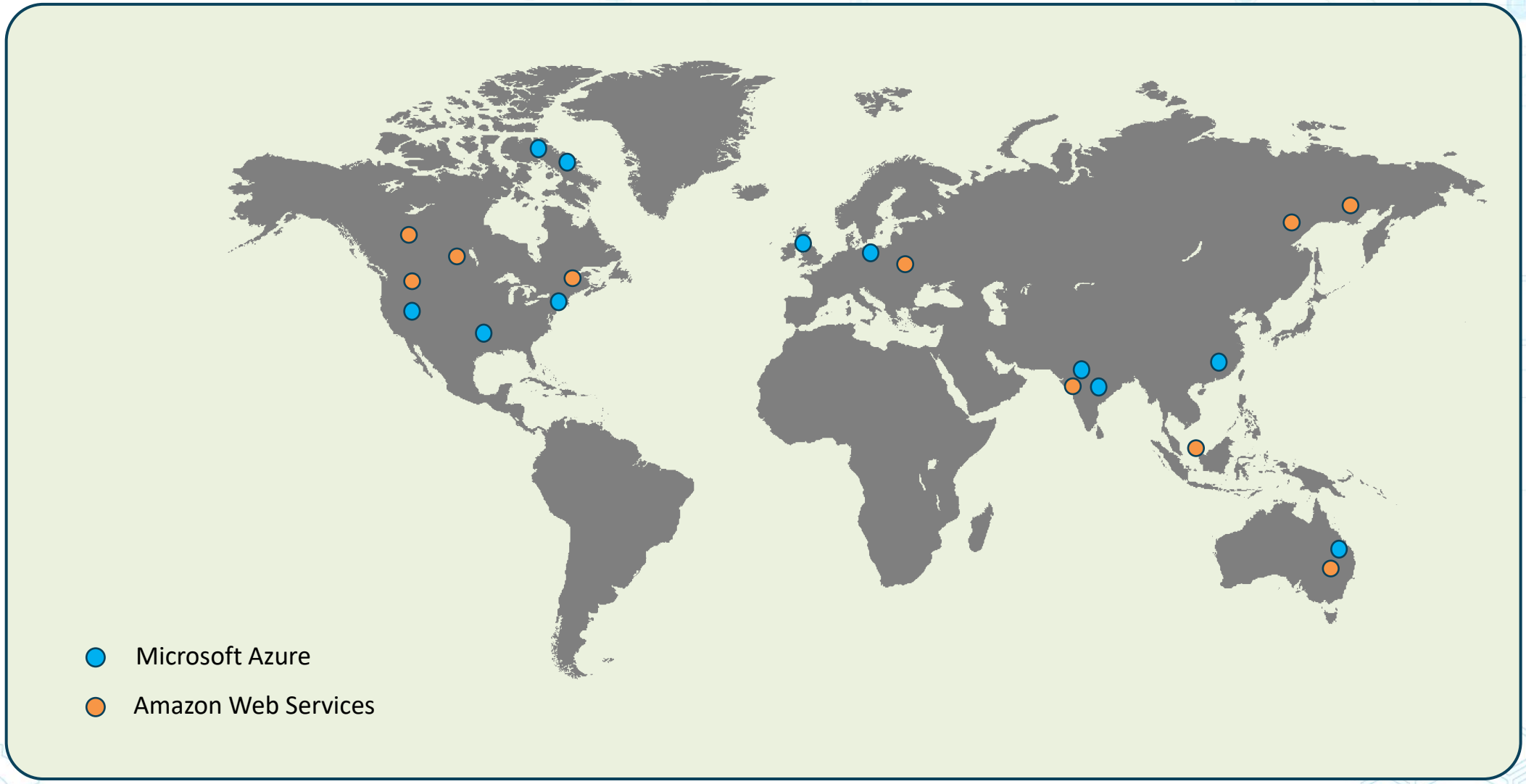


IaaS According to NIST

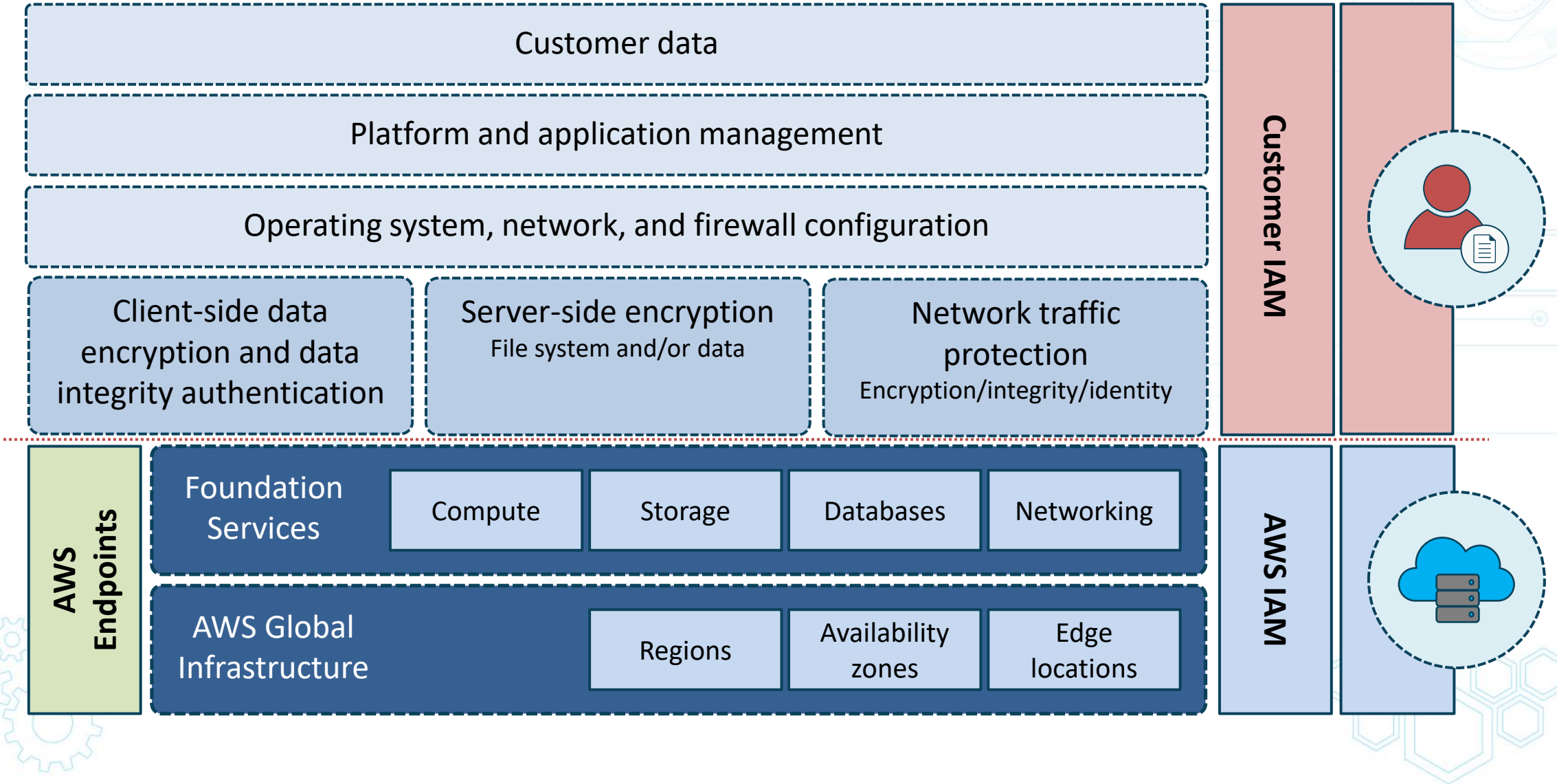
“Infrastructure-as-a-service is where the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)."

Cloud Providers Global Infrastructure



IaaS at Amazon Web Services



PaaS According to NIST

“Platform-as-a-service is the when the provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations"

Common PaaS Services

Development and SDK platforms for Java, PHP, Python, etc.

Container services for Docker and Kubernetes

Managed and fully managed relational and document databases

Managed security and threat modeling services

SSO, machine learning, AI, IoT, Blockchain, media services

SaaS According to NIST

"The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.

"The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

Common SaaS Offerings

- Customer Relationship Management (CRM)
- Human Resources and workplace tools
- Finance, sales, and marketing
- E-mail, collaboration, and storage
- Help Desk and Service Desk

Cloud Deployment Models

Private - deployed in sandbox within an organization

Public - deployed by a provider for customer consumption

Community - deployed by a consortium in a certain sector

Hybrid - combination of private, public, or community

AWS Service Offerings

Archiving

Reasonably priced solutions for data archiving up to petabyte scale

Backup and restore

Durable and cost-effective choices for backup and disaster recovery

Blockchain

Shared ledgers for trusted connections between multiple entities

Business applications

Simplified management and lower cost business applications

Cloud migration

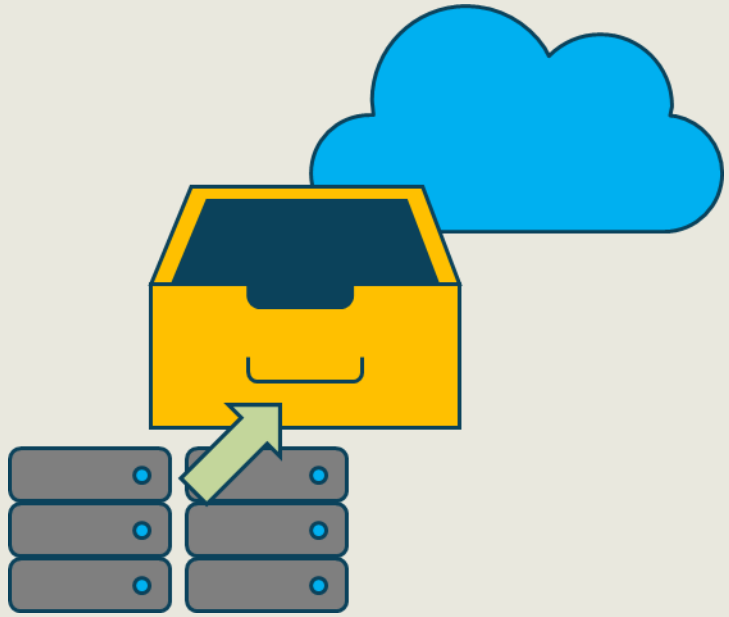
Fluid and simplified migration of applications and data to AWS

Containers

Fully managed services for workloads with Docker and Kubernetes

Content delivery

Low latency, cached delivery of web sites, APIs, and video content



AWS Service Offerings

Database migrations

Time and cost-effective migration to managed and fully managed databases

Data Lakes and analytics

Secure, scalable, and cost-effective data lake and analytics services

DevOps

Rapidly and consistently build and deliver solutions using DevOps practices

E-Commerce

Highly scalable and secure offerings for online sales and retail businesses

High performance computing

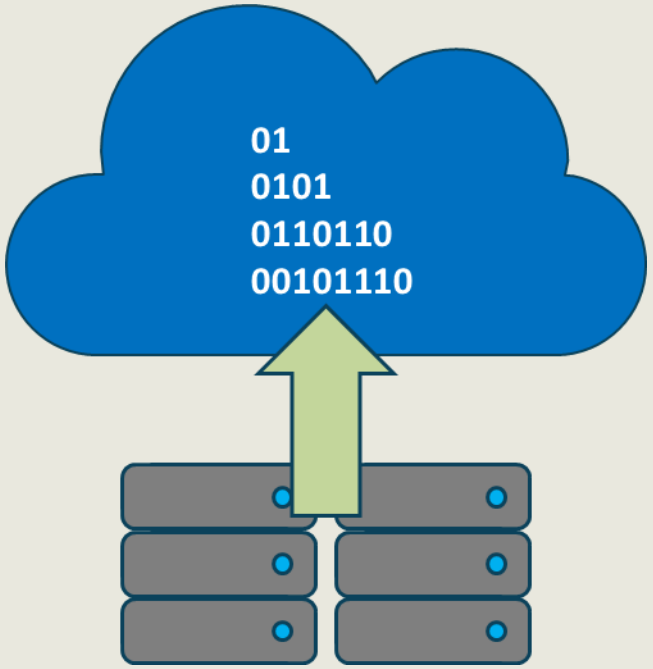
Superior networking and cloud sized clusters for multifaceted challenges

Hybrid cloud architectures

Extend the on-premise IT infrastructure to the AWS cloud

Internet of things

Scale to billions of devices and messages with cutting-edge solutions



AWS Service Offerings

Machine learning

Leverage wide-ranging machine learning framework support

Mobile services

Solutions to help enable mobile application development at scale

Modern application development

Produce and advance applications through rapid innovation lifecycles

Remote work and learning

Modern solutions for remote teleworkers, students, and center agents

Scientific computing

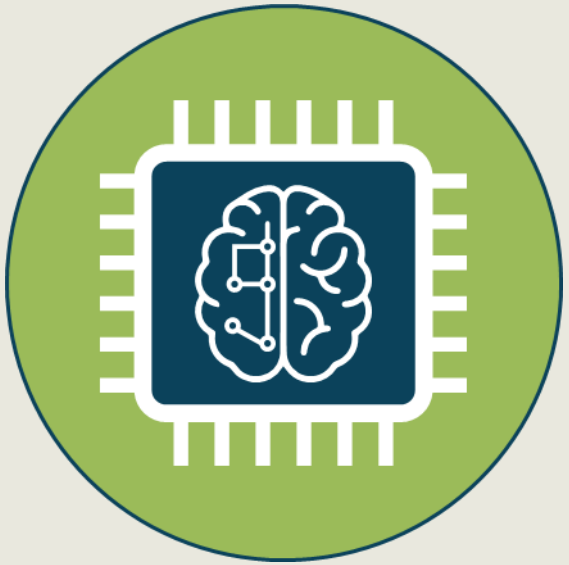
Perform analysis, object storage, and distribution of enormous data sets

Serverless Computing

Build and run applications without needing underlying servers

Web sites

Use dependable, highly scalable, and affordable web application tools



Managed Security Service Providers (MSSP)

- Offers outsourced security monitoring and management for security systems and devices
- These security services can apply to on-premise resources, cloud resources, or both
- Use high-availability security operation centers (either from their own facilities or from other data center/cloud providers)
- Common MSSP services include:
  - Managed layer 3-7 firewalls
  - Intrusion detection and prevention (IDS/IPS)
  - Endpoint response and detection
  - Virtual private networking support
  - Vulnerability scanning and anti-viral services

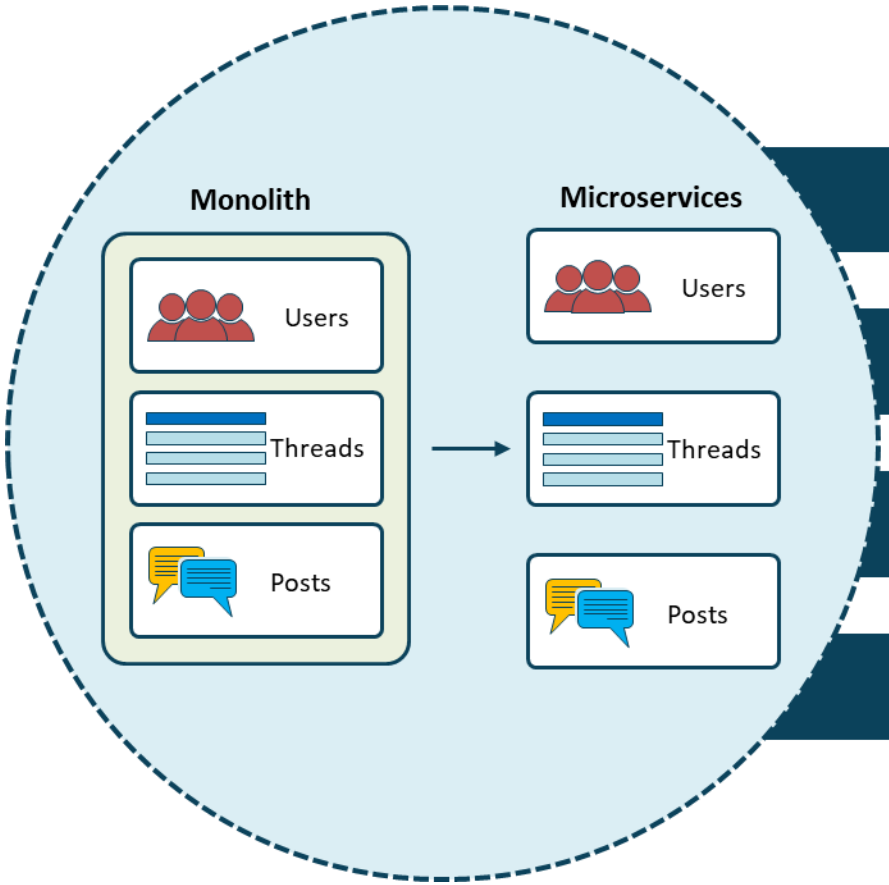
Fog Computing

- Fog computing is also known as 'fogging' and 'fog networking’
- A decentralized computing arrangement where resources such as data and applications are put in logical locations between the data source and the cloud
- Brings analysis services to the network edge
- Improves performance by placing resources close to where they are needed
- Can also be a security countermeasure for securing data

Microservices

- Microservices are specific service-oriented application components
- They are an architectural approach to software development where the results are made up of small independent services that communicate over well-defined APIs
- These services are typically maintained by small, self-contained teams of developers
- Microservices architectures make applications faster to develop and easier to scale
- They enable innovation and fast-tracked delivery of new application features

Microservices

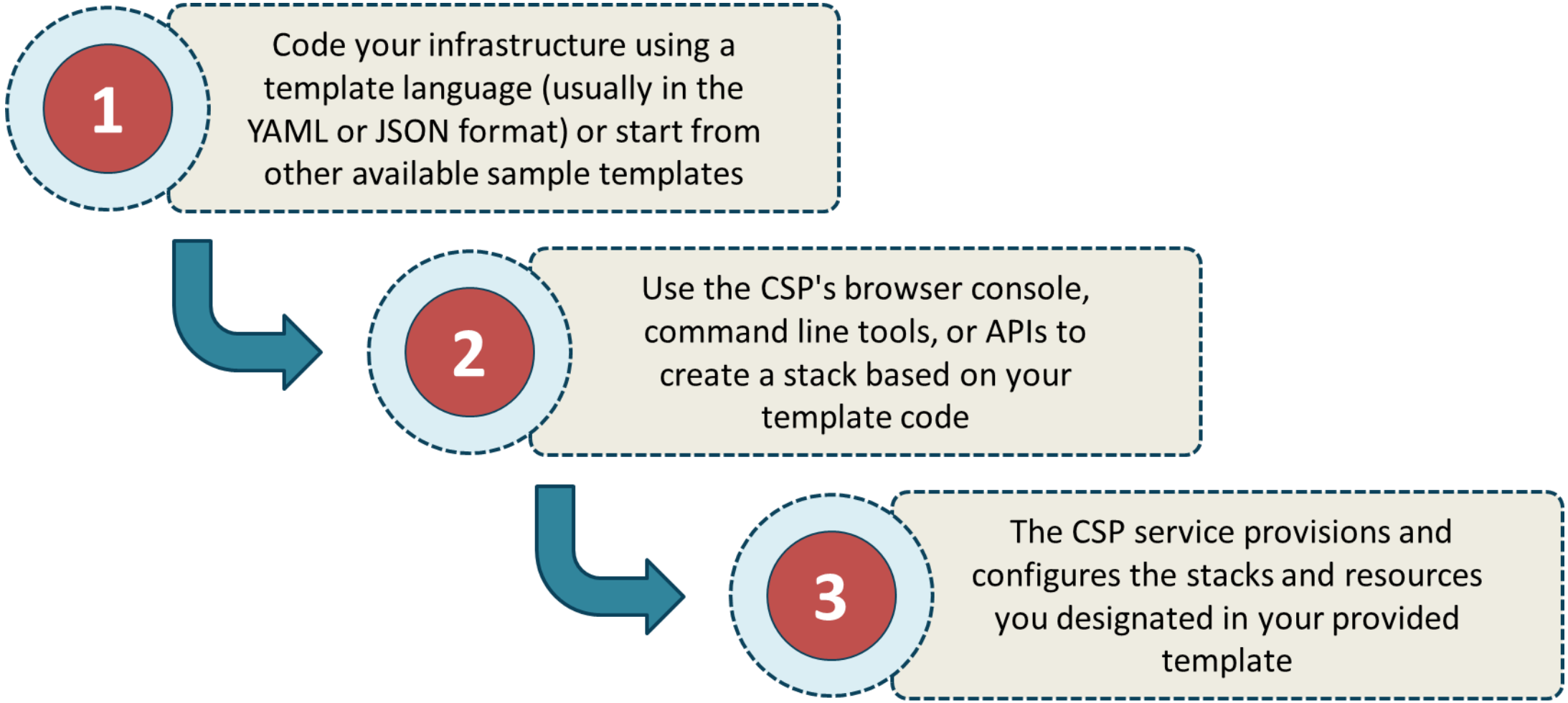


- Tightly scoped but loosely coupled
- Thoroughly modular and encapsulated
- Independently deployable
- Freely scalable

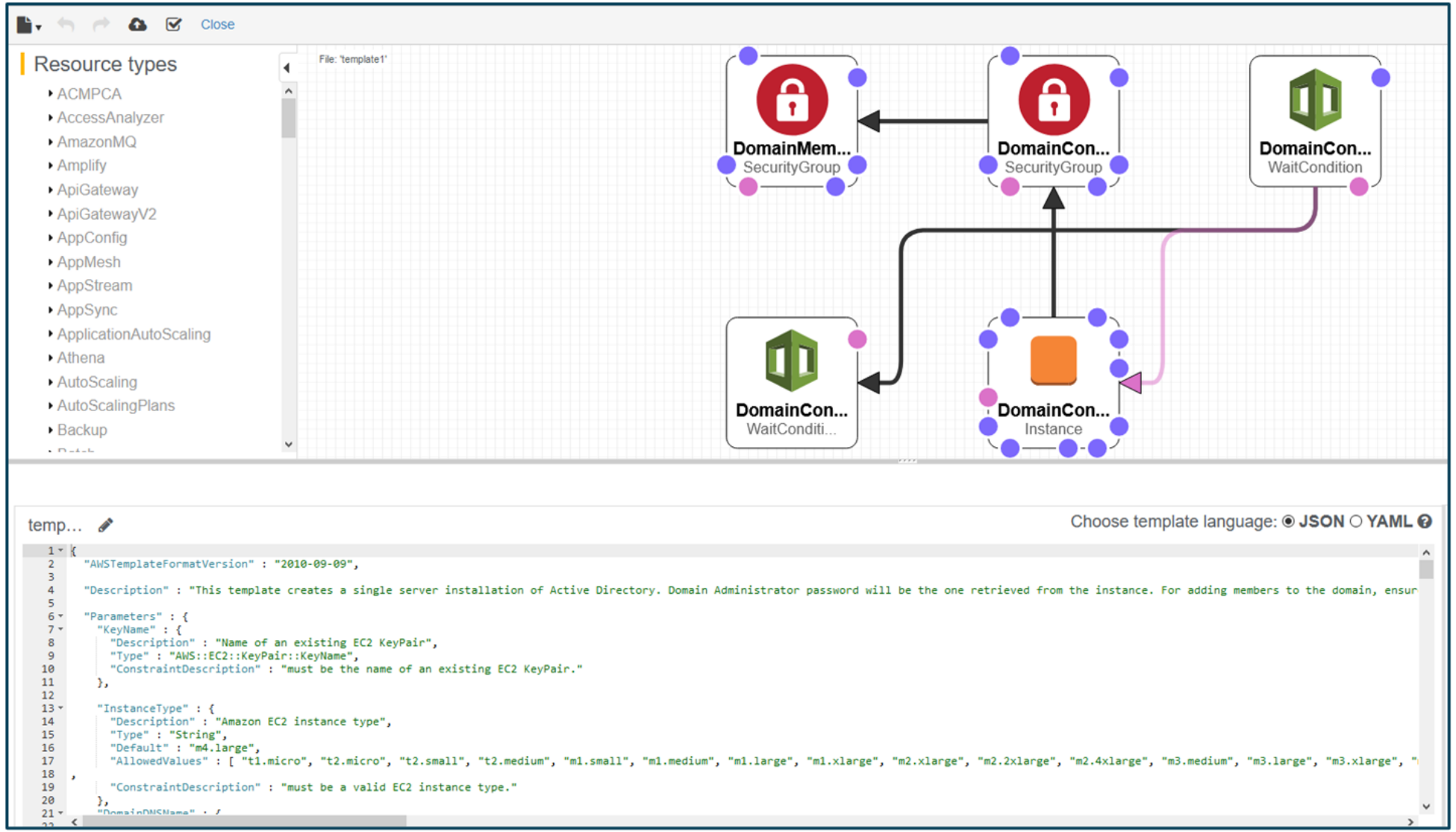
Infrastructure -as-Code

- Infrastructure as Code offers a common language in a file format, defining cloud deployment of infrastructure resources in a secure and repeatable manner
- The stack files can represent a "single source of truth" of your deployment
- A stack is a templatized collection of cloud provider resources that you can control as a single unit
- A stack set allows you to generate, update, or delete stacks across multiple CSP accounts and regions using a single operation via a console or CLI

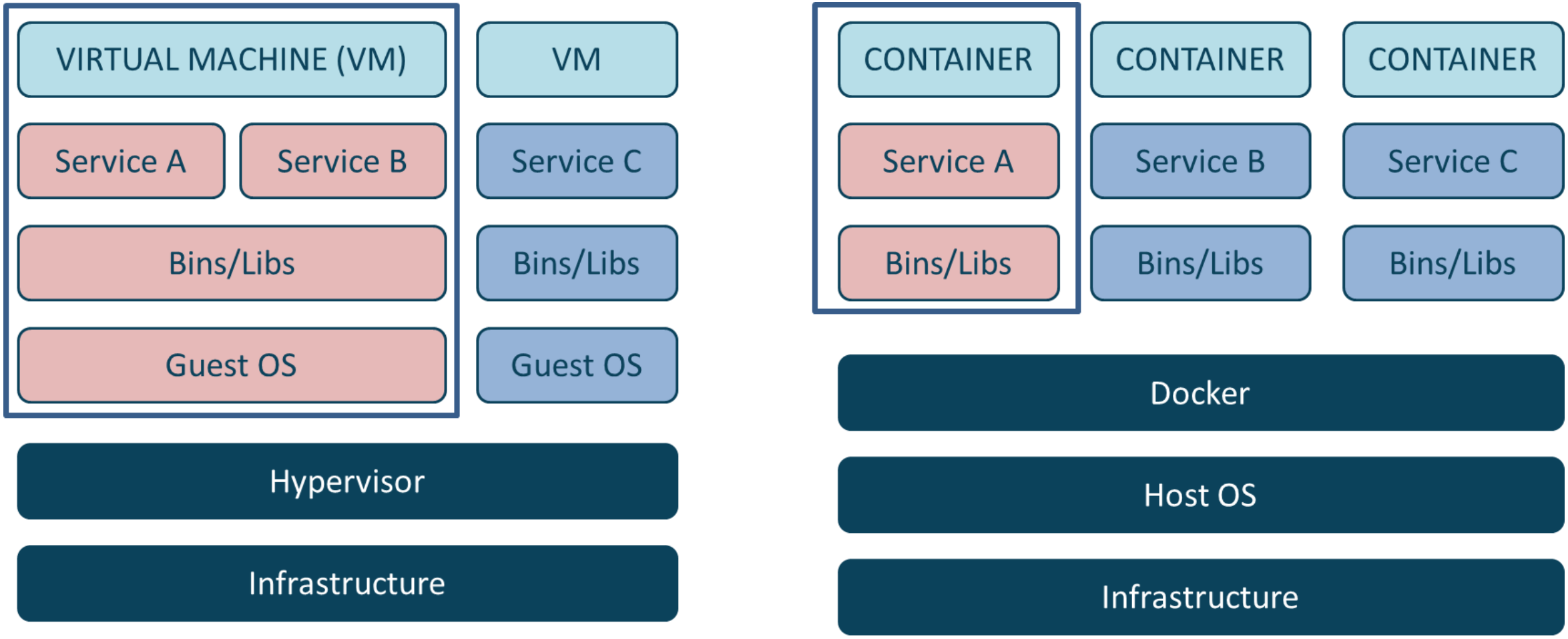
Infrastructure-as-Code



Infrastructure-as-Code



Virtual Machines vs. Containers



Docker vs. Kubernetes

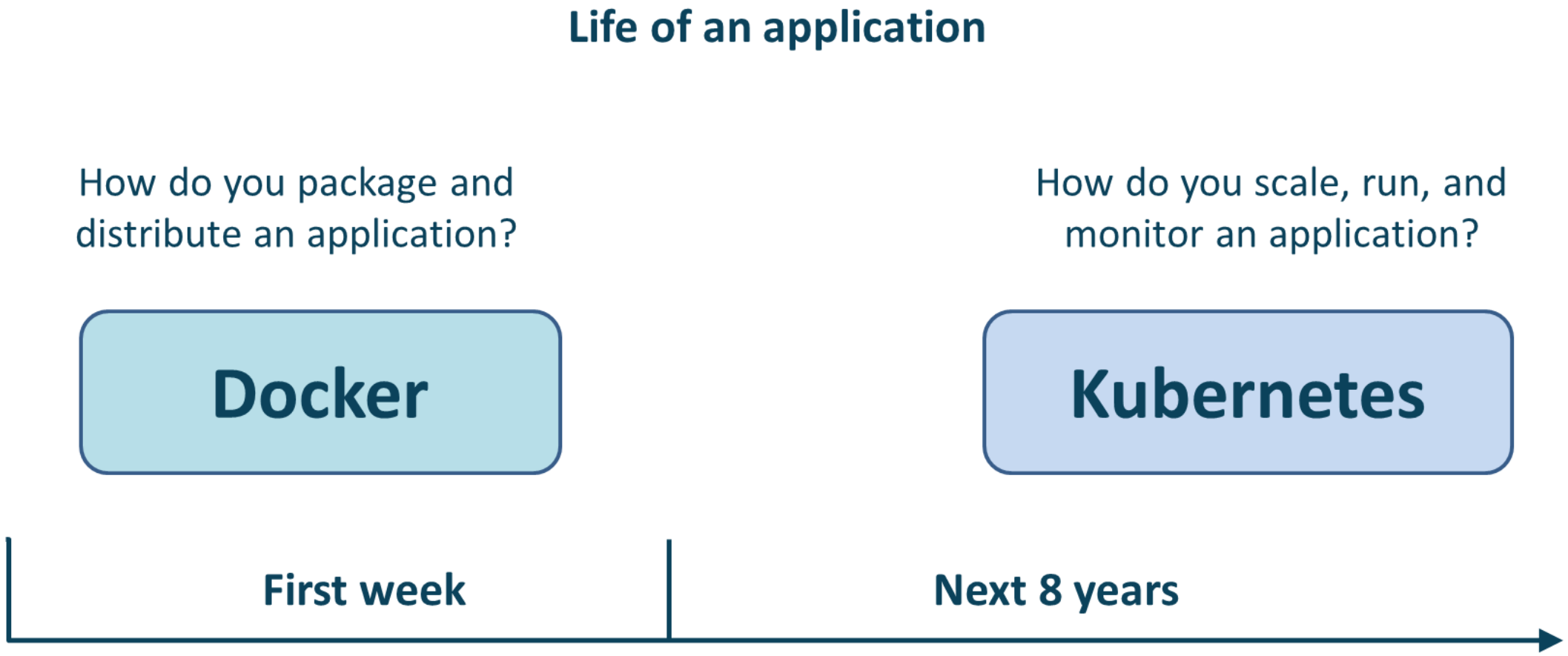
Docker

- Docker is a containerization platform
- The Docker Engine is the runtime that allows you to build and run containers
- Docker is currently the most popular container platform and over 30% of enterprises currently use Docker in their AWS environment

Kubernetes

- Kubernetes is an orchestrator for container platforms
- It is a comprehensive system for automating deployment, scheduling, and scaling of containerized applications
- It is the industry leader and supports many container tools such as Docker

Docker vs. Kubernetes



Serverless Architectures

- Enables the customer to move more responsibility to the provider, while enhancing agility and innovation
- Also known as Functions as a Service when running serverless code in a wide variety of use cases
- Customer can run container applications and services without having to consider underlying servers
- Eliminate infrastructure duties such as provisioning, patching, maintenance, and capacity management
- This solution can be used for nearly every type of application or back-end service and everything needed to run and scale an application with high availability is controlled for you by the CSP
- When building serverless applications, developers can focus on the core product or service as opposed to managing and operating servers or runtimes, either in the cloud or on-premise
- The reduced overhead empowers developers to get back time and energy that can be used on further delivery of reliable and scalable products and services in the cloud

Serverless Architectures

Serverless code

- Solutions like AWS Lambda and Azure Functions let you run small pieces of code called functions
- You do not need to deploy a server or application infrastructure
- Run code based on HTTP requests, predefined schedule, API call trigger, security event, manually, and much more

Serverless containers

- AWS Fargate is a serverless compute engine for containers that works with both Elastic Container Services and Kubernetes
- It eliminates the need to provision and manage servers, lets you stipulate and pay for resources per application, and enhances security through application isolation by design

Services Integration

- DevOps professionals, application developers, and systems architects must determine the optimal path for integrating cloud-hosted, SaaS, and on-premises applications and services
- Success is found in approaches that take full advantage of the value delivered by each integration instead of trying to maximize the value of investments in integration tools

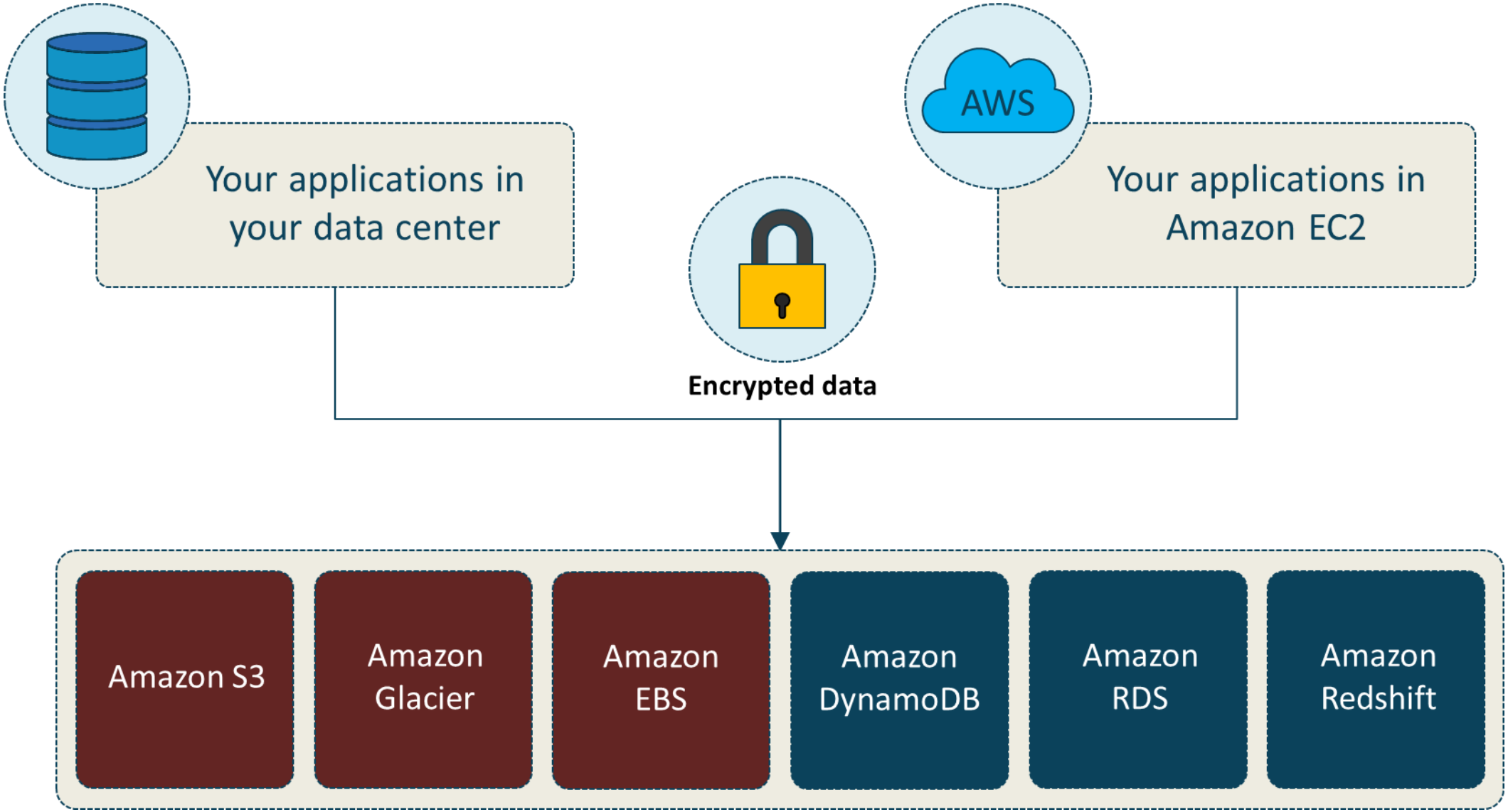
Services Integration Approaches

1. Integration platform software
2. Integration Platform as a Service (iPaaS)
3. SaaS vendor tooling
4. Custom coding
5. Function Platform as a Service (fPaaS)

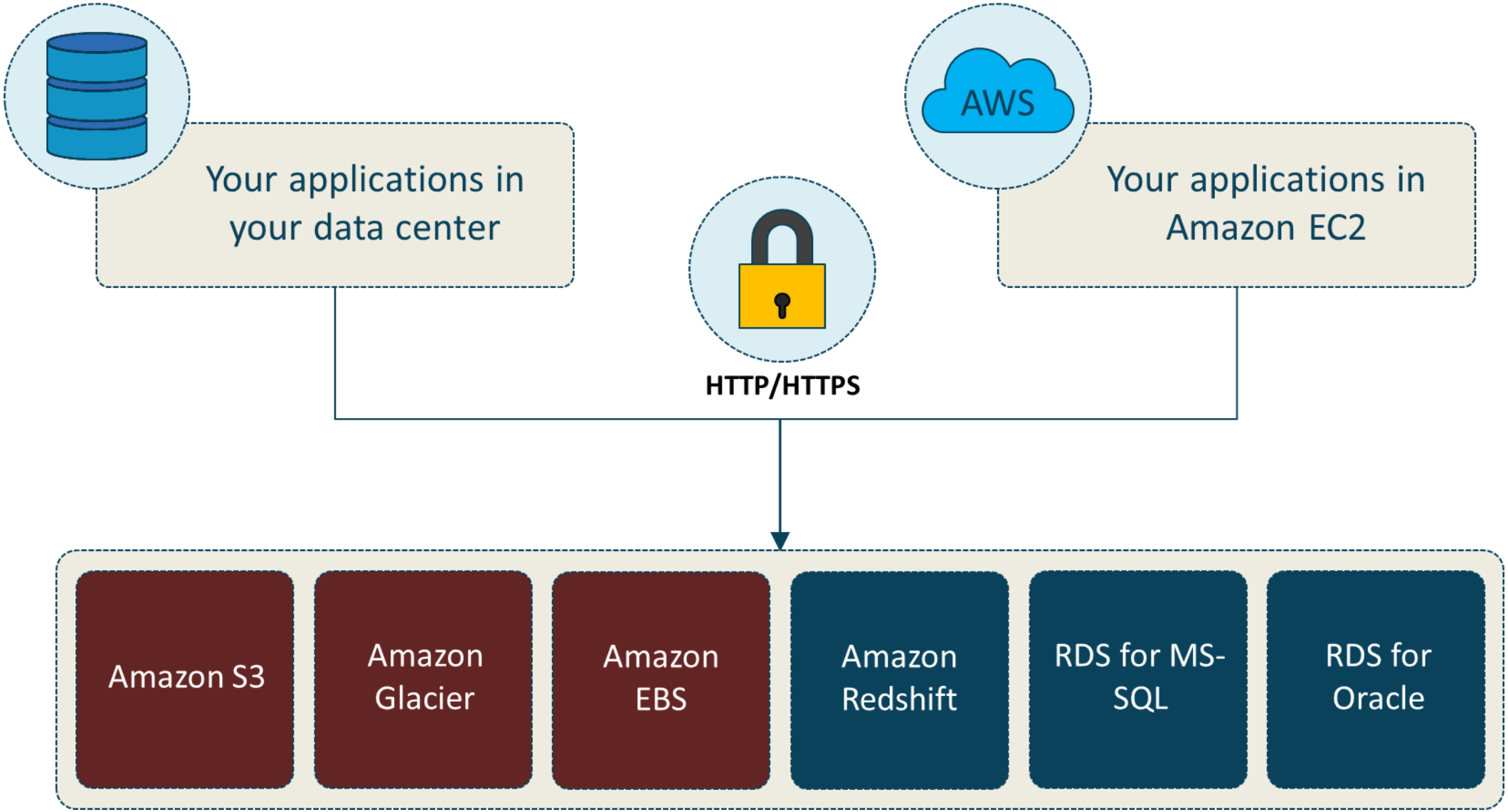
Cloud Storage Security

- Cloud storage includes block and object storage
- Cloud storage permissions are managed through an Identity and Access Management service, cloud-based AD instance, or often SSO using SAML 2.0
- You can also apply Public Access Policies, ACLs, and granular permissions policies to object storage (AWS S3) at the object container or bucket level
- Objects are often publicly accessed via URLs or API calls, which should be TLS protected and/or digitally signed
- The data at rest in cloud storage is provided by server-side encryption or through a managed key service of the service provider
- The disk drives and snapshots are often encrypted by default
- AES-128-GCM and AES-256-GCM are highly recommended

Client-side Encryption



Server-side Encryption



CSP High Availability and Fault Tolerance

High availability ensures continuous access and durability of cloud storage by placing redundant copies in availability zones or multiple regions

Fault tolerance is provided by the CSP infrastructure's storage area network and RAID arrays in highly secure data centers

Cloud Network Security

Begins with virtual network subnet design

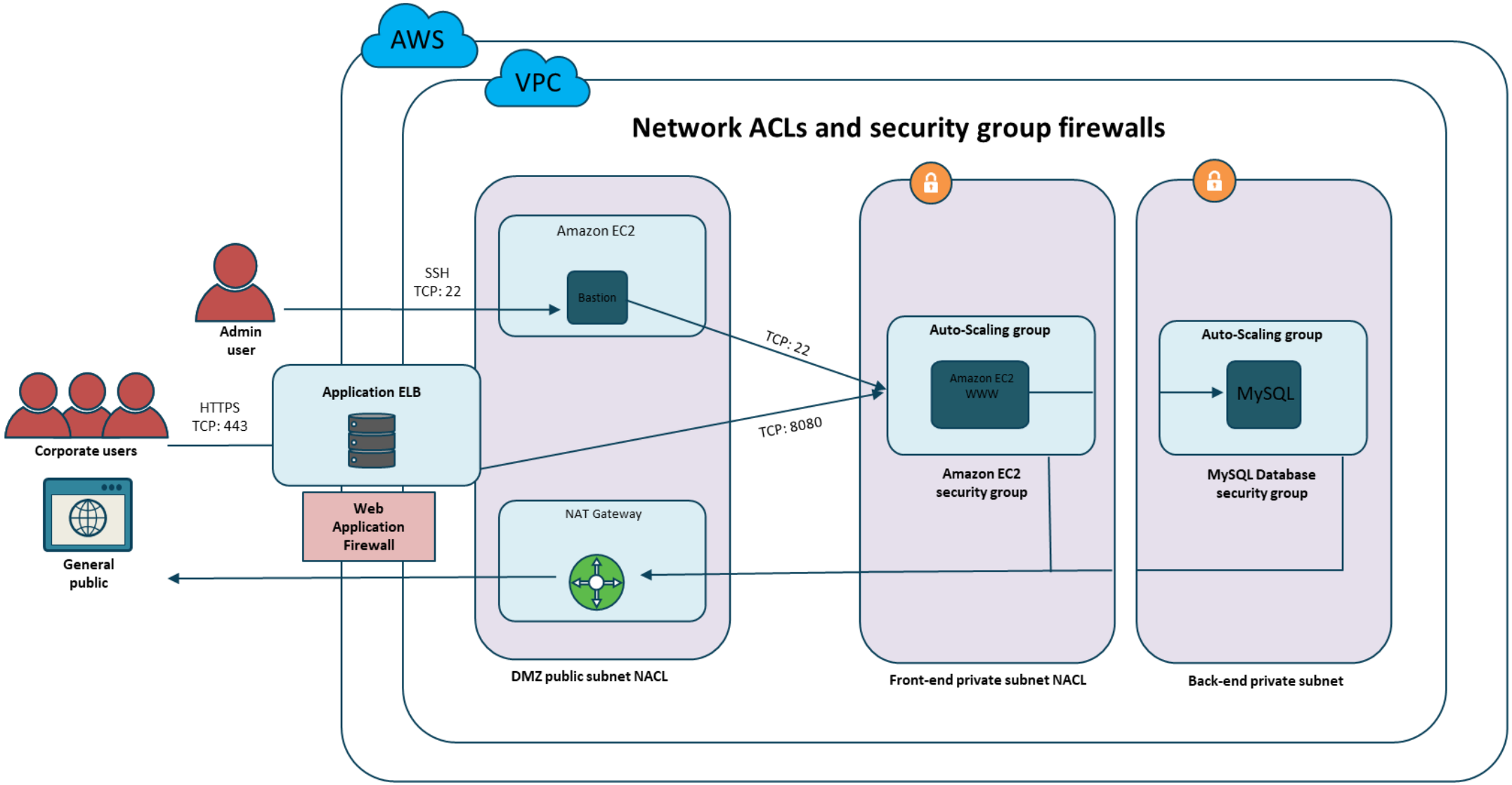
Must evaluate all connectivity options (gateways, endpoints, VPN)

Various Layer 3/4 static and stateless firewalls

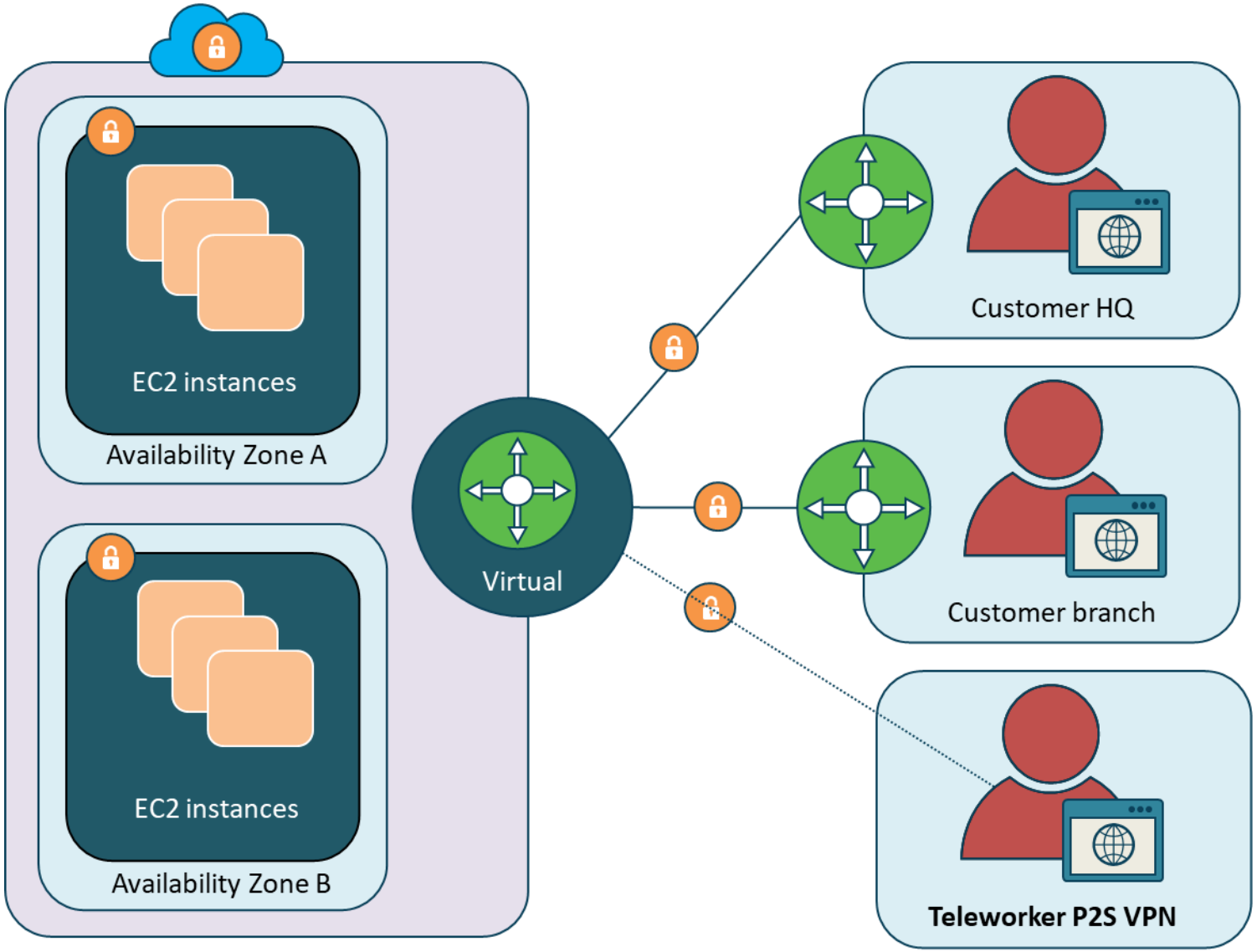
WAF deployment on load balancers, CDN distributions, API GWs

Managed threat modeling and DDoS solutions

Network Security Design Basics



Managed CSP VPNs



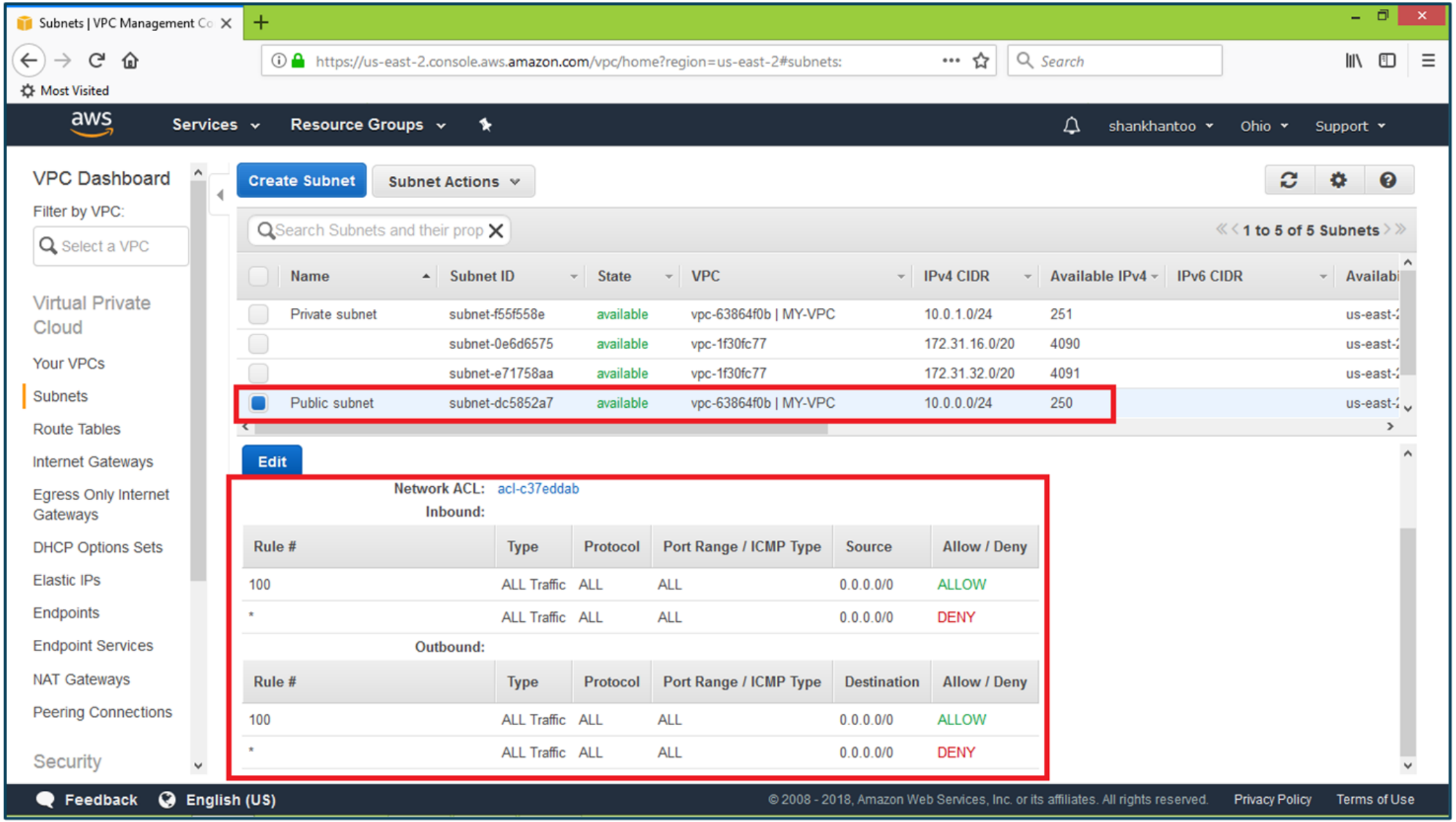
Cloud Compute Security

- Security group firewalls and VPC endpoint policies
- Dynamic resource allocation and visibility
- Container security by design
- Functions as a Service (AWS Lambda or Azure Functions)
- API gateway Web Application Firewall

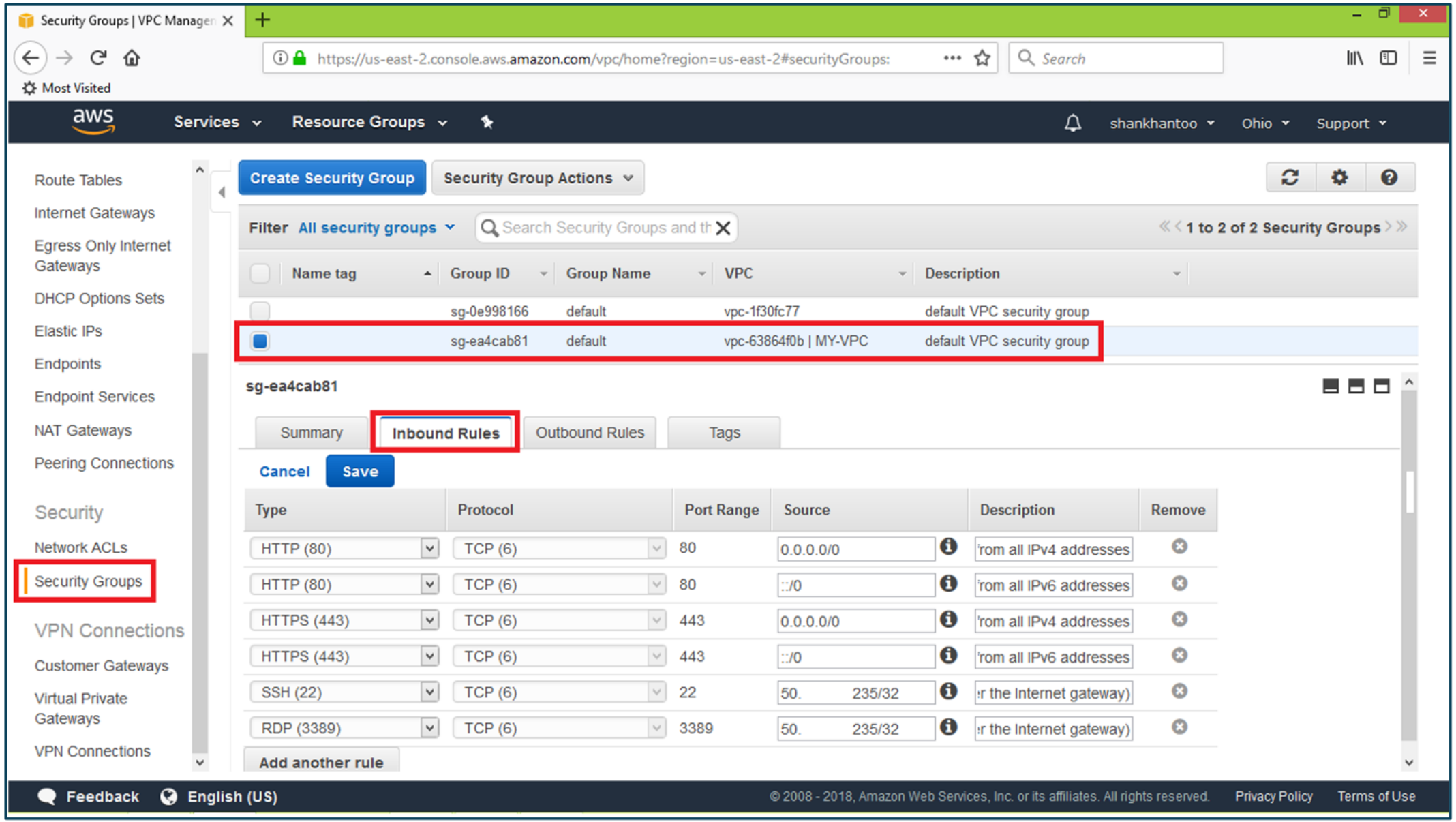
OWASP Top 10 IoT Vulnerabilities

1. Weak, guessable, or hardcoded passwords
2. Insecure network services
3. Insecure ecosystem interfaces
4. Lack of secure update mechanisms
5. Use of insecure or outdated components
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of physical hardening

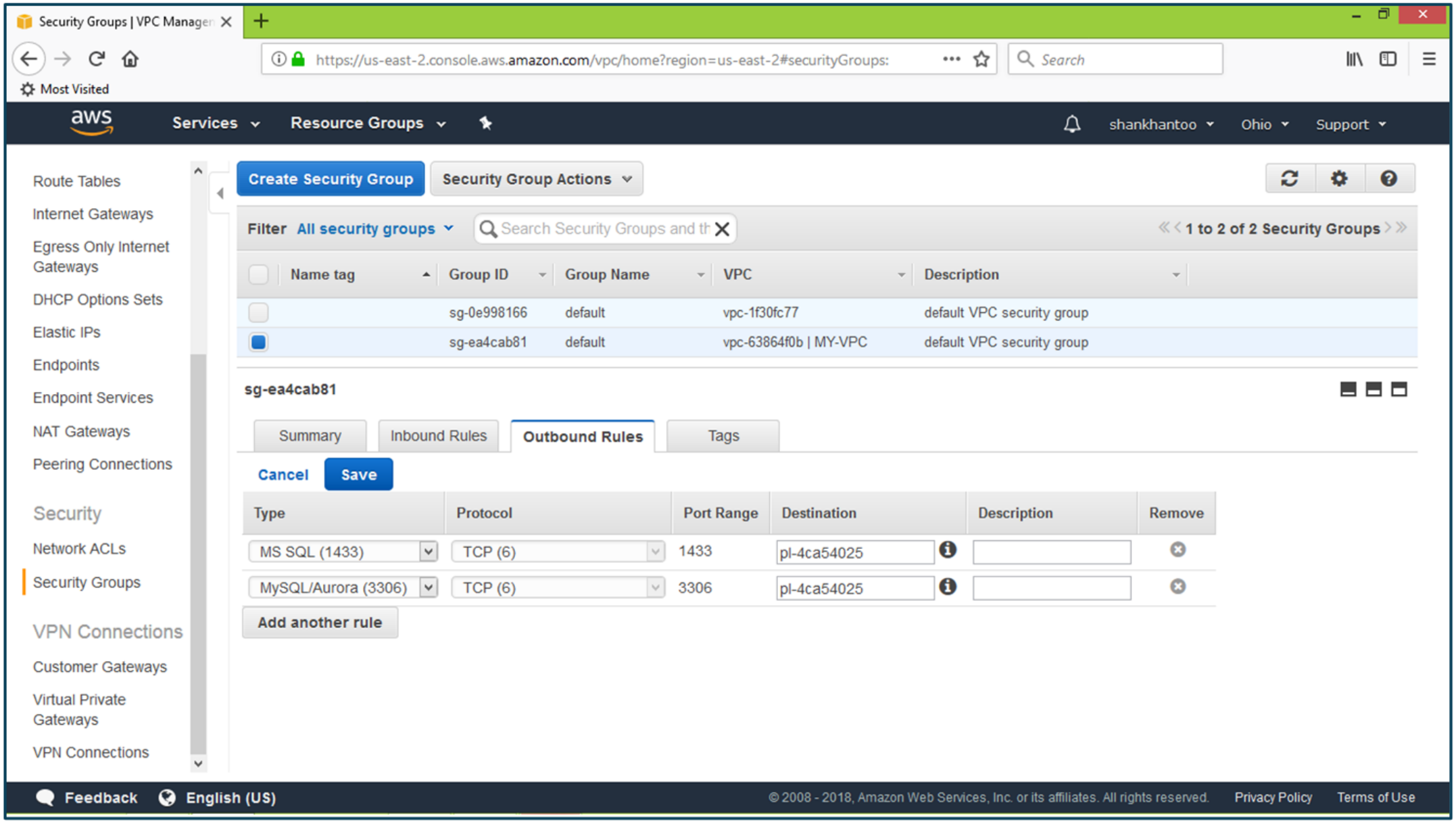
Network Access Control Lists



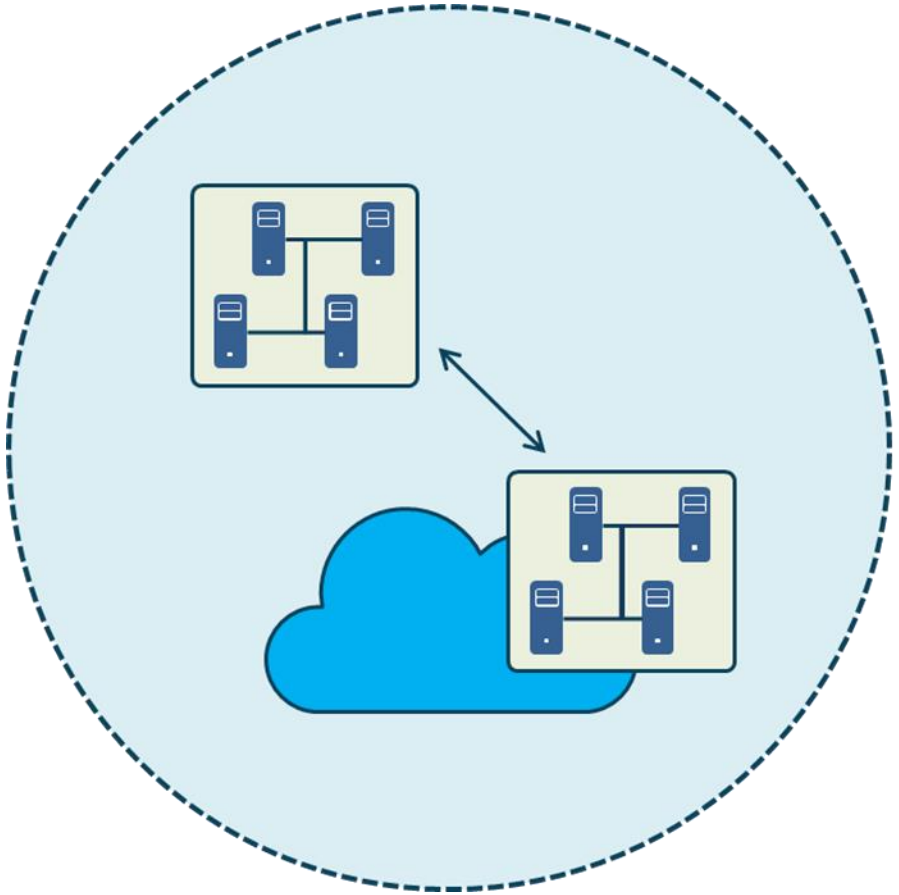
Stateful Firewalls in the Cloud



Stateful Firewalls in the Cloud



Cloud Access Security Brokers (CASB)



- Software service implemented between cloud customer and Software as a Service provider
- Could be on-premise or in-service provider cloud
- Acts as a gatekeeper to help enforce enterprise security policies while cloud resources are being accessed

Next Generation Secure Web Gateway (SWG)

- A next generation SWG protects your enterprise from the mounting volume and complexity of cloud-enabled threats and data theft
- It helps ensure that users are safely and securely utilizing cloud apps such as personal storage and the web according to AUP

SWG Features

Web content filtering with dynamic ratings

TLS decryption at cloud performance and scale

CASB and DLP services

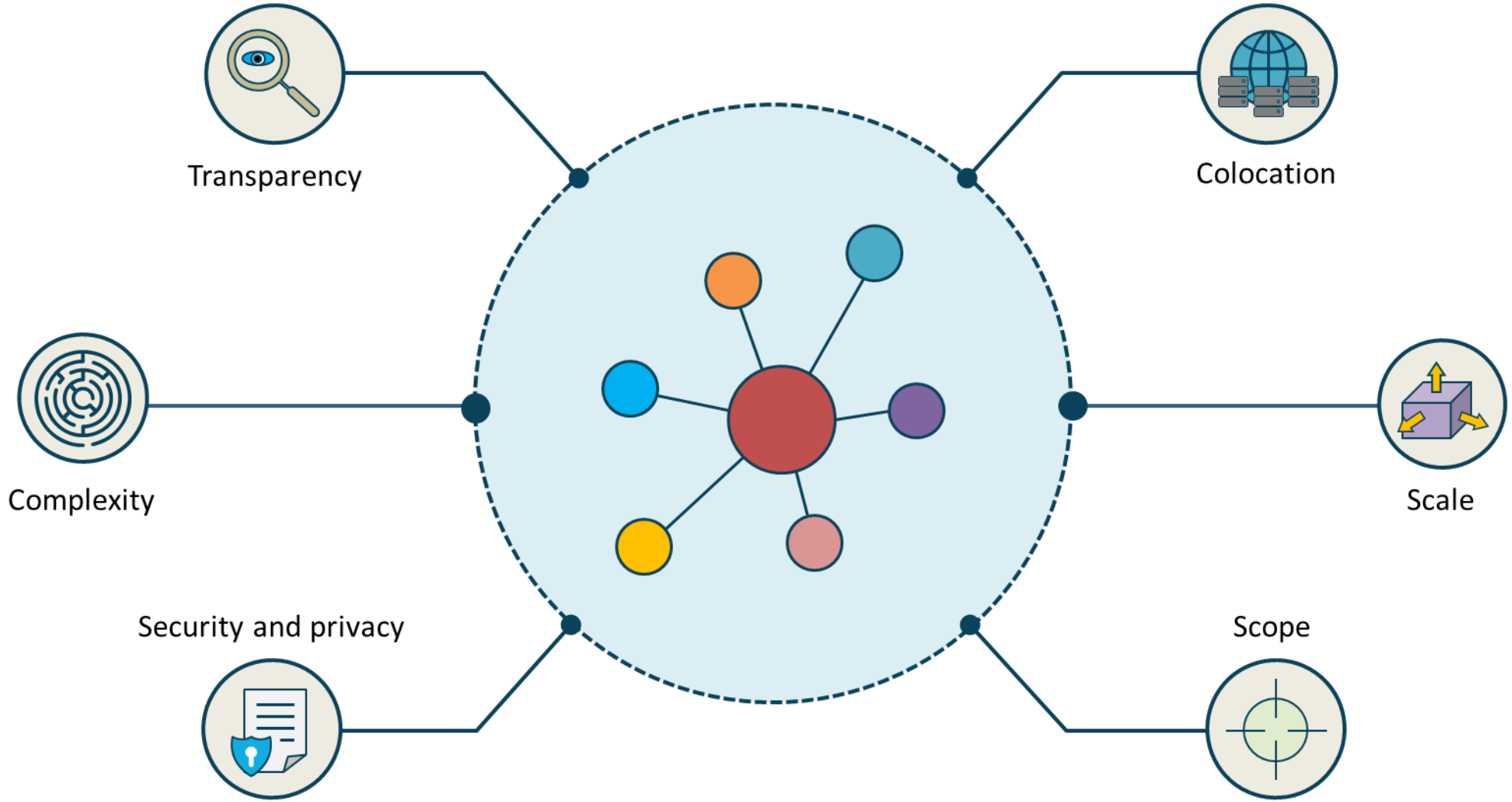
Advanced threat protection (ATP) including sandboxing

Visibility and rich metadata context for incident handling and reporting

Audit Processes and Methodologies for the Cloud

The biggest challenges for auditors are getting familiar with cloud computing terminology and having a working knowledge of a cloud system's composition and service delivery variations

Factors for Auditing the Cloud



Audit Processes and Methodologies for the Cloud

SAS

Statement on Auditing Standards No. 70: Service Organizations (SAS 70) was an authoritative auditing standard that was developed by the American Institute of Certified Public Accountants (AICPA)

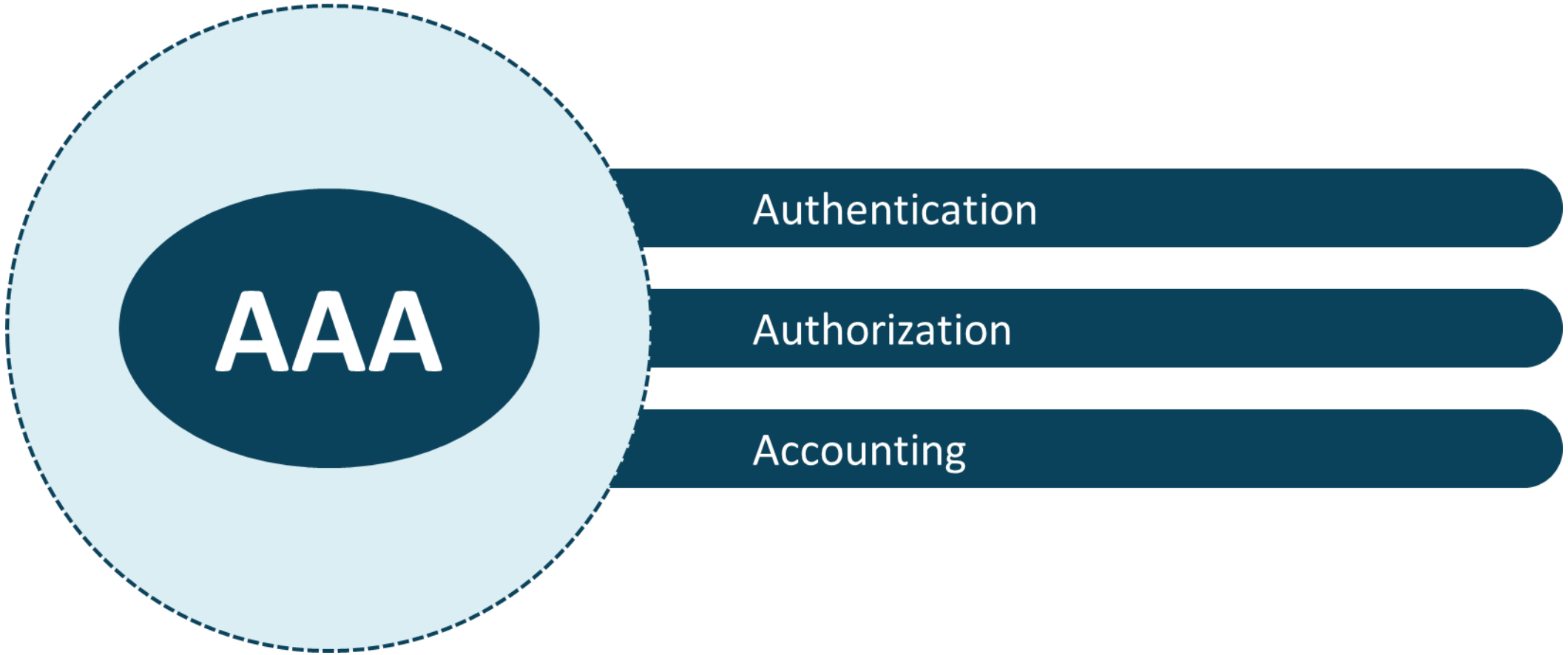
SSAE

Statement on Standards for Attestation Engagements no. 16 (SSAE 16) is an auditing standard for service organizations, superseding SAS 70 (Statement on Auditing Standards no. 70)

ISAE

International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization, was issued in December 2009 by the International Auditing and Assurance Standards Board (IAASB)

AAA Services



Authentication

Who or what are you?

- Authentication is the process of validating that an entity (user, application, or system) is who or what they claim to be
- Passwords are the most common authentication factor although they are rapidly being replaced or augmented with other factors
- Authentication can occur in multiple layers, where origin authentication comes first followed by more advanced forms of identification and authentication

Authorization

What can you access and what actions can you perform?

- Authorization is the process of granting an authenticated entity the permission to access a resource or perform a specific function
- This term is often referred to as access control, client privilege, or subject sensitivity level
- In a secure environment, although authorization is technically optional, it must always follow authentication

Accounting

Billing and chargeback

- Departments are responsible for staying within established budgets
- Accounting can provide visibility to senior management on costs
- Showback offers management of IT costs due to each department, without actually cross-charging those costs
- RADIUS and DIAMETER are popular IT accounting protocols

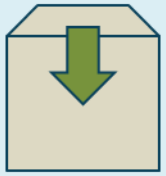
Auditing and reporting

- Accounting is most often used for auditing the usage of resources for security, operational, and forecasting reasons
- Auditing and reporting may be part of governance and adherence to regulations and mandates such as GDPR or HIPAA

Character Mode vs. Packet Mode

Character mode

- Character mode sends keystrokes to a networked device (often using RADIUS or TACACS+) through the TTY, vty, AUX, and CON ports
- It is for the purpose of configuration or query commands ON the device



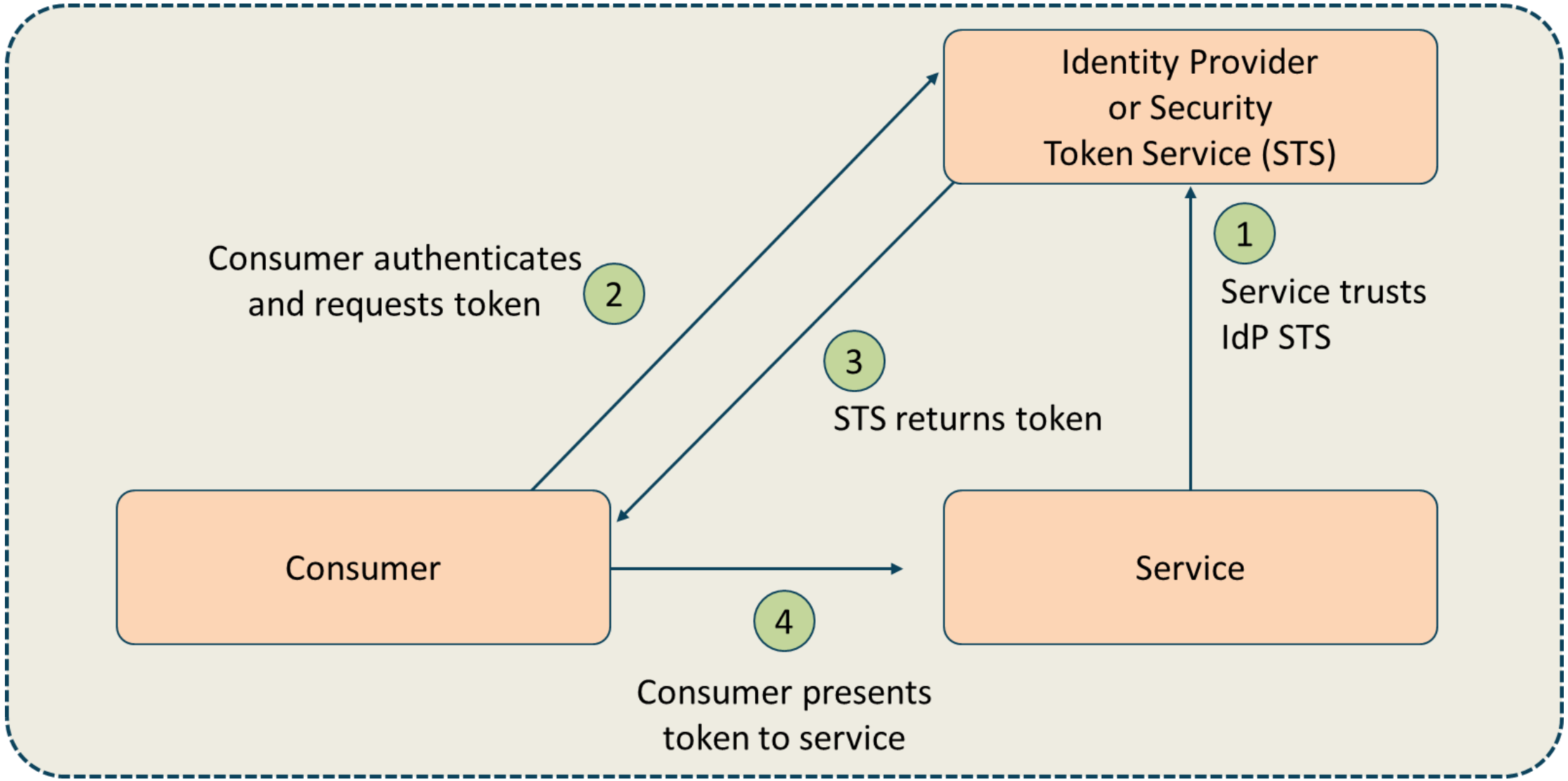
Packet mode

- Packet mode uses interface mode or a link protocol session to communicate with a device on the other side of the authenticating device
- It is also called network mode since AAA is being used to grant access to a server in a network

Identity Providers

- An identity provider is a system service that offers consumers (end users or devices) a single set of login credentials that authenticates and authorizes over multiple platforms, applications, networks, and sites
- A common scenario is when Active Directory is the IdP when logging into a cloud service provider
- A federated identity is a single, consistent profile that can be used across various services
- The IdP's role is to protect the federated identity's stored credentials and then provide them to different service providers (SPs) using translation and assertion services

Identity Providers



Identity Controls

Tokens

AWS Security Token Service enables you to request temporary, limited-privilege credentials for IAM or federated users

Assertions

An Azure shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources

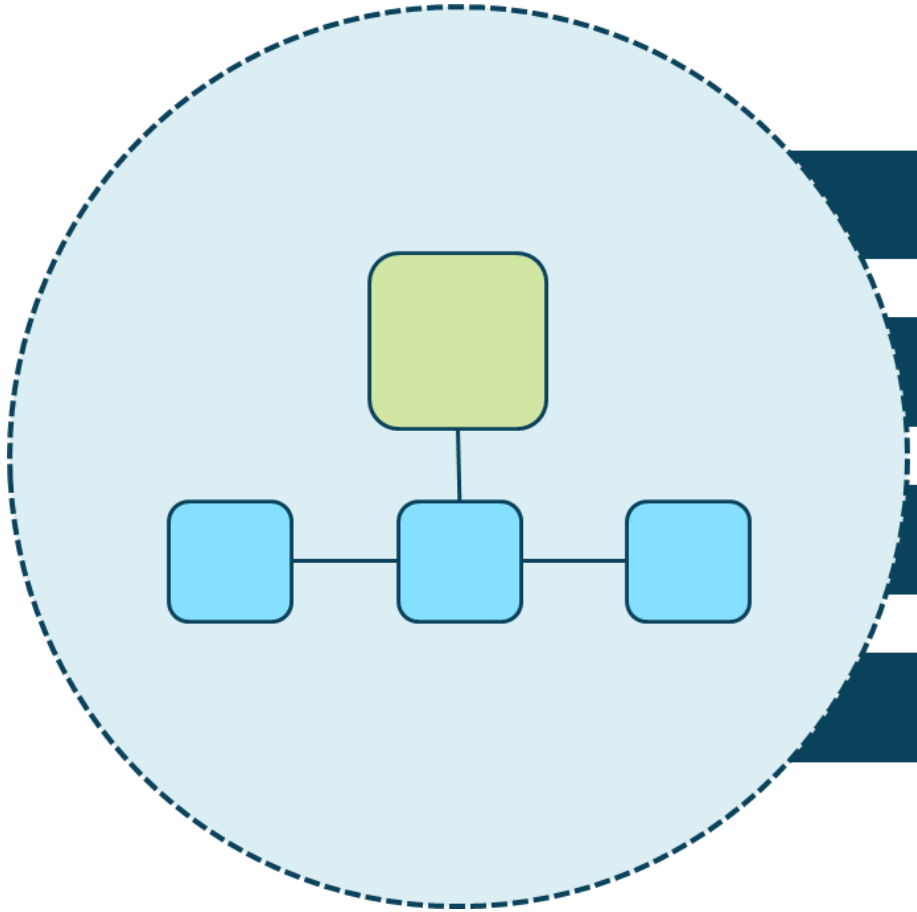
Certificates

X.509v3 digital certificates can be embedded in various smart cards, CAC cards, and OTP tokens

Directory Services

- A directory service is a vital AAA system for the SMB to large global enterprise
- It is a hierarchical structure that stores data about network objects
- Active Directory Domain Services (AD DS) is one of the world's most popular and it stores usernames, passwords, phone numbers, departments, assigned devices, and much more
- It also allows other authorized users and systems on the same network to access this information

Active Directory Components



- A set of rules called the schema
- A global catalog of all objects
- A query and indexing service
- A replication service for data distribution

Lightweight Directory Access Protocol (LDAP)

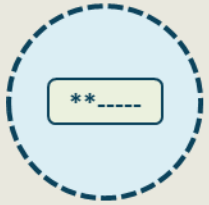
- LDAP is often used to provide access for management apps and browsers that need interactive read/write access to an X.500 or Active Directory service
- AAA systems can leverage existing user repositories for authentication
- For example, if a company uses LDAP, those systems can offer robust user repositories with sophisticated password management features to the AAA front end

Lightweight Directory Access Protocol (LDAP)

- LDAP is often used to provide access for management apps and browsers that need interactive read/write access to an X.500 or Active Directory service
- AAA systems can leverage existing user repositories for authentication
- For example, if a company uses LDAP, those systems can offer robust user repositories with sophisticated password management features to the AAA front end

Securing the Directory

Separate administrative accounts



Just in time local admin passwords

Implement Azure Advanced Threat Protection (ATP)

Enable MFA for all administrative accounts

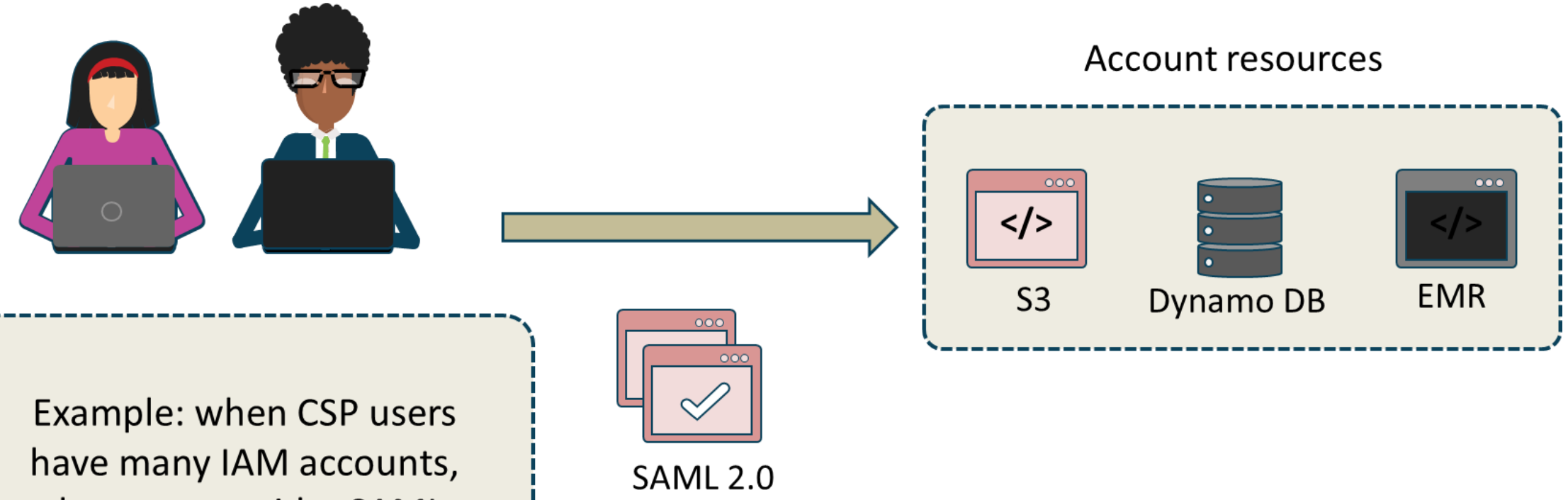
Secure all data in transit

Federation and Attestation

Trust relationships between domains

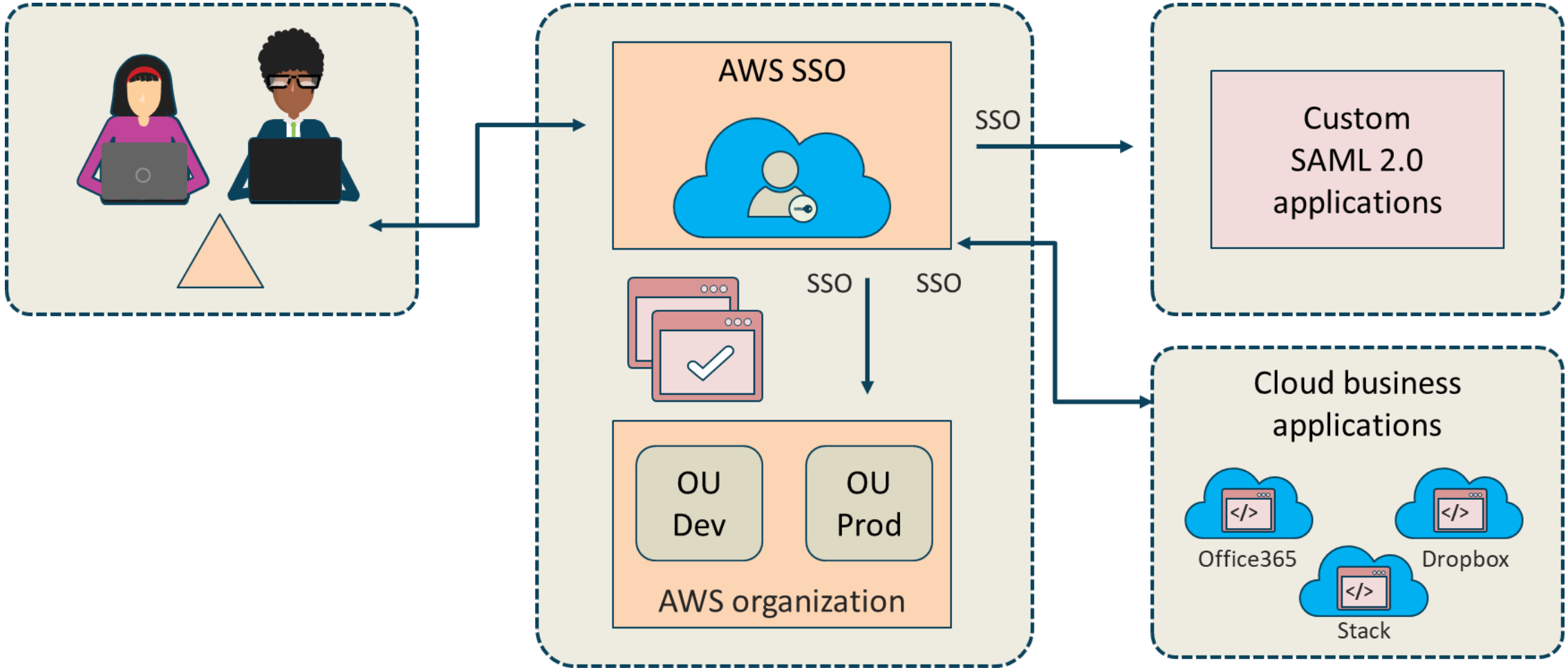
- When federation standards started to mature in the early 2000's, specifically SAML, universities and government organizations rapidly adopted trusted federation networks where identity information could easily flow between institutions
- Federation involves identity providers, trusted service providers, and attestation using assertions or tokens

Single Sign-on (SSO)



Example: when CSP users have many IAM accounts, they can consider SAML 2.0 federation to enable single-on (SSO)

AWS SSO


AWS SSO
SSO
Custom
SAML 2.0
applications
SSO
SSO
OU
Dev
OU
Prod
AWS organization
Cloud business
applications
Office365
Dropbox
Stack

AWS SSO

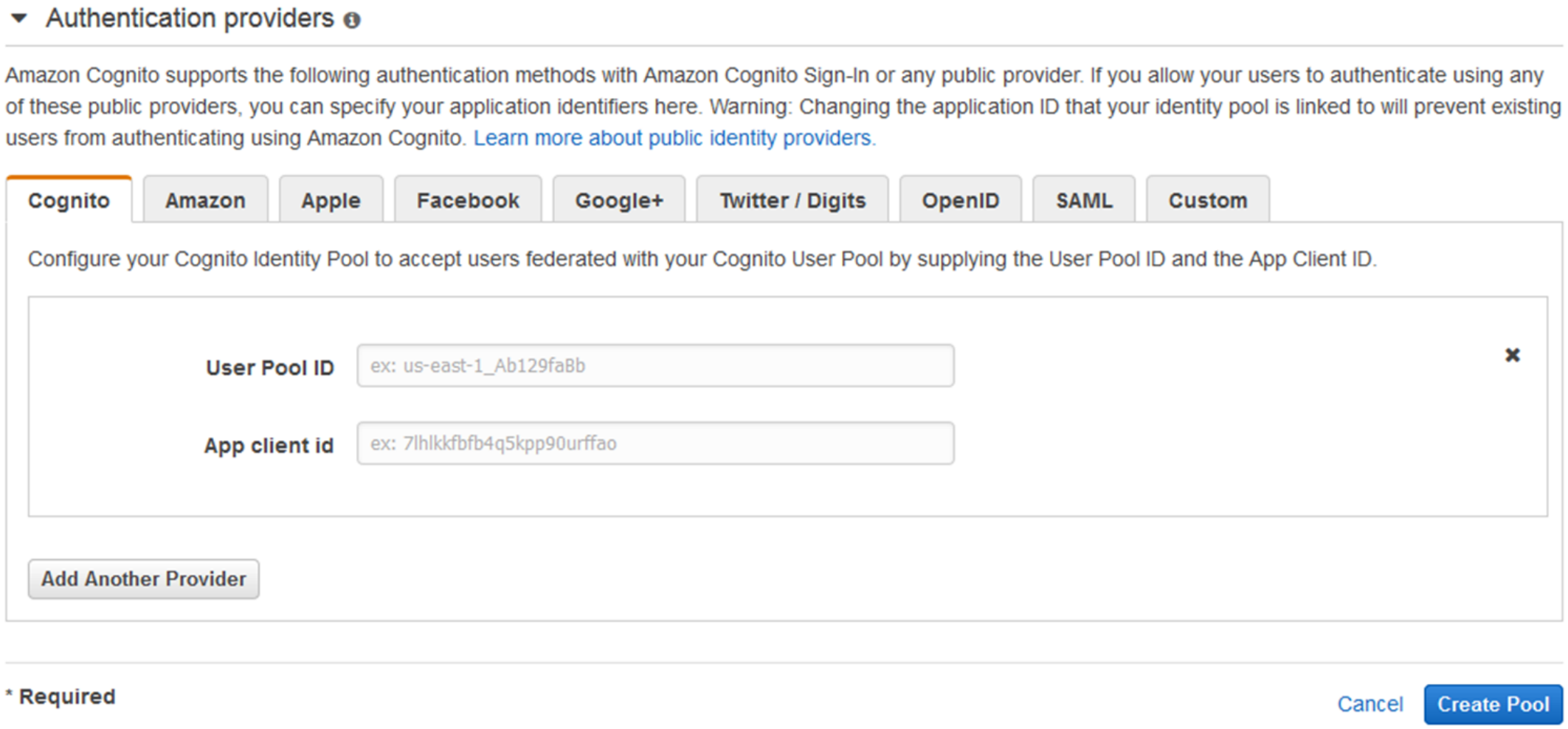
Enable AWS SSO

Connect corporate identities

Grant SSO access to your accounts and applications

Centrally manage user permissions

AWS Cognito


Authentication providers
Amazon Cognito supports the following authentication methods with Amazon Cognito Sign-In or any public provider. If you allow your users to authenticate using any of these public providers, you can specify your application identifiers here. Warning: Changing the application ID that your identity pool is linked to will prevent existing users from authenticating using Amazon Cognito. Learn more about public identity providers.
Cognito
Amazon
Apple
Facebook
Google+
Twitter / Digits
OpenID
SAML
Custom
Configure your Cognito Identity Pool to accept users federated with your Cognito User Pool by supplying the User Pool ID and the App Client ID.
User Pool ID
ex: us-east-1_Ab129faBb
App client id
ex: 7lhlkkfbfb4q5kpp90urffao
Add Another Provider
* Required
Cancel
Create Pool

Multifactor Authentication (MFA)

Uses at least two methods

- Something you **know** (password, passphrase, or PIN)
- Something you **have** (smart card, fob, token, CAC)
- Something you are (biometrics)
  - Attributes (ABAC)
    - Somewhere you are
    - Something you can do
    - Something you exhibit
    - Someone you know

Cloud vs. On-premise

Cloud Provider

- Concern is only at layer 3 and above
- Identity Access Management (IAM) and or SSO
- Programmatic or console access
- Shared responsibility based on level of managed service

On-premise

- Must include physical security and layer 2 protections
- More control over access model and frameworks
- More flexible protocols and solutions

Authentication Technologies

- Time-based one-time password (TOTP)
- HMAC-based one-time password (HOTP)
- Short message service (SMS)
- Token key
- Static codes
- Authentication applications
- Push notifications
- Phone calls

Smart Card Authentication

A form of 2-factor authentication

Users connect smart cards to their host computer

Software on the laptop interacts with keys or secrets

The information stored on the card authenticates user

Common Access Card (CAC) is used for active-duty military

Common Access Card (CAC)

- Expiration Date
- Federal Identifier
- Affiliation
- Service / Agency
- Color Indicator
- Pay Grade
- Rank
- Integrated Circuit Chip

Fingerprint Biometrics

One of the most common biometrics

- One of the most common biometrics since they vary from person to person and do not change over time
- Integrated into mobile devices and laptop computers using hardware and/or software
- A fingerprint scanner system has two functions
  - Gets an image of the finger
  - Determines whether the outline of ridges and valleys in the image matches the patterns in pre-scanned images

Facial recognition

Becoming the dominant form pre-pandemic

- One of the fastest growing mechanisms
- Commonly used to identify or verify an individual in still or video images
- The main applications of face recognition are in areas of security biometrics and human-to-computer interaction (including robotics)
- Main method for modeling facial images is Principal Component Analysis (PCA)

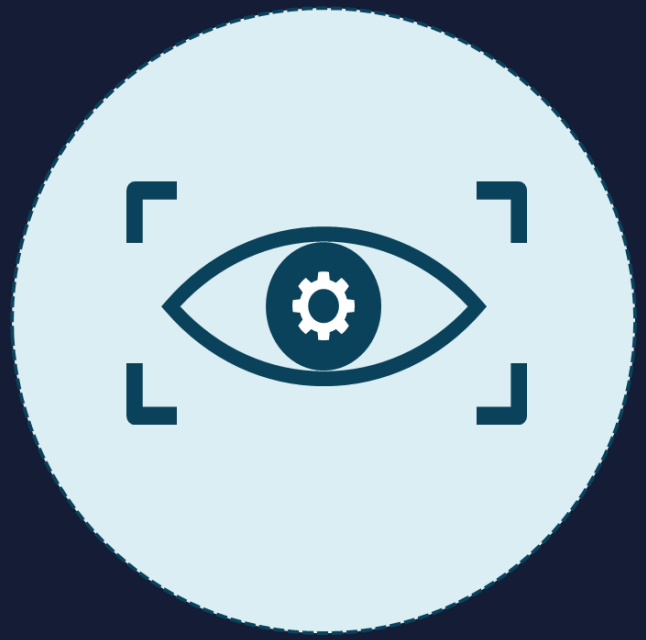
Iris Scans

Retina scanning is a method of ocular identification that is more invasive than iris scanning

- The iris is the thin, circular structure "color" part of the eye and controls the diameter and size of the pupils and therefore the amount of light reaching the retina
- Muscles attached to the iris expand or contract the pupil so the larger the pupil, the more light that can enter
- Unlike retina scanning, iris scanners use camera technology to get images of the intricate and detailed structures of the iris using delicate infrared illumination

Retinal Scans

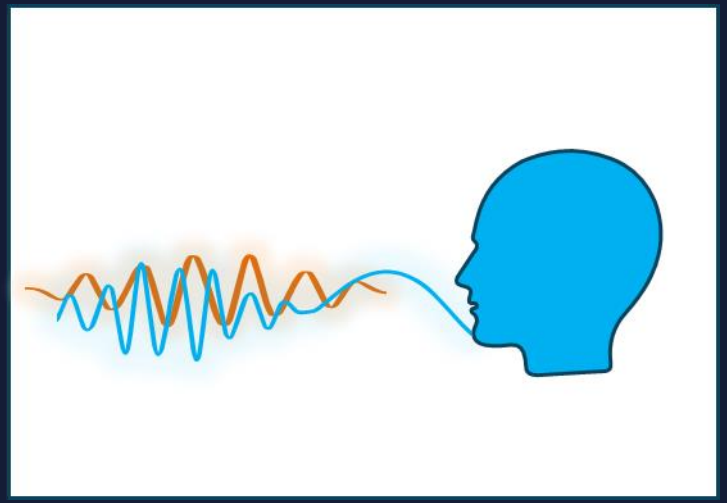
Retina scanning is a method of ocular identification that is more invasive than iris scanning



- The retina is a thin tissue composed of neural cells located in the back portion of the eye
- Due to the complex make-up of the capillaries, every person's retina is distinctive
- Scanner sends a beam of low-energy infrared light into an eye when user looks through the scanner's eyepiece
- Beam of light traces a standardized path on the retina and the pattern of variations are converted to code and stored in a database
- Retinal scanning is categorized as invasive since the eye must be very close to the eyepiece

Voice Recognition

There is a difference between speaker recognition and speech recognition



- There is a difference between speaker recognition and speech recognition
- "Voice recognition" can be used for both terms
- Speaker recognition leverages the aural aspects of speech that diverge among people
- Traits include human physical structure learned social communication patterns
- Voice recognition is classified as a "behavioral biometric"

Vein and Gait Analysis

These are more esoteric forms of non-invasive identification

- Vein pattern recognition comes in three variants
  - Palm vein pattern recognition
  - Finger vein pattern recognition
  - Retina vein pattern recognition
- Gait biometrics identify people based on their unique walking pattern
  - It has the advantage of being unobtrusive, in that it requires no subject contact.

False Acceptance Rate (FAR)

- False Acceptance Rate (FAR) measures the probability that the biometric system will incorrectly accept an access effort by an unauthorized user
- A system's FAR is often specified as the ratio of the number of false acceptances divided by the amount of authentication attempts

False Rejection Rate (FRR)

- The False Rejection Rate is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input with a template

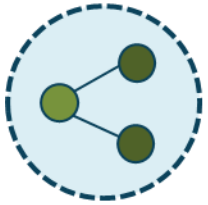
Crossover Error Rate (CER)

- The crossover error rate (CER) is the value of FAR and FRR when the sensitivity is setup so that FAR and FRR are the same
- An excellent metric for quantitative comparison of differing biometrics

Account Types

User accounts

Guest and generic accounts



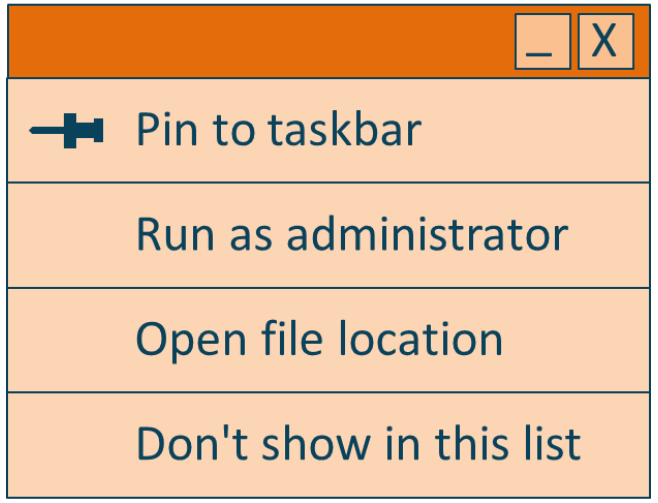
Shared accounts and credentials

Service and application accounts

Privileged and emergency (fallback) accounts

Account Types

- A big challenge is overprivileged users
- The least privilege and dual operator principles should be used
- There may be a lack of logging, auditing, and reporting
- Use separate account for admin tasks (Run as…)
- Use centralized secure systems
  and directory services whenever possible
- Assess vulnerabilities from privileged insiders



Advanced Account Policies

Driven by new technology like IoT

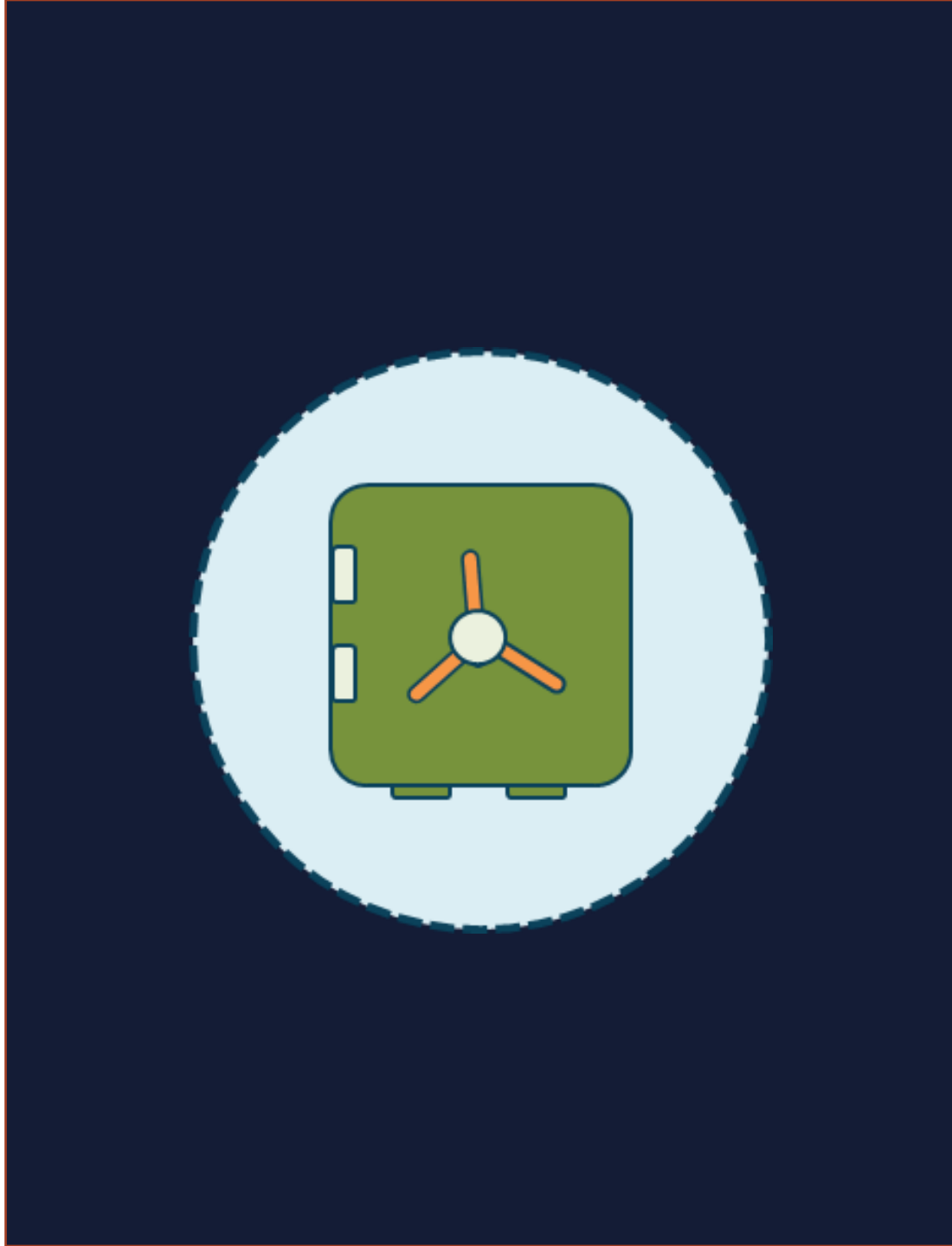
- Geofencing and geolocation services allow IT to physically track mobile devices
- Geolocation is a point on a map whereas geofencing is an area on the map
- Administrators can use geolocation to find a lost or stolen device and geofencing can determine when a device moves in and out of a certain (secure) area
- Mobile device management (MDM) systems have added these features for the enterprise
  - MDM can also be used to apply time-of-day restrictions on provisioned devices
- GPS Tags is an effective and easy-to-use app that can perform as a personal GPS tracker on your Android-based smartphone, tablet, or other mobile device

Password Key Management

- Key management is the main vulnerability to cryptosystems and credentials
- If passwords must still be used, the policies should be strictly enforced
- AUP sections on password storage and clean desk should be clear

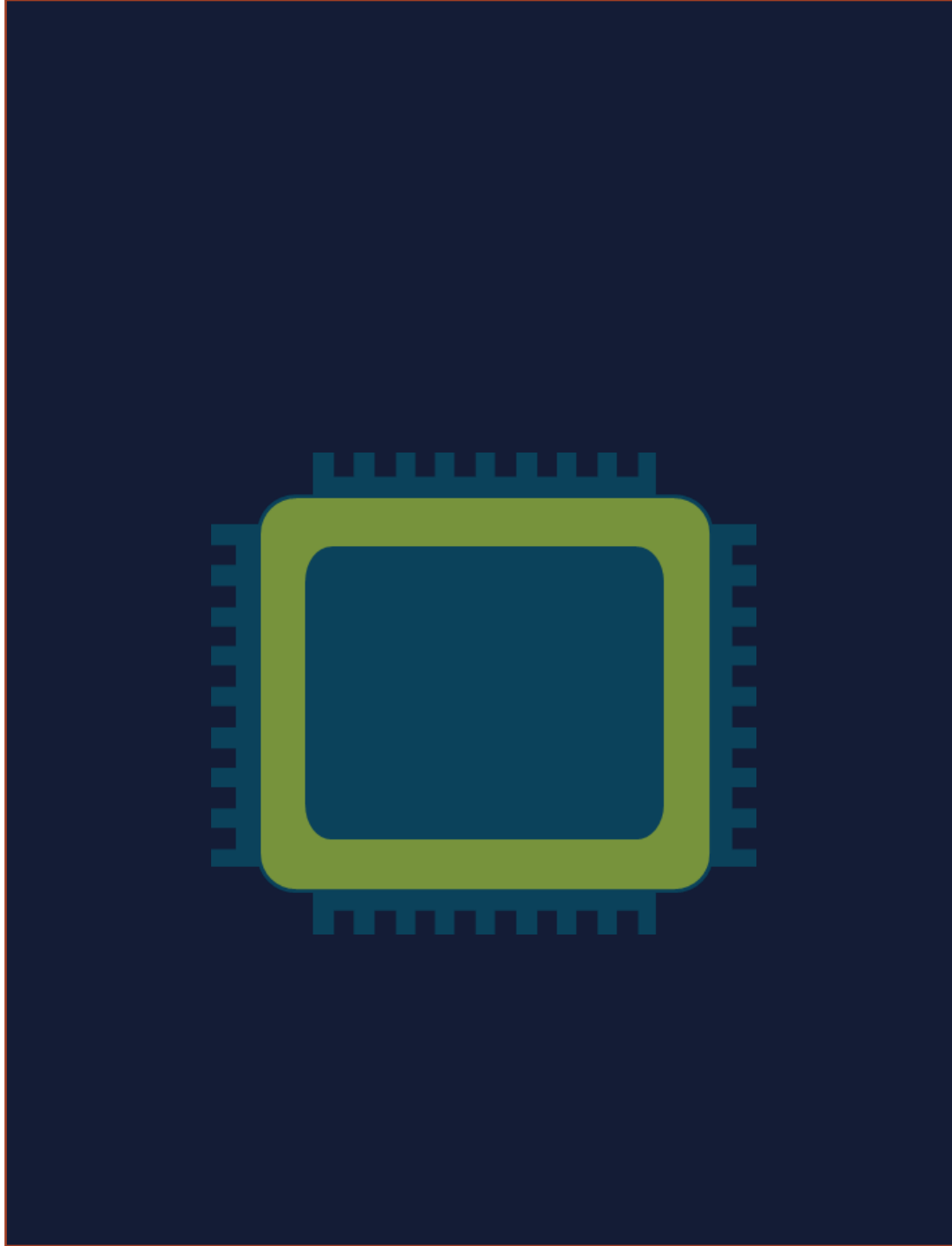
Password Vaults

- Password vaults are also known as password managers (Dashlane, LastPass, 1Password)
- Password vaults are also enterprise solutions that facilitate credential storage and single sign-on from desktops, smartphones, and tablets
- They can be a standalone unified directory or use other directory protocols like OpenLDAP

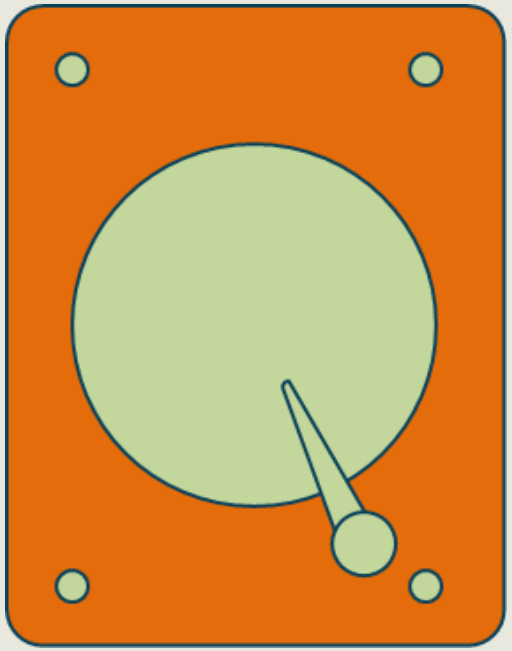


Trusted Platform Module (TPM)

- TPM is a tamper-resistant security chip installed on the device or built into PCs, tablets, and phones
- It stores the passwords, certificates, and encryption keys needed to authenticate the platform
- TPM provides the platform:
  - Integrity (ensures system has not been altered at a low level)
  - Authentication (ensures system is in fact the correct system)
  - Privacy (ensures system is protected from prying eyes)

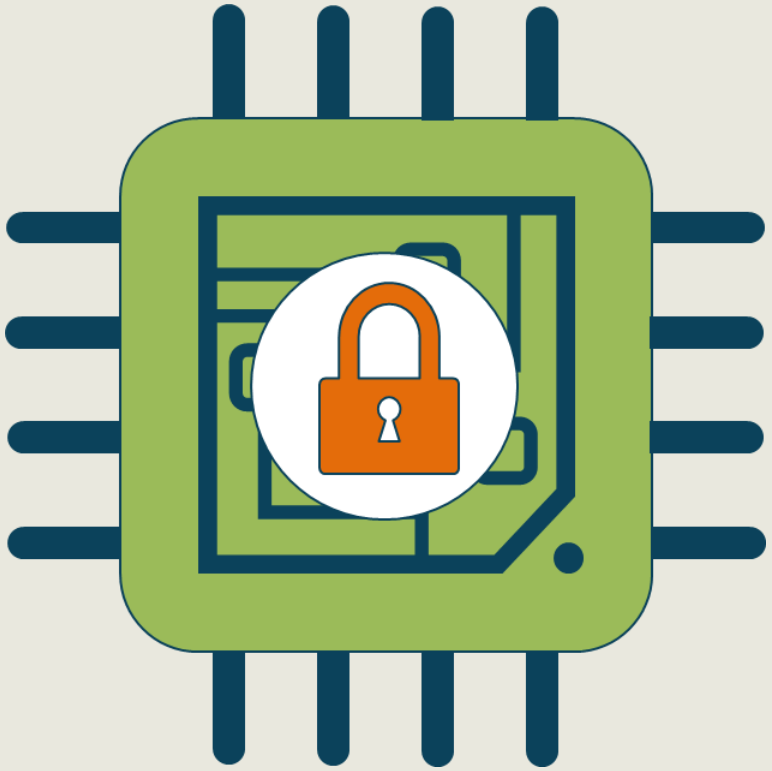


Self-encrypting Drives (SED)



- Also called full-disk encryption (FDE)
- All contents on the drive are constantly encrypted (including keys)
  - Encrypts data as written, decrypts data as read
- Invisible to the end user and cannot be turned off
- Less susceptible to threats when compared with software-based encryption
- SED/FDE provides:
  - Pre-boot authentication, endpoint security, and device authentication
  - Encryption, key management, network access control, and policy compliance

Hardware Security Module (HSM)



- Hardened, tamper-resistant dedicated appliance or module in a PC/server
  - HSMs can be physical or virtualized
- Responsibilities include:
  - Managing, processing, generating, and storing keys
  - Verifying digital certificates
  - SSL connection accelerator
  - Encrypting sensitive data
  - Verifying the integrity of stored data

Knowledge-based Authentication (KBA)

Allows users to choose security questions and answers

Goal is to prove someone is the exact person

Based on several pieces of info that only that user could have

Static or dynamic sophisticated solutions

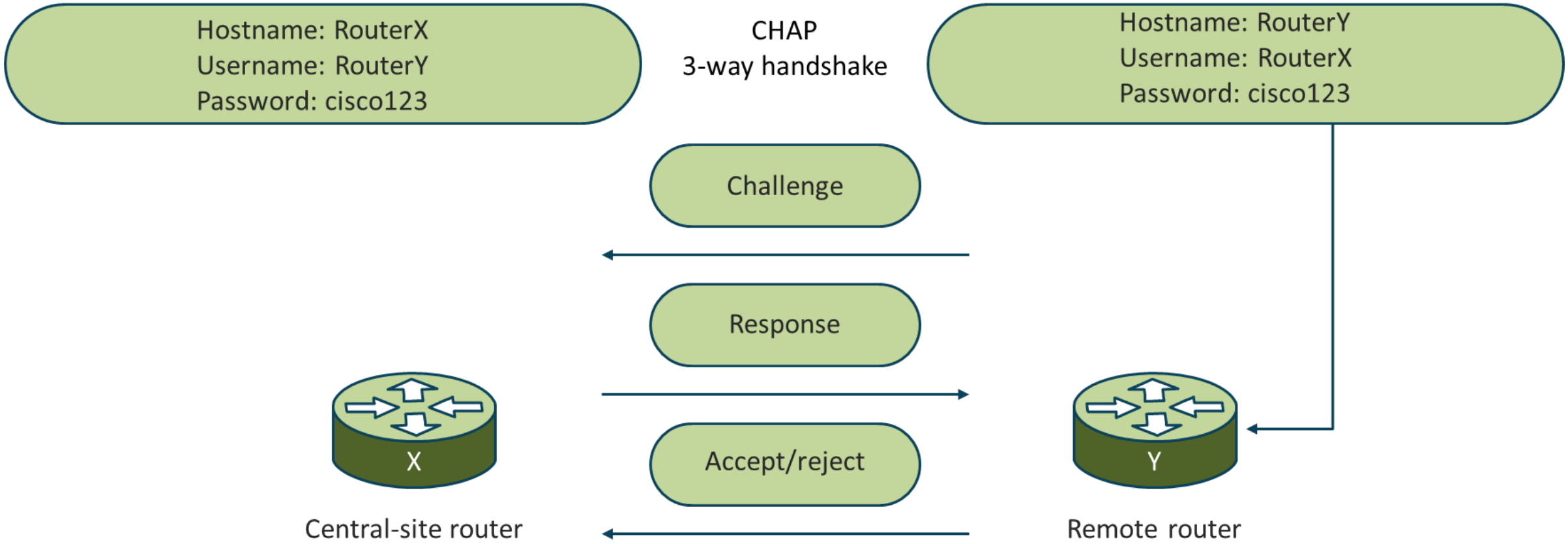
Can be combined with MFA and biometrics

MS-CHAPv2

Designed from the original PAP and CHAP protocols

- Microsoft's most common iteration of the original Challenge Authentication Protocol (CHAP)
- It secures PPP traffic by encapsulating it a PPTP tunnel
- The PPP payload is encrypted using MSCHAP, and the encryption keys are generated during the user authentication process
- After encryption, encapsulation takes place in PPP and the frame is encapsulated with Generic Routing Encapsulation (GRE) and an IP header

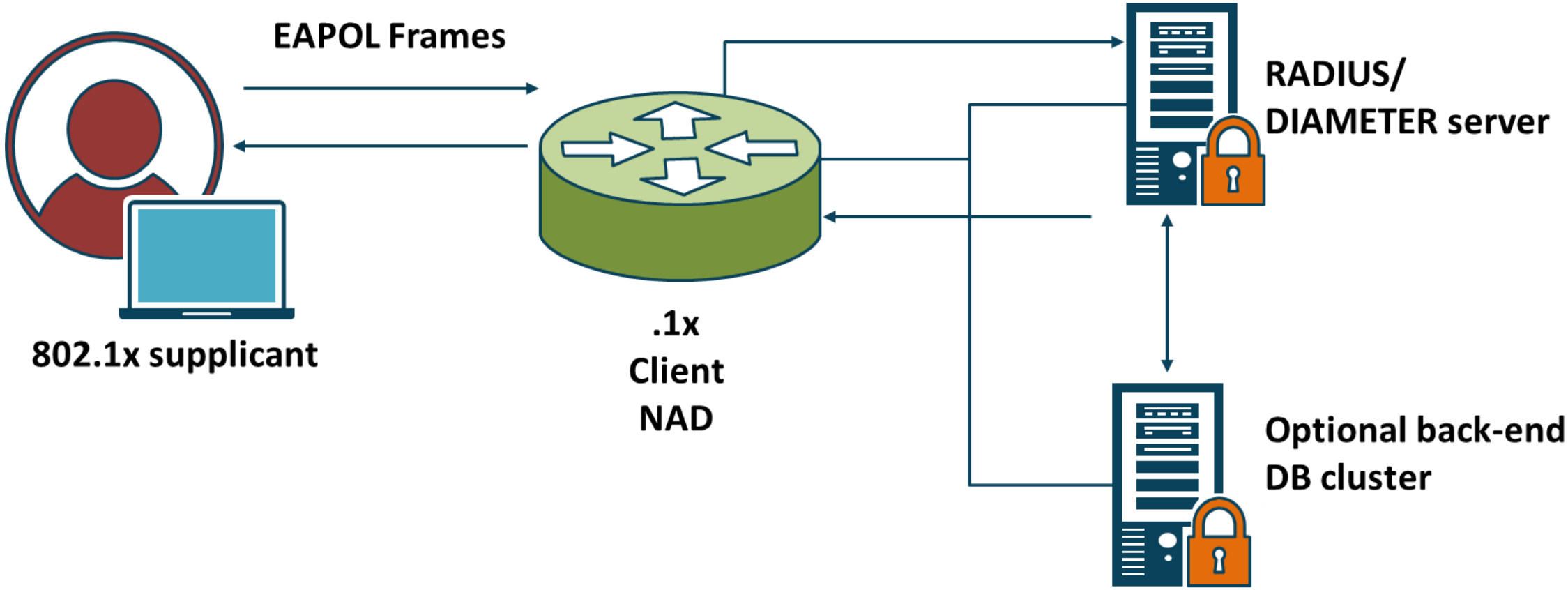
MS-CHAPv2


Hostname: RouterX
Username: RouterY
Password: cisco123
CHAP
3-way handshake
Hostname: RouterY
Username: RouterX
Password: cisco123
Challenge
Response
Accept/reject
X
Y
Central-site router
Remote router

IEEE 802.1X (PNAC)

- 802.1X is an ongoing extension of the original PPP protocols, also known as port-based network access control (PNAC)
- It is commonly used by AAA and identity services in wired and wireless network environments

IEEE 802.1X (PNAC)



IEEE 802.1X EAP Options

Extensible Authentication Protocol (EAP)

Protected EAP (PEAP)

EAP-FAST (Cisco)

EAP-TLS

EAP-TTLS

EAP Comparisons

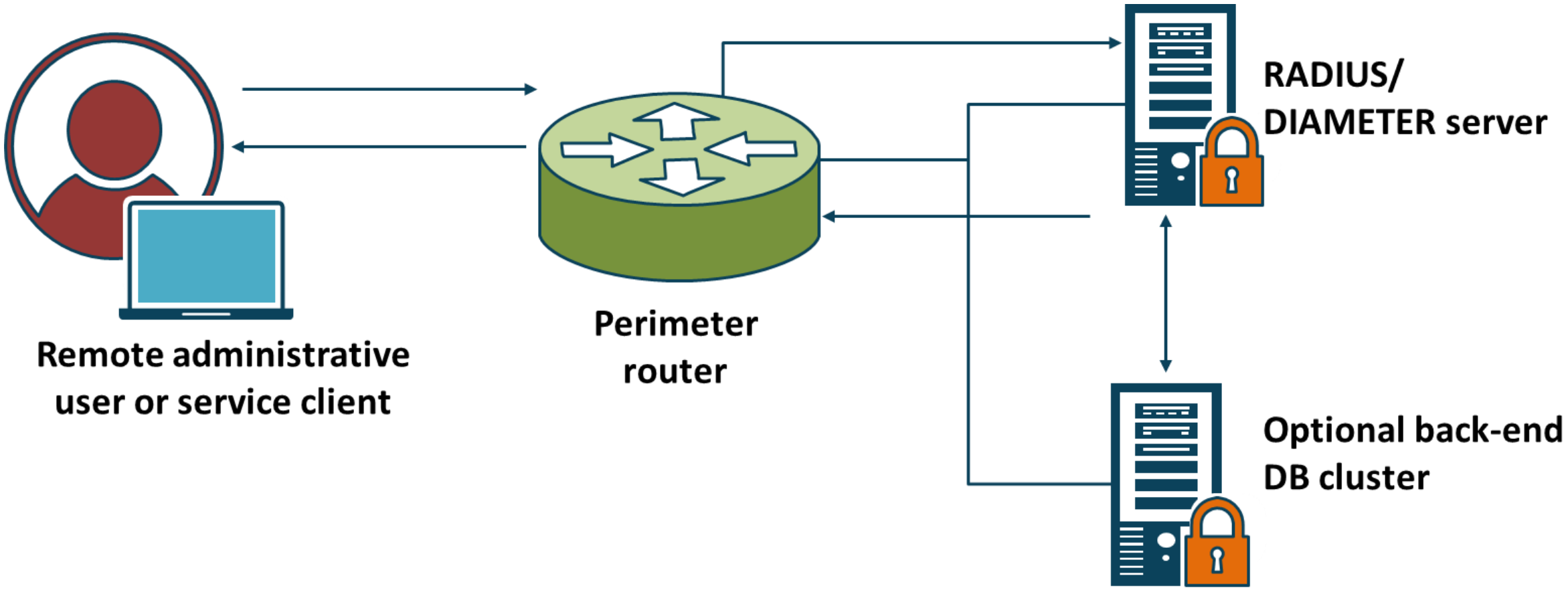
802.1x EAP types feature/benefit	MD5 --- Message Digest 5	TLS --- Transport Level Security	TTLS --- Tunneled Transport Level security	PEAP --- Protected Transport Level Security	FAST --- Flexible Authentication via Secure Tunneling
Client-side certificate required	No	Yes	No	No	No (PAC)
Server-side certificate required	No	Yes	No	Yes	No (PAC)
WEP key management	No	Yes	Yes	Yes	Yes
Rogue AP detection	No	No	No	No	Yes
Provider	MS	MS	Funk	MS	Cisco
Authentication attributes	One way	Mutual	Mutual	Mutual	Mutual
Development difficulty	Easy	Difficult (because of client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi security	Poor	Very high	High	High	High

RADIUS

- Remote Authentication Dial-In User Service
- Widely deployed client-server protocol and software that enables a remote access server (RAS) to communicate with a central server to authenticate dial-in users and authorize their access to systems
- Uses a client-server model and transactions use a shared secret between the client and the RADIUS server for authentication
  - The shared secrets are never sent over the network and only the password is encrypted
- Officially uses UDP ports 1812 (authentication) and 1813 (accounting)

  Earlier implementations used UDP ports 1645 and 1646
- Often preferred for its robust integrated accounting features

RADIUS


RADIUS/
DIAMETER server
Perimeter
router
Remote administrative
user or service client
Optional back-end
DB cluster

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

Shibboleth

It connects users to both interorganizational and intraorganizational applications and services

Empowers sites to make well-informed authorization choices for discrete access to protected online resources while maintaining user privacy

Is free, open source, and popular with universities and public service organizations

Kerberos

SSO authentication using a secret key cryptosystem

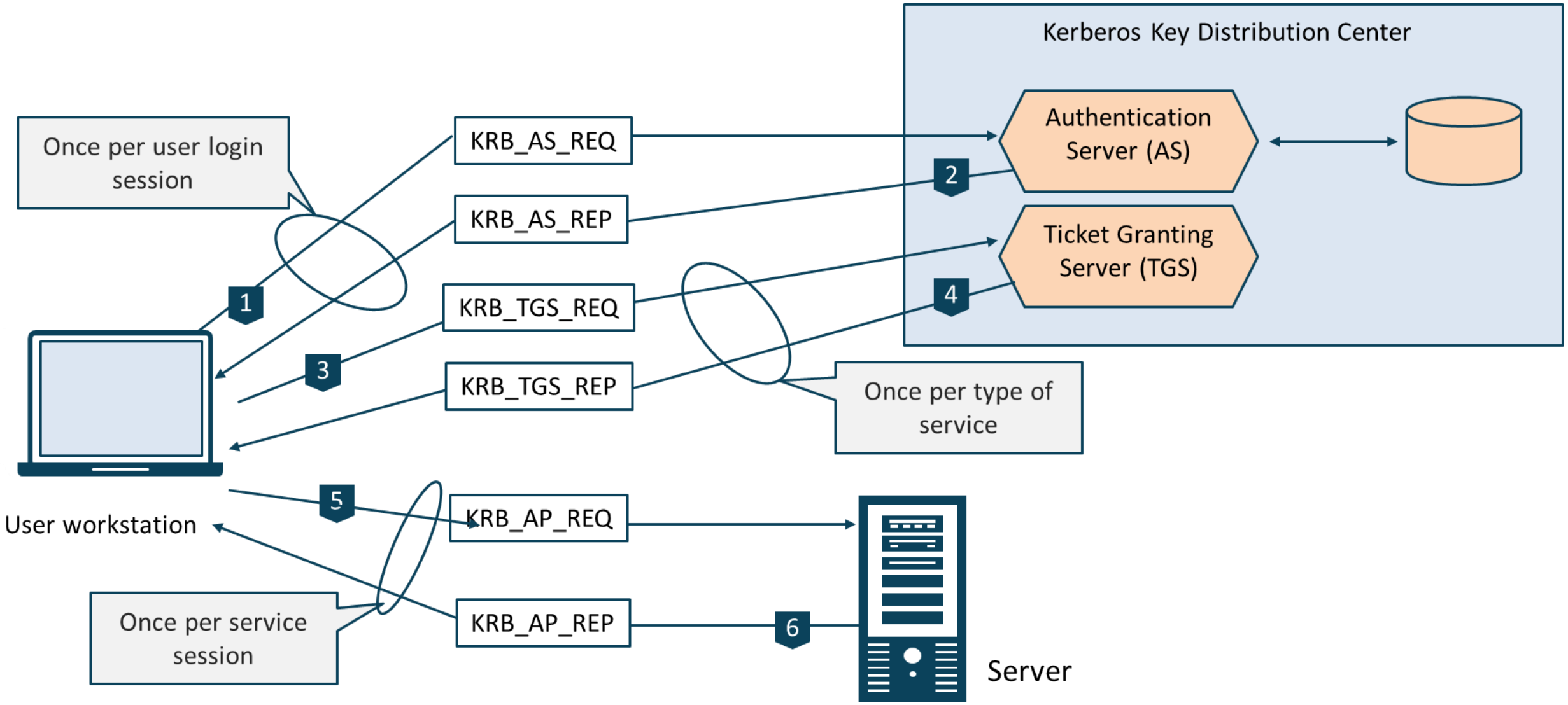
Uses a ticket for the assertion or token

Performs mutual authentication

All communications can be encrypted

Depends on a trusted 3rd party called a Key Distribution Center (KDC)

Kerberos


Kerberos Key Distribution Center
Authentication Server (AS)
Ticket Granting Server (TGS)
Once per user login session
KRB_AS_REQ
KRB_AS_REP
KRB_TGS_REQ
KRB_TGS_REP
1
2
3
4
Once per type of service
User workstation
5
KRB_AP_REQ
KRB_AP_REP
6
Once per service session
Server

Discretionary Access Control (DAC)

Common in directory services

- DAC restricts access to data and systems based on the identity of users and/or their group membership
- Access results are usually based on authorization granted to a user based on the various forms of credentials he/she presented at the time of authentication
- In most DAC implementations, the owner of the resource can change its permissions at their discretion
- A DAC framework can deliver the capability for granular access control

Pros and Cons of DAC

PROS

Advantages

- Easy to implement and operate
- Aligns with the least privilege security principle
- Object owner has control over granted access

CONS

Disadvantages

- Documentation of the access must be strictly maintained
- There is a propensity for privilege (scope) creep to occur

Role-based Access Control

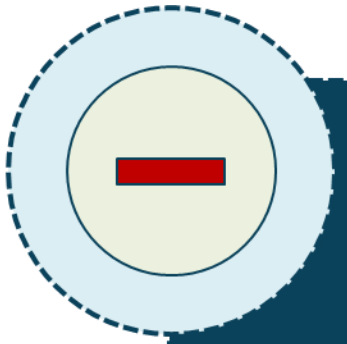
Common in databases and cloud services

- Access decisions rely on org chart, roles, responsibilities, or location in a user base
- Role is typically set based on evaluating the essential objectives and architecture of the enterprise
- RBAC framework is determined by security administrators and officers and not at the discretion of the user
- An RBAC framework should provide web application security admins with the ability to determine who can perform what actions, when, from where, in what order, and in some cases under what circumstances

Pros and Cons of RBAC

Advantages

- Easy to implement and control
- Roles are assigned using written security policy
- Built into many security frameworks
- Aligns accepted security principles

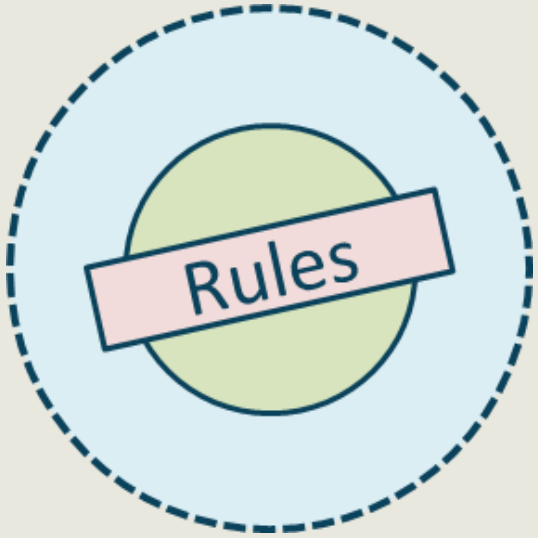


Disadvantages

- Scope creep can take place over time
- Roles and access must be audited rigorously
- Multi-tenancy capabilities need things like AD OUs

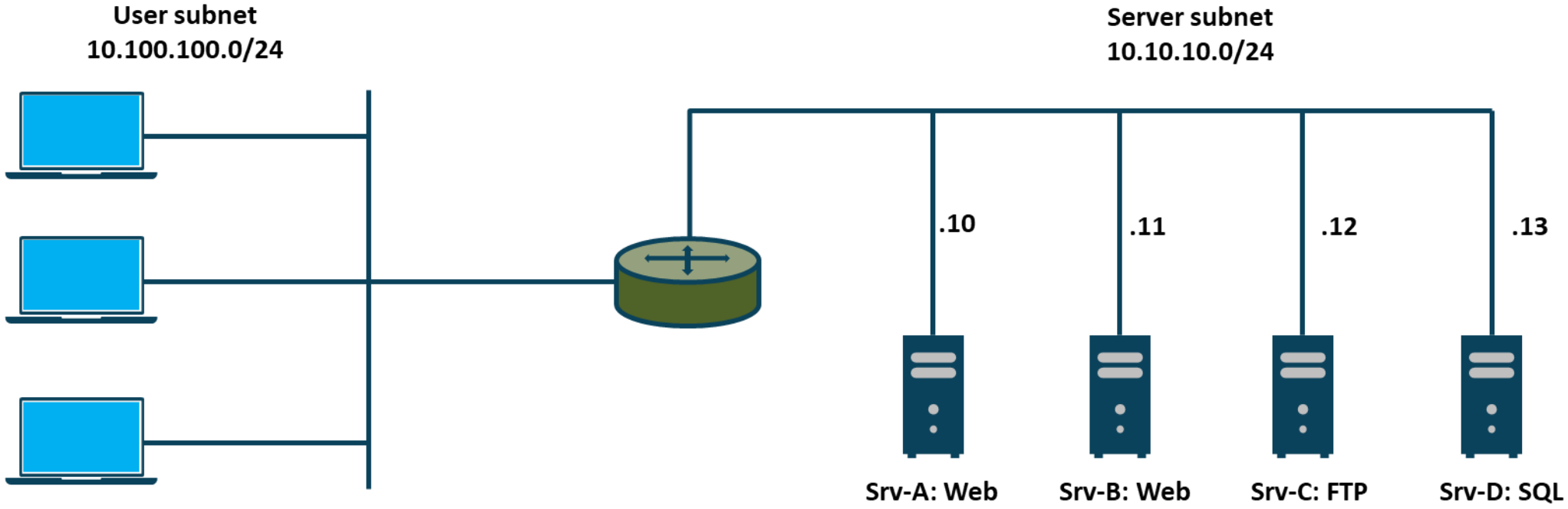
Rule-based Access Control

Common in access control lists



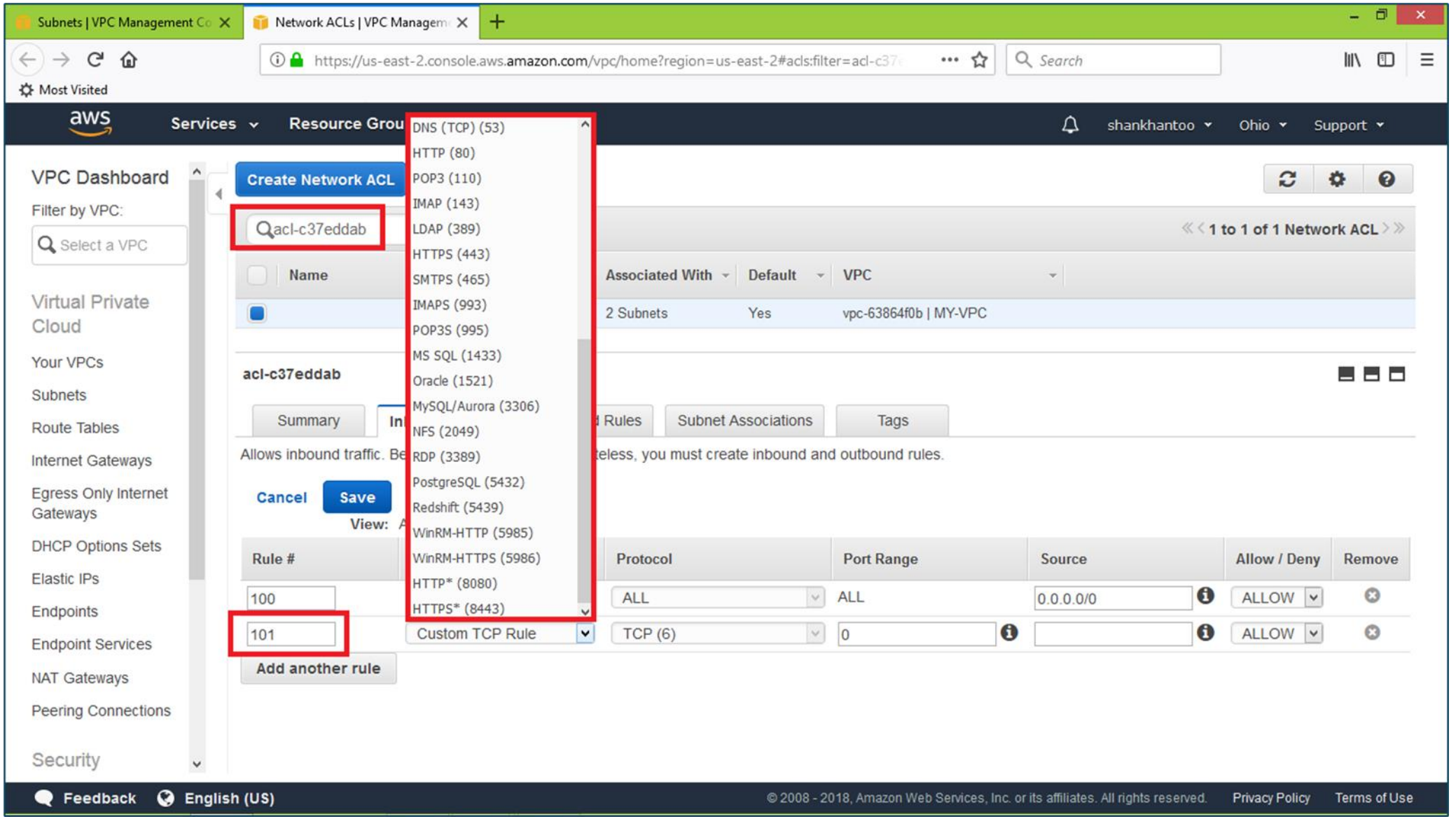
- Rule-based access control uses the acronyms RBAC or RB-RBAC
- It can dynamically assign roles to users based on criteria defined by the custodian or system administrator
- It could also be a time-based ACL if NTP is being used
- Example: a user is only allowed access to a drive on a server from
  6 a.m. to 6 p.m. Monday through Friday
- It is common for infrastructure devices like routers, switches, and firewalls to use rule-based access controls

Rule-based Access Control




```
access-list 100 permit tcp any 10.10.10.10 eq www
access-list 100 permit tcp any 10.10.10.10 eq 443
access-list 100 permit tcp any 10.10.10.11 eq www
access-list 100 permit tcp any 10.10.10.11 eq 443
access-list 100 permit tcp any 10.10.10.12 eq ftp
access-list 100 permit tcp any 10.10.10.12 eq ftp-data
access-list 100 deny ip any any log
```

AWS Network ACL (NACL)

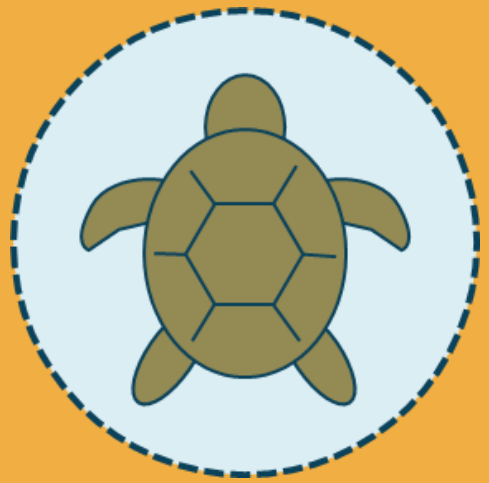


Mandatory Access Control

Common in government agencies and military environments

- MAC is a strict non-discretionary model defining relationships between subjects and objects
- It secures data by assigning sensitivity labels, then compares the labels to the level of user sensitivity
- Appropriate for extremely secure systems such as multilevel secure military applications
- Main advantage is that access based on "need to know" is strictly adhered to and scope creep is minimized
- All MAC systems are based on the Bell-LaPadula model for confidentiality

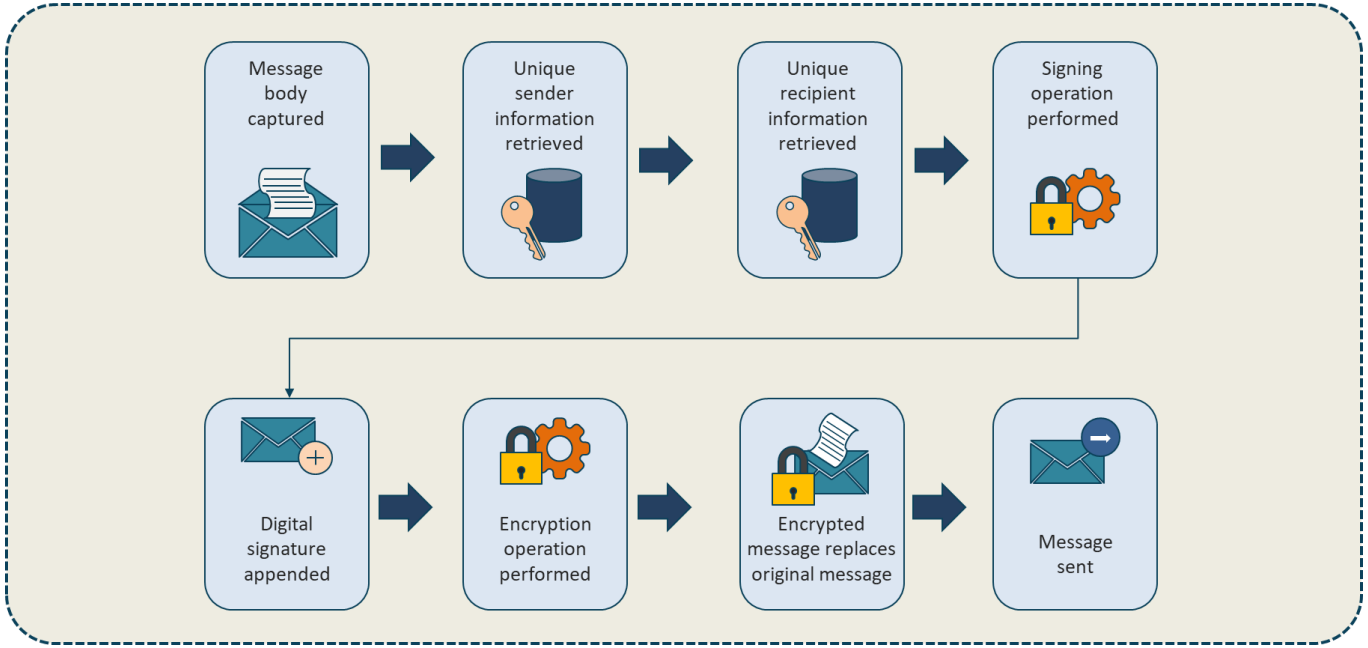
Secure Shell (SSH)



- Management access should be limited to secure protocol alternatives, as in SSH instead of Telnet
- SSH2 is preferable to SSH1 whenever possible
- SSH2 uses symmetric encryption for the bulk data encryption and asymmetric algorithms in their key management processes
- SSH2 uses DH for key exchange

S/MIME

- Secure/Multipurpose Internet Mail Exchanger
- SMTP is not natively secure, so it needs an extra security layer
- S/MIME v3 has become the standard for email message security
- Digital signatures are the most common S/MIME service providing authentication, data integrity, and non-repudiation



FTPS

- FTPS is essentially the File Transfer Protocol with SSL/TLS Security
- It extends the FTP protocol by adding SSL/TLS functionality
- Also called FTP over TLS and FTP Secure
- Typically used server-to-server
- Uses AES, RSA/DSA, and X509v3 certificates
- Explicit FTPS
  - Selected parts or components for communication are encrypted
- Implicit FTPS
  - All communications are encrypted

SFTP

- IETF designed version of FTP that provides secure data access and transfer over an SSH2 channel
- It is a function of the SSH Protocol and is also called SSH File Transfer Protocol
- Both the commands and data are encrypted
- Platform-independent
- Slower than SCP

Domain Name System Security Extension (DNSSEC)

- DNSSEC (DNS Security Extensions) protects users from DNS attacks and forces systems to detect DNS attacks
- It adds a layer of trust on top of DNS by providing authentication while the root DNS name servers help verify domains
- To facilitate signature validation, DNSSEC adds a few new DNS record types:
  - RRSIG - contains a cryptographic signature
  - DNSKEY - contains a public signing key
  - DS - contains the hash of a DNSKEY record
  - NSEC and NSEC3 - for explicit denial-of-existence of a DNS record
  - CDNSKEY and CDS - for a child zone requesting updates to DS record(s) in the parent zone

Secure RTP

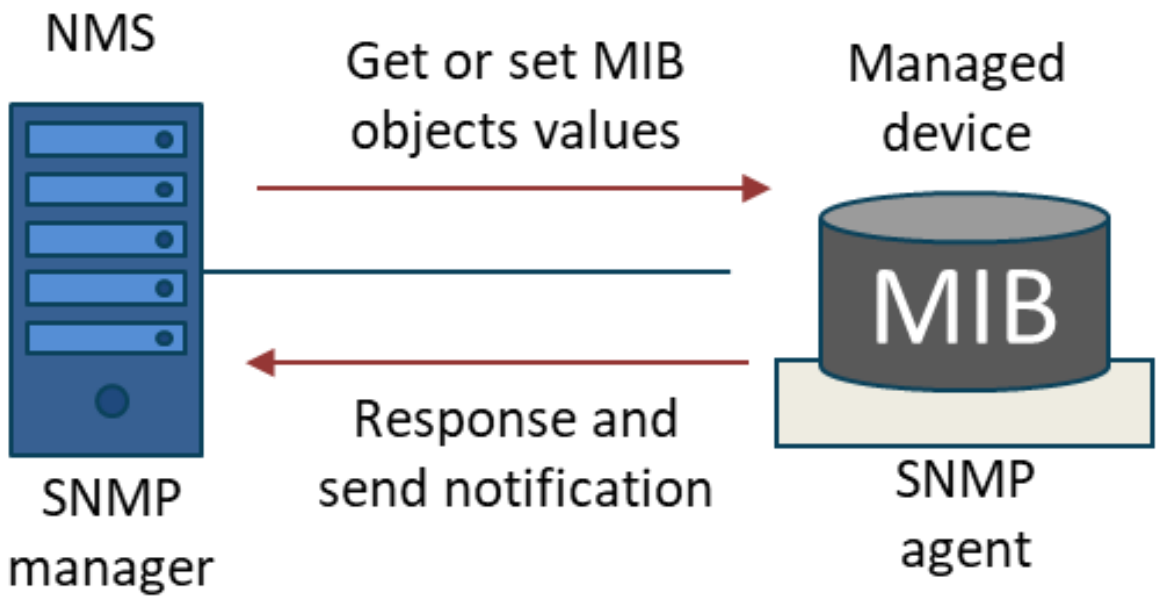
- Secure Real-Time Transport Protocol (SRTP) extends the RTP protocol by providing enhanced security techniques
- Provides encryption, integrity, and authentication verification of data and messages transported by RTP
- Released in 2004 by Cisco Systems and Ericsson

LDAPS

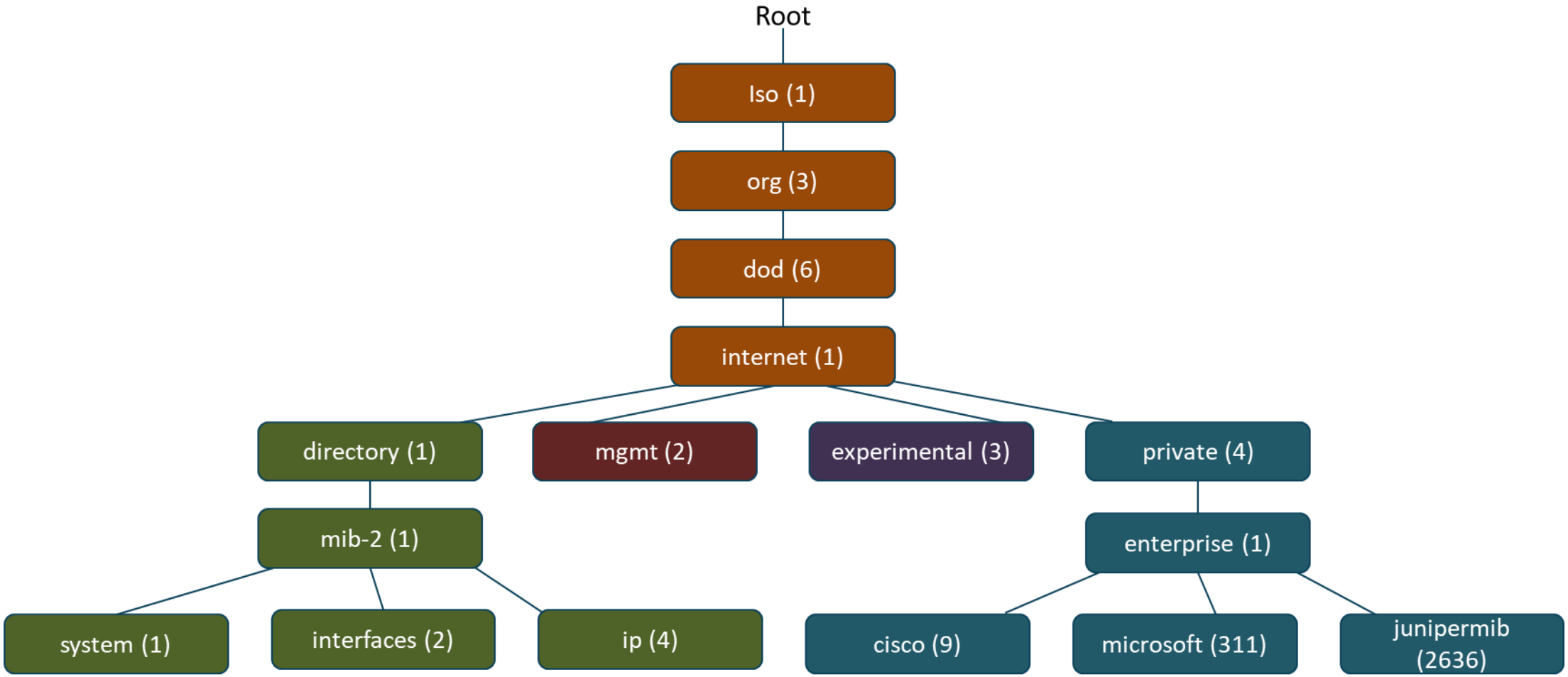
- LDAP was based on X.500 but is a lighter, cross-platform, and standards-based solution
- LDAP servers are easy to install, maintain, and optimize but they are without solid security of the queries, updates, and valuable information in the LDAP directory
- LDAPS (TCP 636) is LDAP over SSL/TLS
- SASL (Simple Authentication and Security Layer) BIND also offers authentication services using mechanisms like Kerberos, or a client certificate sent with TLS

Simple Network Management Protocol (SNMP)

- Simple Network Management Protocol (SNMP) deservedly has a bad security reputation for versions 1 and 2c, which are both clear text protocols and use community strings for authorization
- All versions of SNMP use a tree-structured MIB



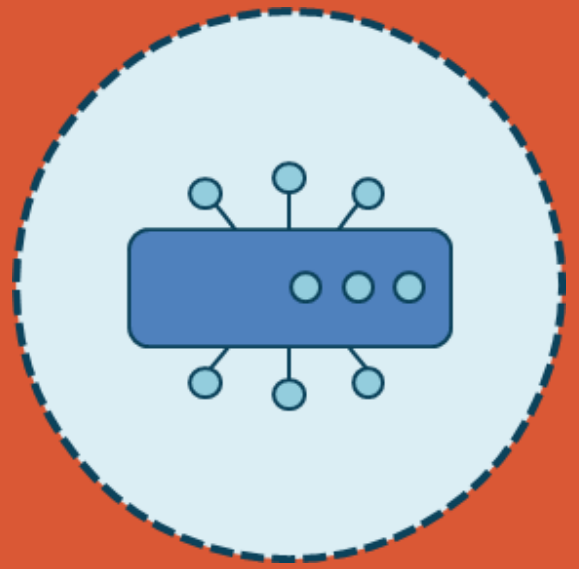
Simple Network Management Protocol (SNMP)



OID Tree Example

SNMPv3

- SNMPv3 can be configured in three modes:
  - noAuthNoPriv - no cryptographic hash or encryption (passwords)
  - AuthNoPriv - cryptographic HMAC (SHA1 or SHA2) to secure authentication credentials and provide integrity, but no data encryption
  - AuthPriv - HMAC for integrity and secure authentication credentials, and encryption (AES) of data



SSL/TLS

- SSL/TLS is the most ubiquitous certificate-based peer authentication in use on the Internet (HTTPS)
- Transport Layer Security (TLS) is standardized by IETF
- TLS 1.3 is the most recent published version
- It is also used with SMTP, LDAP, and POP3
- The only mandatory cipher suite includes RSA for authentication, AES for confidentiality, and SHA for integrity and digital signatures

SSL/TLS

3 User software verifies signature on identity certificate, validating authenticity of public key

4 User software creates a shared-secret key

TLS VPN tunnel

1 User makes a connection to TCP port 443

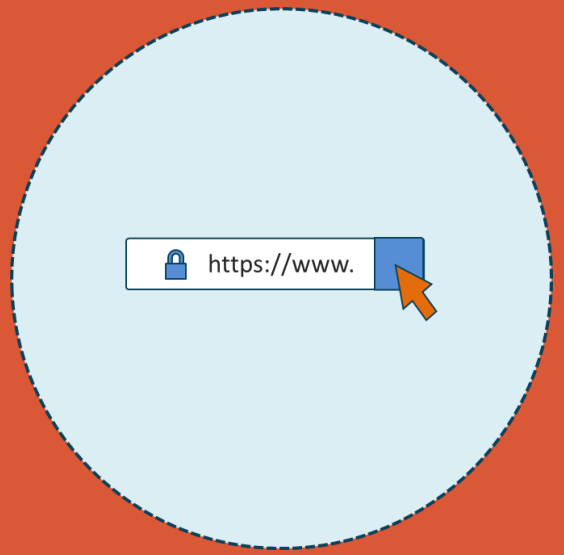
2 The server response contains server's public key

5 Shared-secret key, encrypted with public key of the server, is sent to the server

6 Bulk encryption occurs using the shared-secret key
etric encryption algorithm

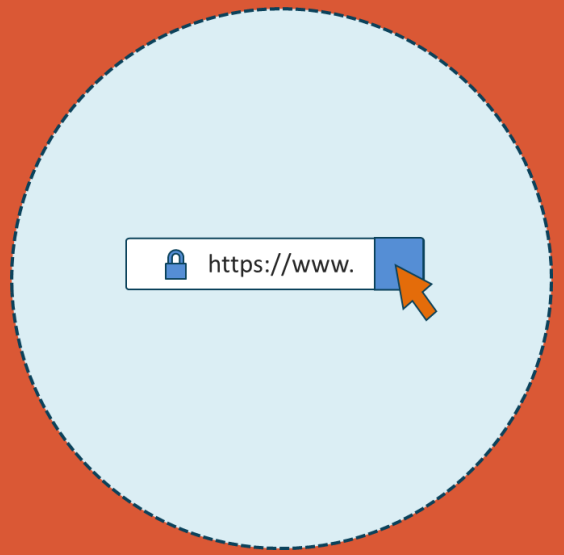
HTTPS

- The most widely used protocol on the Internet for any secure commercial transaction, financial service, contract, agreement, file transfer protection, and voice or video service
- Mozilla is deprecating non-HTTPS secured search results in order to hasten the global adoption of HTTPS
- A cryptographic key exchange happens when you first connect to a secure web site and all ensuing activities on the web site are encrypted



HTTPS

- It is still possible to see that web sites have been visited – but not the web pages you read, or data transferred
- If a padlock icon is shown, then the web site is secure
- If the icon is green, it signifies that the web site has presented your browser with an Extended Validation Certificate (EV)
- This verifies that the SSL certificate presented is accurate for the domain name, and the domain name belongs to the entity you would expect to own the web site



POPS and IMAPS

- These are versions of the POP (POPS) and IMAP (IMAPS) email protocols that run over SSL/TLS
- IMAP over SSL (IMAPS) is assigned the port number 993
- Encrypted communication for POP3 is either:
  - Requested after protocol initiation using the STLS command
  - Connected to the server using SSL/TLS on well-known TCP port 995

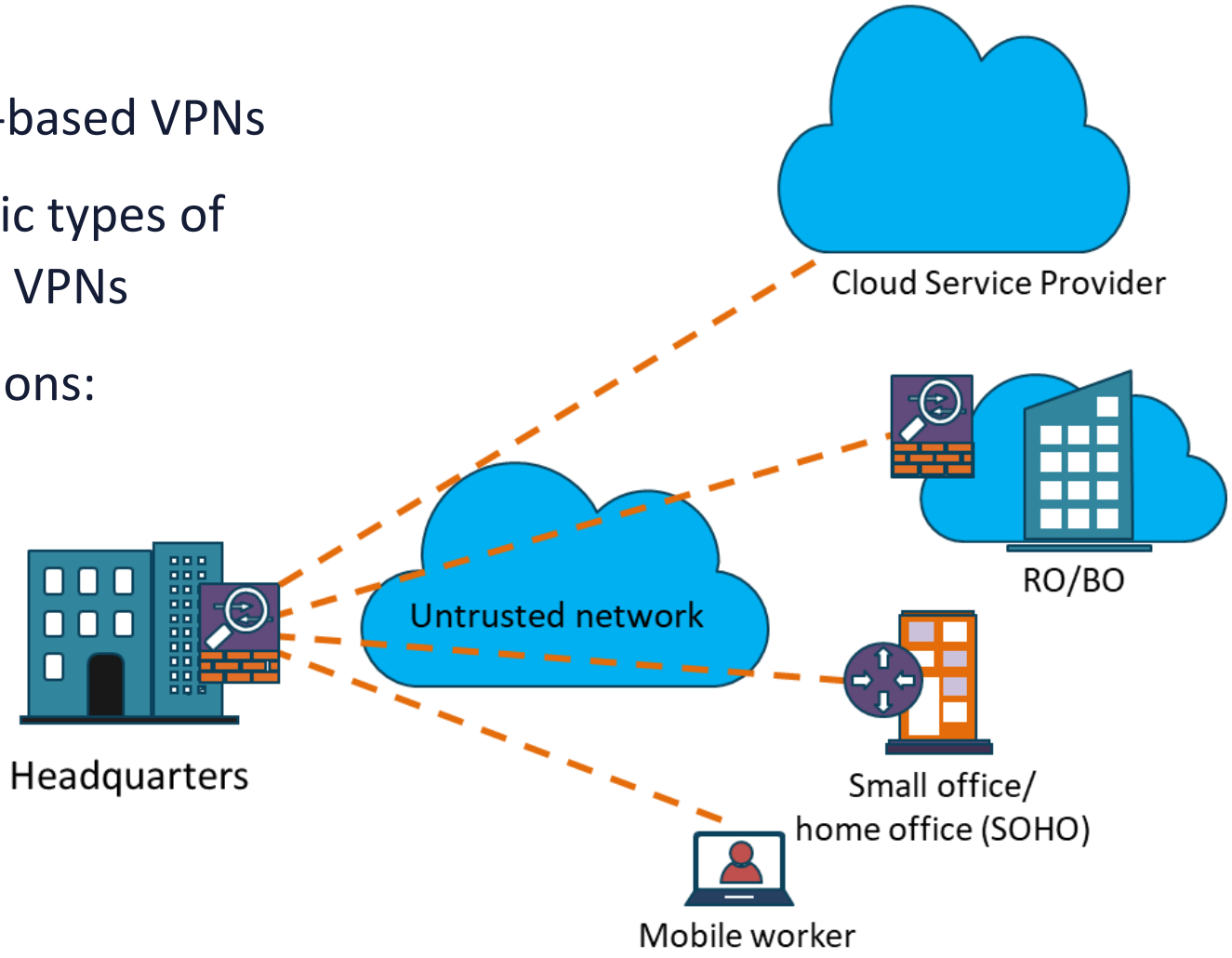
IPsec Overview

IP Security for IPv4 and IPv6

- IP Security (IPsec) offers security services to traffic crossing untrusted networks, like the Internet, between two or more trusted devices or networks
- IPsec VPNs can also be used to protect management traffic as it crosses an organization's intranet and between front-end and back-end services
- IPsec is also popular when connecting to cloud service providers

IPsec VPNs

- IPsec and SSL VPNs are both cryptography-based VPNs
- In terms of deployment, there are two basic types of VPNs: site-to-site VPNs and remote-access VPNs
- IPsec provides five essential security functions:
  - Confidentiality (3DES, AES-128/256)
  - Data integrity (SHA1, SHA2/3)
  - Origin authentication
    - Pre-shared keys or RSA or ECDSA signatures
  - Anti-replay protection
  - Key management (IKEv1/2, DHKE, ECDHE)
- Operates in tunnel or transport modes



IPsec Security Suites

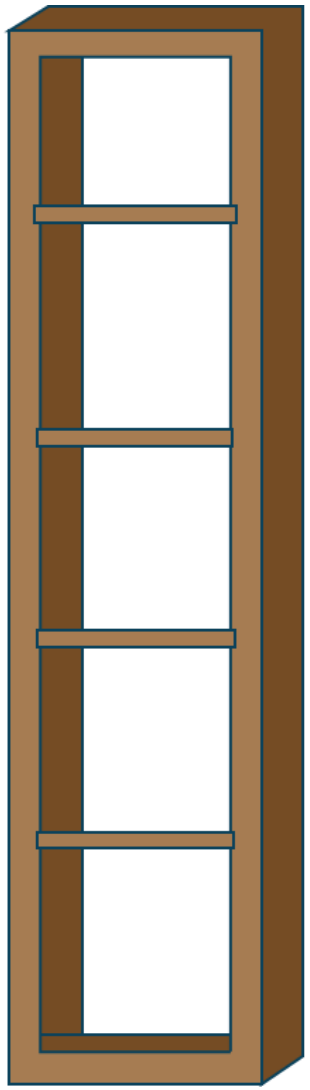
IPsec Protocol

Confidentiality

Data integrity

Origin authentication

Key management



ESP | ESP +AH | AH

DES | 3DES | AES

MD5 | SHA-1 | SHA-2

PSK | RSA | ECDSA

DH | ECDH | IKE | IKEv2

Acceptable Use Policies

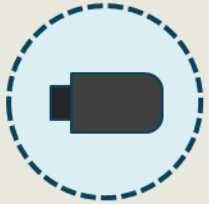
- The most important aspect of the written security policy from the customer perspective is the Acceptable Use Policy (AUP)
- An AUP is a document specifying constraints and practices that a user must agree to for access to a corporate network or the Internet
- It is often divided into different sections based on various categories of access
- There should always be an enforcement mechanism in place to support the policy

Endpoint Physical Security

Computer and laptop locking mechanisms

Screen savers with strong passwords

Disable unused peripherals



Adhere to removable device AUP

Use strongest biometric authentication and MFA

Endpoint Physical Security

Use smart cards and tokens according to AUP

Place electronics in a locked drawer or cabinet

Disconnect and/or remove unused computers

Take responsibility for client-side encryption

Protect printers and fax machines

Hardware and Software Updates

- Organizations will have varying degrees of end-user participation in hardware and software upgrades
- If fully automated (i.e., WSUS, Java, Silverlight, O/S services, KACE), the end-user can only, at the most, potentially postpone the process

Personal Security Suites and Endpoint Protection

- These are all-in-one, full-scale security packages that offer a single, integrated solution
- There is only one vendor to get the upgrades and updates from
- Depending on the security vendor, the suite may also include a two-way firewall, parental control system, a local spam filter, VPN to protect your data in transit, online backup, and dedicated ransomware protection

Web Browser Best Practices

Be certain browser software is updated

Manage and disable unnecessary/malicious plugins

Try to always connect using HTTPS (TLS1.2+)

Choose EV validated sites, if possible

Clear browser histories

Web Browser Best Practices

Never store passwords in a browser

Use strong passwords and password managers

Disable popups (install AdBlock)

Use VPNs and proxy servers (Cisco Umbrella)

Utilize browser security configurations

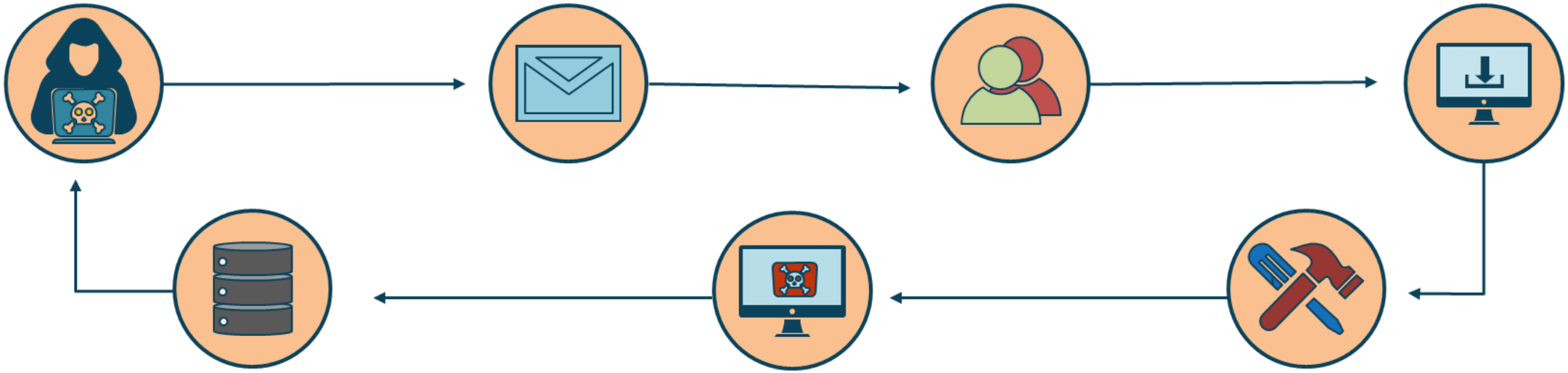
E-Mail Security Fundamentals

1. Attacker
Attacker sends e-mail with malware attachments to use

2. Phishing email
Poorly trained and unaware users open the attachment

3. Targeted users
Target system is exploited

4. Compromised system
Remote Access Trojan (RAT) is installed on the target system



5. Remote Access Trojan
RAT is used to gain access to additional systems on the internal network

6. Internal network
Data is stolen from the compromised machines

7. Data
Data is exfiltrated to the attacker in a stealthy manner

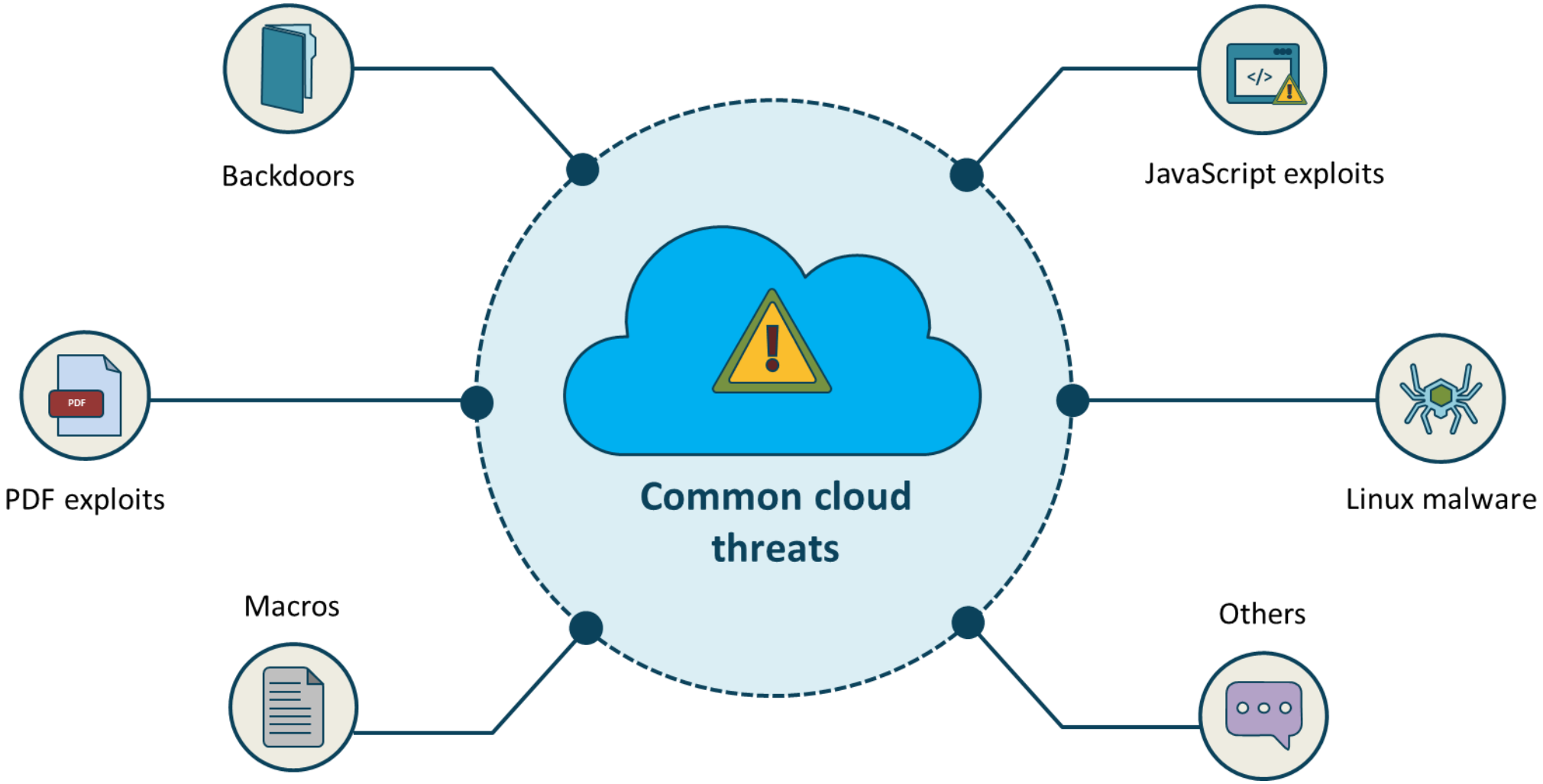
E-Mail Security Fundamentals

- Use rotating passwords that involve four random words separated by "-" or "."
  - For example, texmex-world-glove-listen
- Implement strong malware scanners and spam filters
  - Never reply to spam or click any "unsubscribe" links as this will only confirm to the spammer that your e-mail address is real
- Gain expertise in recognizing phishing e-mails
  - Corporate and small business spear phishing is on the rise
  - Conduct awareness programs
- Use "two-tier" or multi-factor authentication when logging on to your webmail, if available

E-Mail Security Fundamentals

- Before opening an attachment, make certain that you know who it’s from and that you are expecting it
- Consider a confirming SMS text or phone call
- Only send personal information over email when necessary
- Use encrypted email where possible
- Avoid using email over free Wi-Fi

Personal Cloud Storage Security Issues



Endpoint Detection and Response (EDR)

Next-gen beyond HIDS/HIPS

- Endpoint Detection and Response (EDR) tools primarily focus on detecting and investigating suspicious activities and are indicators of compromise (IoCs) on hosts/endpoints
- EDR tools monitor endpoint and network events and send information to a SEIM system or centralized database so further analysis, investigation, and reporting can take place
- A software agent installed on the host system often provides the basis for event monitoring and reporting

Endpoint Detection and Response (EDR)

Next-gen beyond HIDS/HIPS

- Key EDR features:
  - Filtering - reduces alert fatigue and lowers the possibility for real threats to slip through unnoticed
  - Advanced Threat Blocking: prevents threats the moment they are detected and throughout the lifecycle of the attack
  - Incident Response Capabilities - threat hunting and incident response can help prevent full-blown data breaches (DLP)
  - Multiple Threat Protection – cloud-based visibility into many finding categories

Next-generation Endpoint Protection

IT hygiene

Next-generation antivirus (NGAV)

Managed hunting

Threat intelligence

Cloud-based architecture