COMPTIA SECURITY+ DAY 03

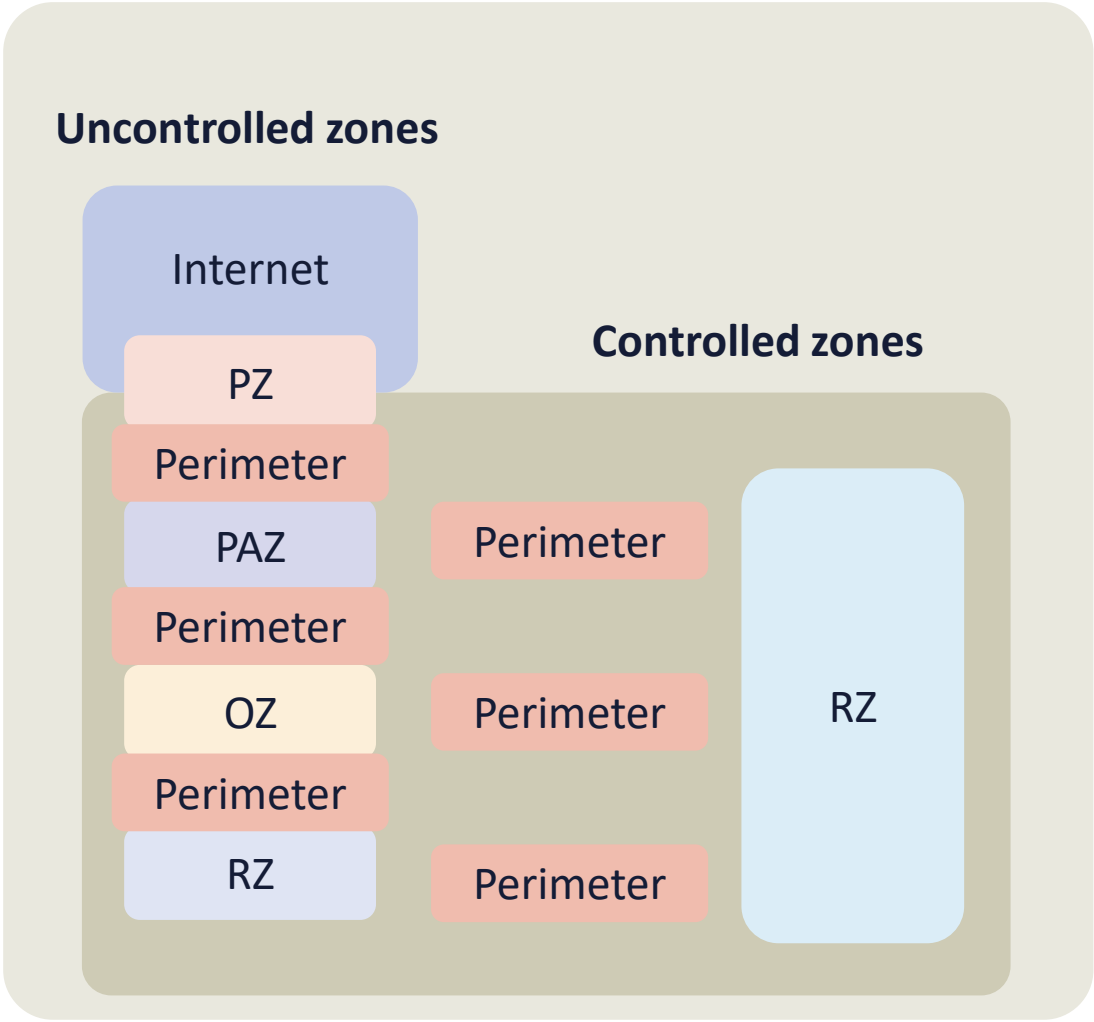
ENTERPRISE INFRASTRUCTURE SECURITY PRINCIPLES

In this course, we will:

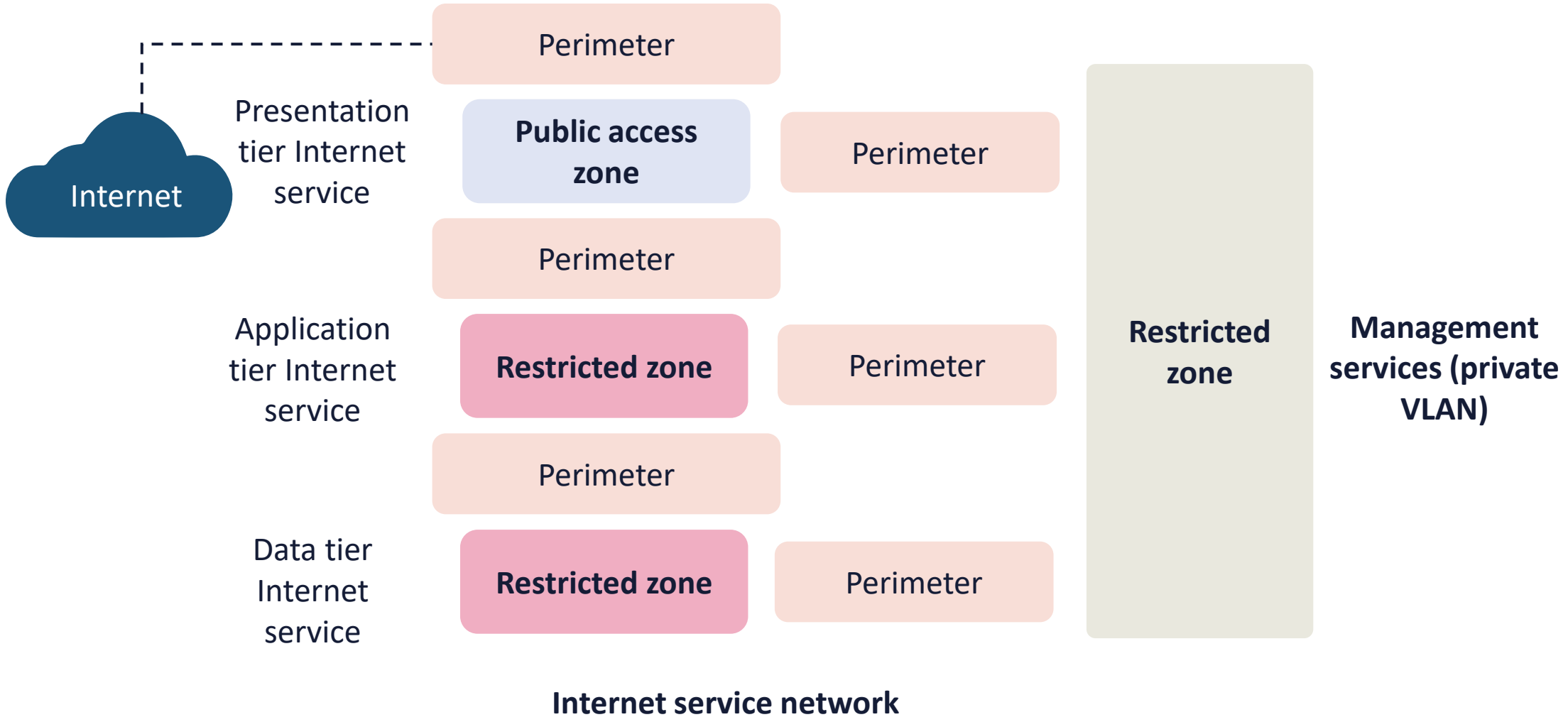
- Discover infrastructure security considerations
- Explore port security and firewalls
- Define IPsec and TLS virtual private networks (VPN)
- Examine SD-WAN and SASE

SECURITY ZONES

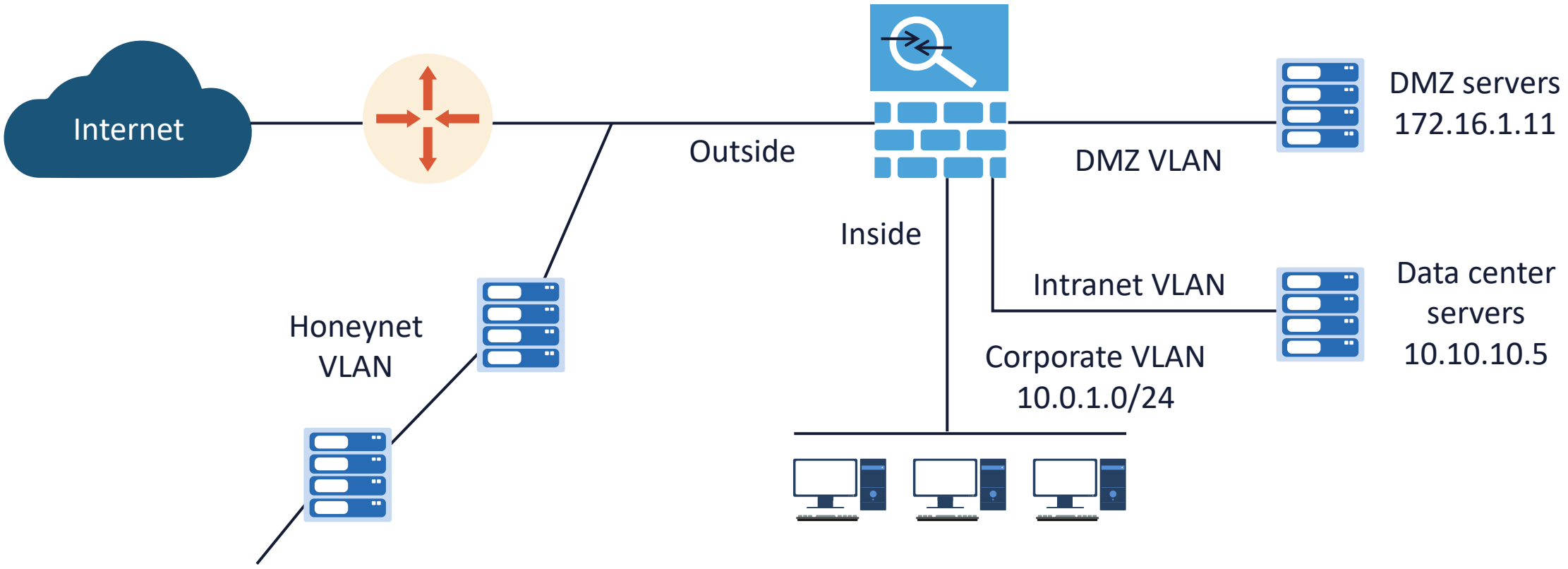
- Zoning is a logical design approach used to mitigate the risk of an open network by segmenting infrastructure services
- Each zone has fundamental characteristics, defined by the security policy:
  - Every zone contains one or more separate, routable networks
  - Every separate, routable network is contained within a single zone
  - Every zone connects to another zone via a perimeter that contains zone interface points (ZIPs)
  - The only zone that may connect to the public zone is the public access zone (PAZ), or DMZ



SEGMENTATION AND ZONING



ZONES AND VIRTUAL LOCAL AREA NETWORKS (VLANS)



ATTACK SURFACE

- The attack surface consists of all possible attack vectors that a threat actor can use to access a system and extract data
- It represents the targets of the cyber kill chain
- The smaller the attack surface, the easier it is to counter with various controls
- The attack surface is split into two categories: digital and physical

ATTACK SURFACE

- Enterprises must continuously monitor their attack surface to recognize, expose, and block potential threats as quickly as possible
- They must also endeavor to minimize the attack surface area to reduce the risk of successful attacks
- Attack surface reduction becomes more difficult as organizations expand their digital footprint and leverage new technologies

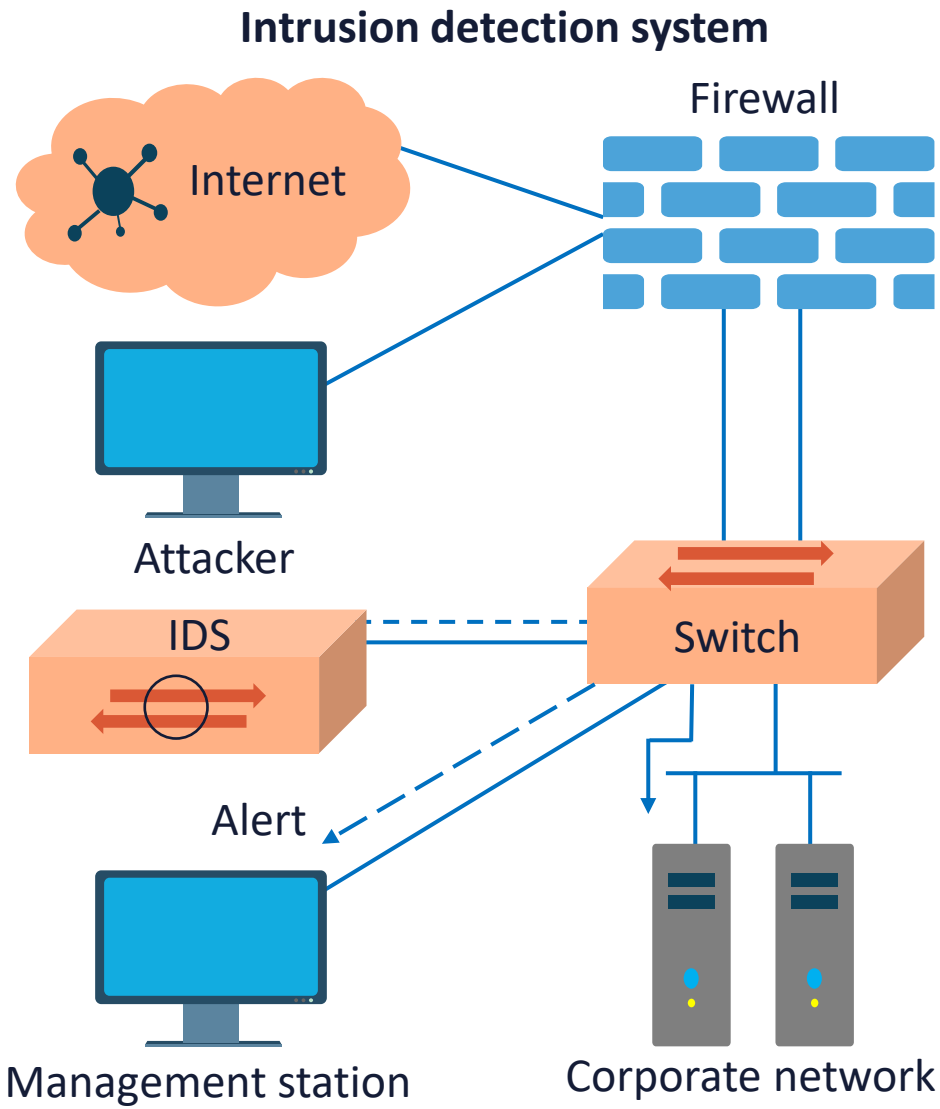
FAILURE MODES

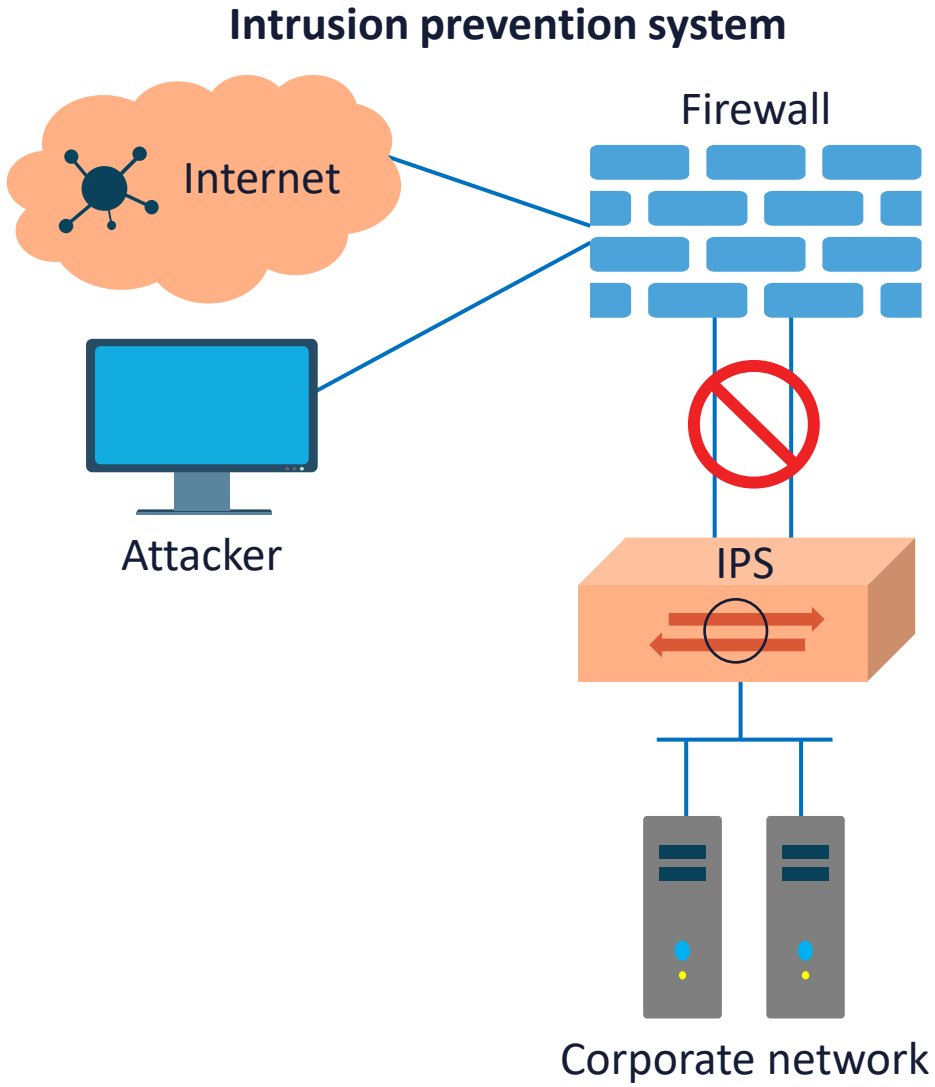
- Certain security infrastructure devices such as firewalls and IPS sensors can be deployed in "fail-open" or "fail-closed" modes
- Fail-open means that even if there is a system or component failure on the device IP traffic should continue to flow to zones on the outbound interfaces
- In fail-closed mode the device will stop processing packets
  - Example: One of the failover interfaces to the standby device shuts down or fails

NETWORK APPLIANCES: IDS/IPS

- An intrusion prevention system (IPS) is a network security hardware or software solution that continuously monitors a zone for malicious activity
- It then proactively takes action to prevent it in the line of traffic
- It is more advanced than an intrusion detection system (IDS), which reactively detects malicious activity
- IPS systems are often integrated into security appliances or part of a next-generation firewall (NGFW) or unified threat management (UTM) solution

INTRUSION DETECTION VS. PREVENTION





IPS ACTIONS

- Alerts and alarms
- Verbose dumps
- Transmission Control Protocol (TCP) resets
- Drop packets or addresses
- Blocking (shun) on firewalls and routers
- Simple Network Management Protocol (SNMP) traps
- Logging to Syslog and security information and event management (SIEM) systems
- Flows to NetFlow collectors

INTRUSION DETECTION VS. PREVENTION

True positive

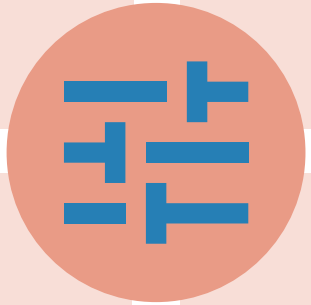
True (accurate) + positive

(action taken)

False positive

False (error) + positive

(action taken)



True negative

True (accurate) + negative

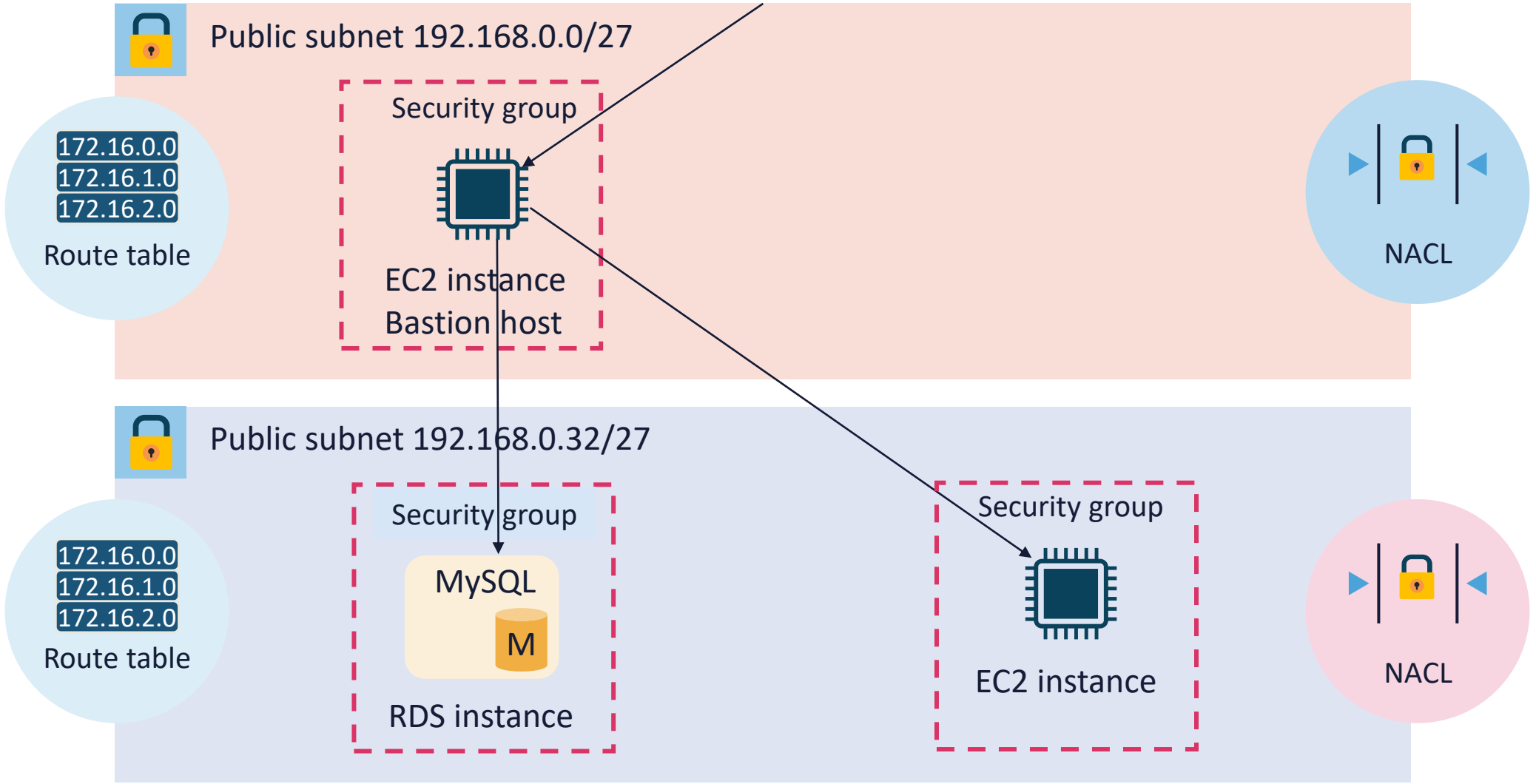
(action not taken)

False negative

False (error) + negative

(action not taken)

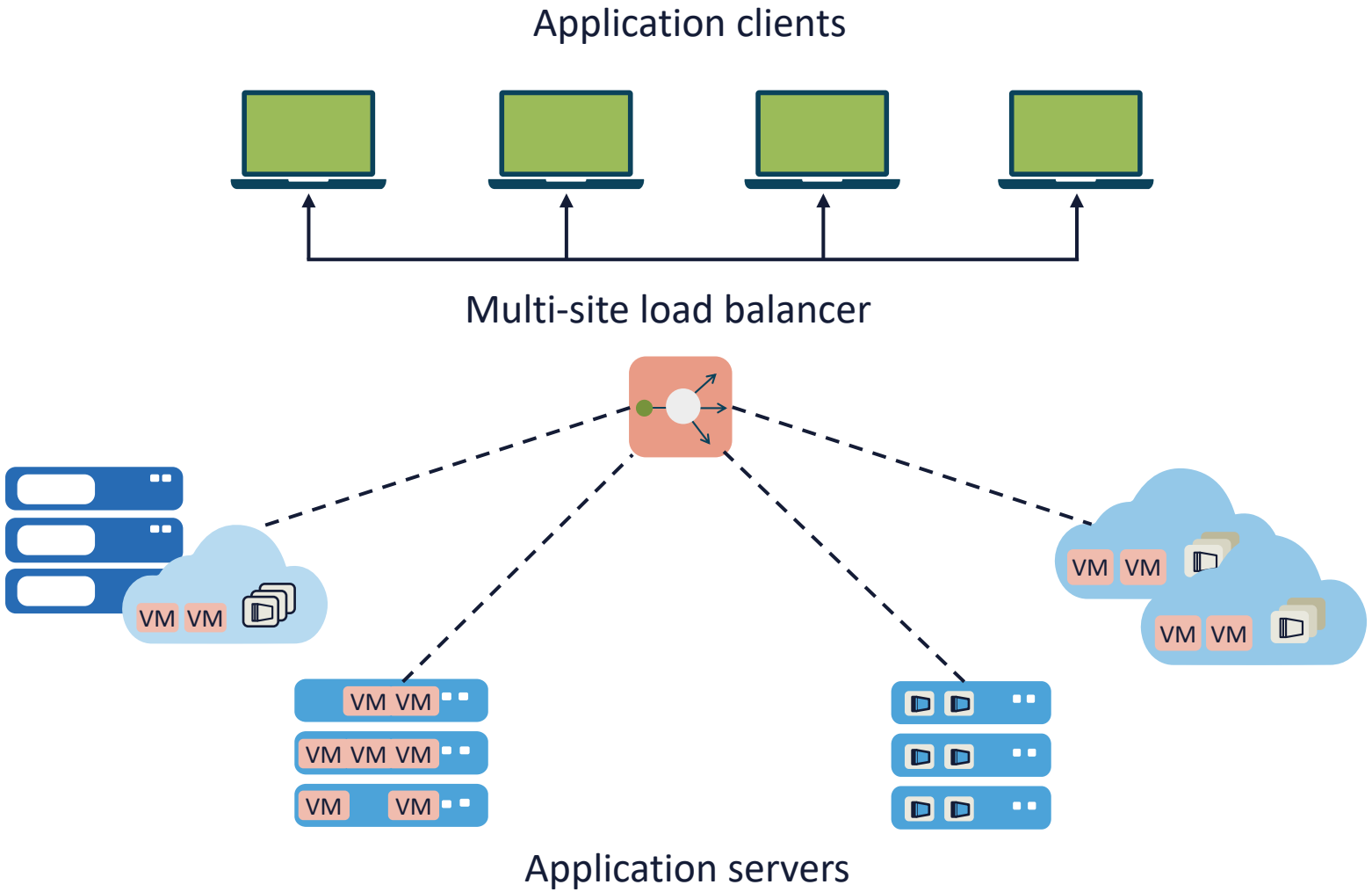
JUMP BOXES AND BASTION SERVERS



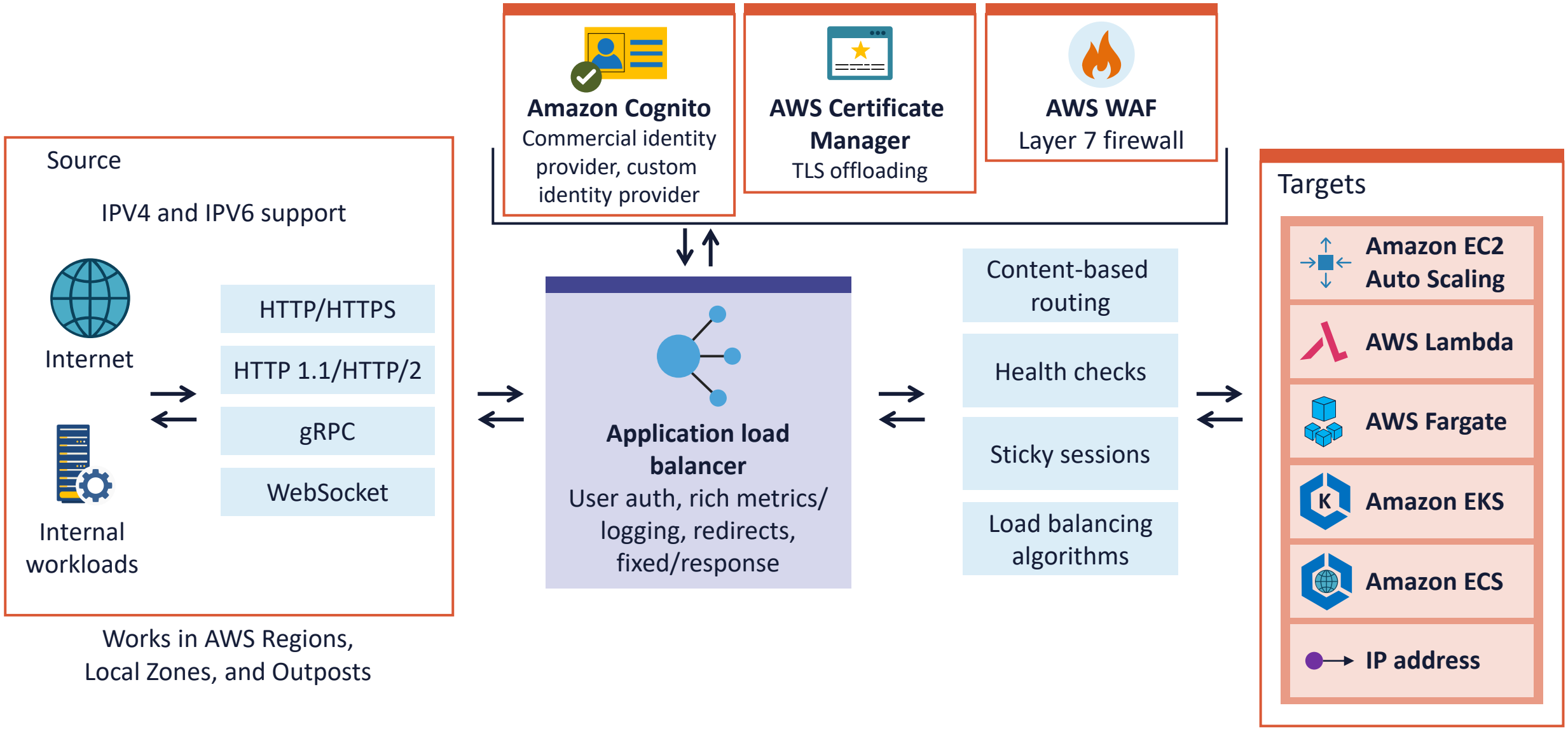
PROXY SERVERS (MEDIATED ACCESS)

- Authentication (interactive or transparent)
- Translation services – Network Address Translation (NAT)
- Bastion (jump) hosts and cloud service provider (CSP) managed services
- Web proxies for content storage and security
- URL filtering
- Managed security service providers (MSSP)
- Cloud access security brokers (CASB)

LOAD BALANCERS

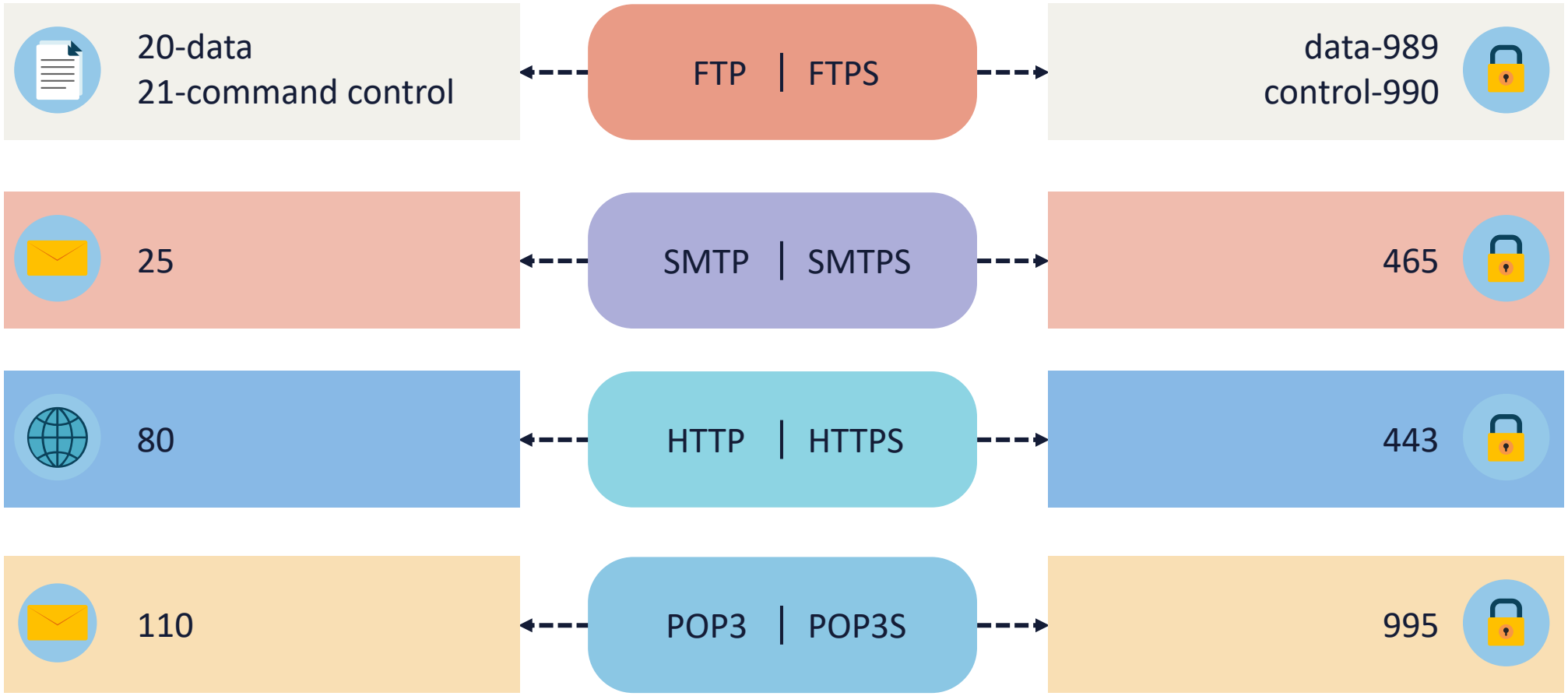


CLOUD LOAD BALANCERS

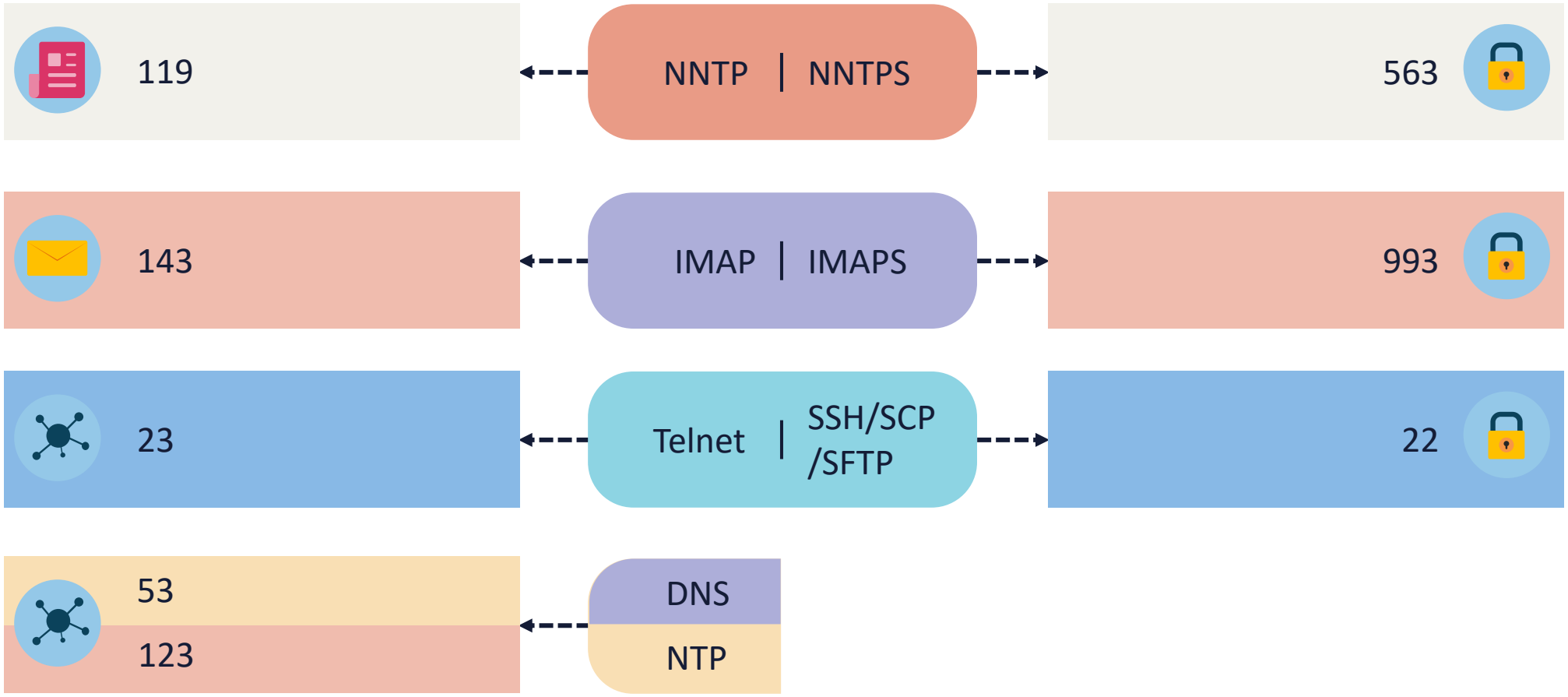


Works in AWS Regions, Local Zones, and Outposts

COMMON PORT NUMBERS



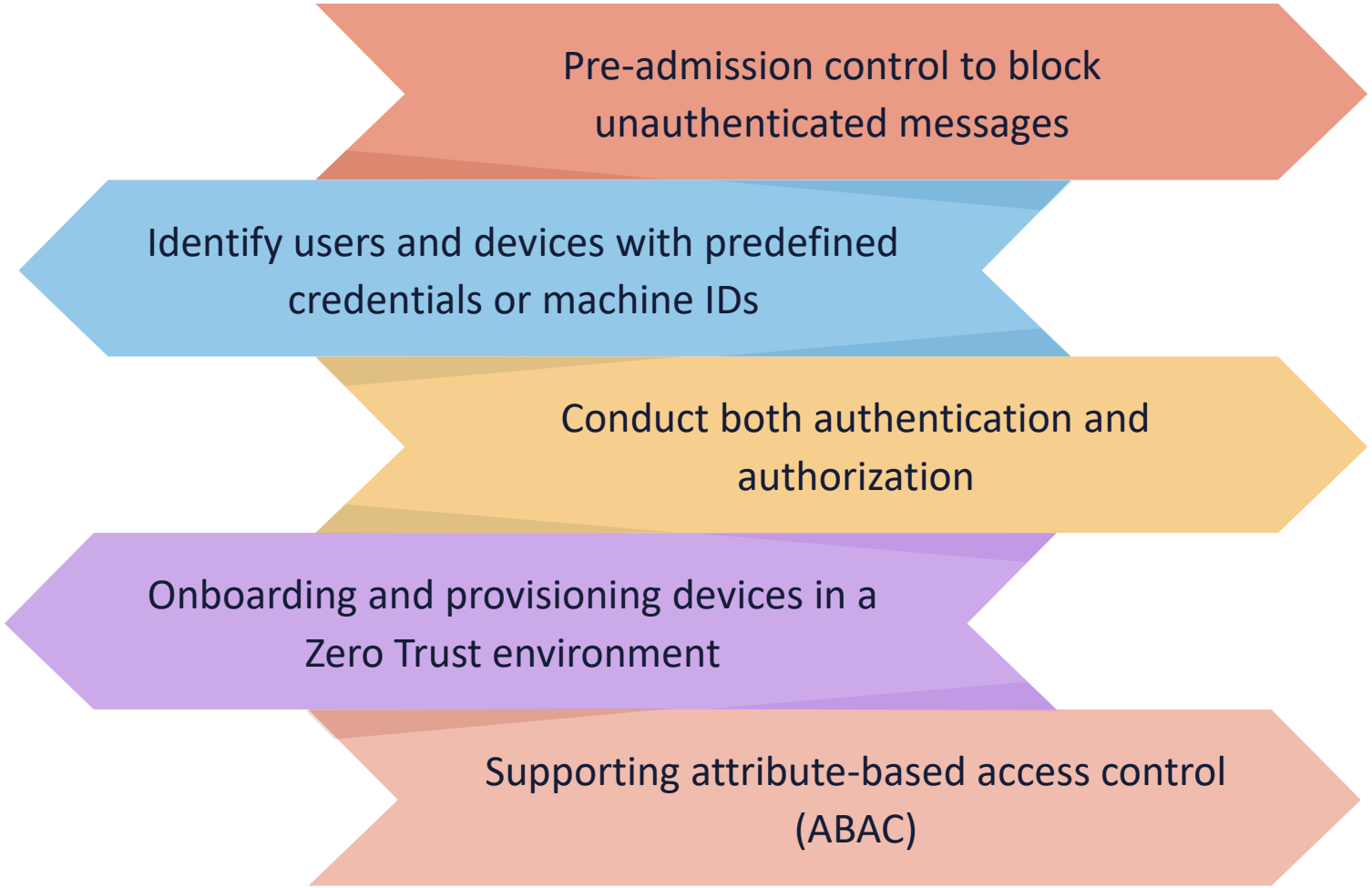
COMMON PORT NUMBERS



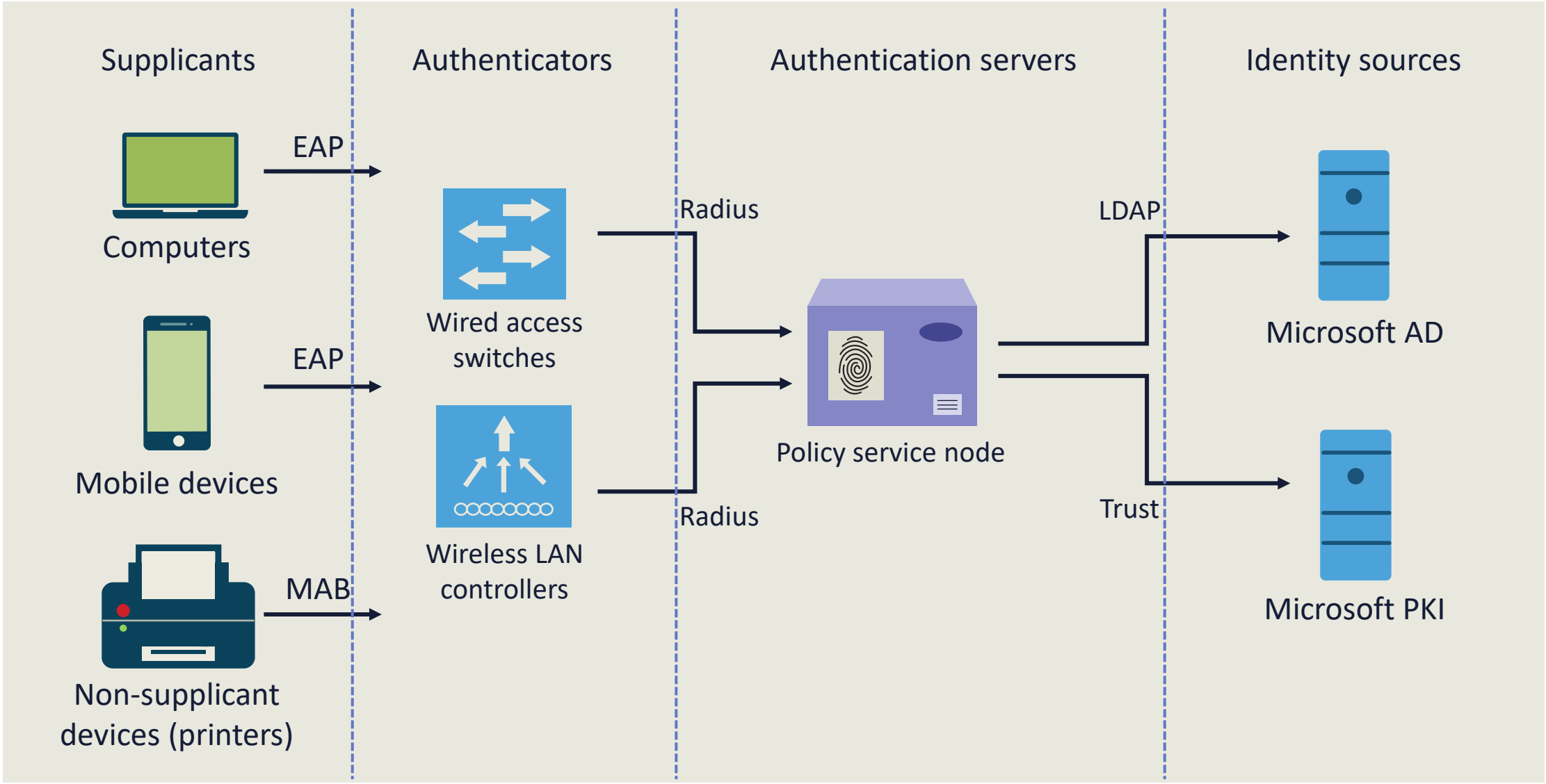
802.1X PORT-BASED NETWORK ACCESS CONTROL (PNAC)

- IEEE 802.1X authentication is also referred to as port-based network access control, or PNAC
- It involves making sure something interfacing with the system is what it claims to be
- When someone wants to gain access to an Ethernet or 802.11 wireless network, it verifies the entity connecting is who they say they are in flexible ways

802.1X CAPABILITIES

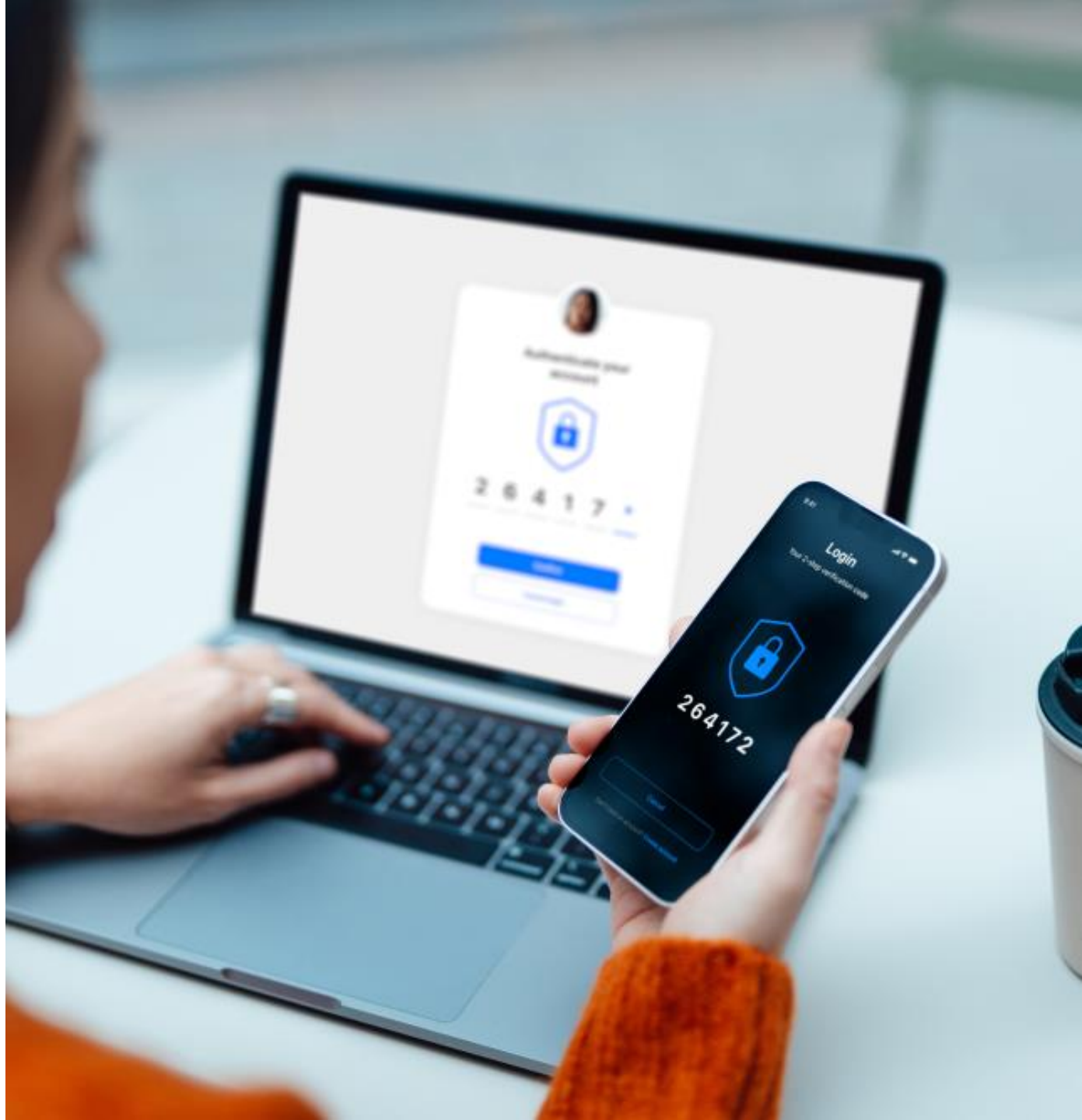


IEEE 802.1X


Supplicants
Authenticators
Authentication servers
Identity sources
Computers
EAP
Mobile devices
EAP
Non-supplicant devices (printers)
MAB
Wired access switches
Wireless LAN controllers
Radius
Radius
Policy service node
LDAP
Trust
Microsoft AD
Microsoft PKI

EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

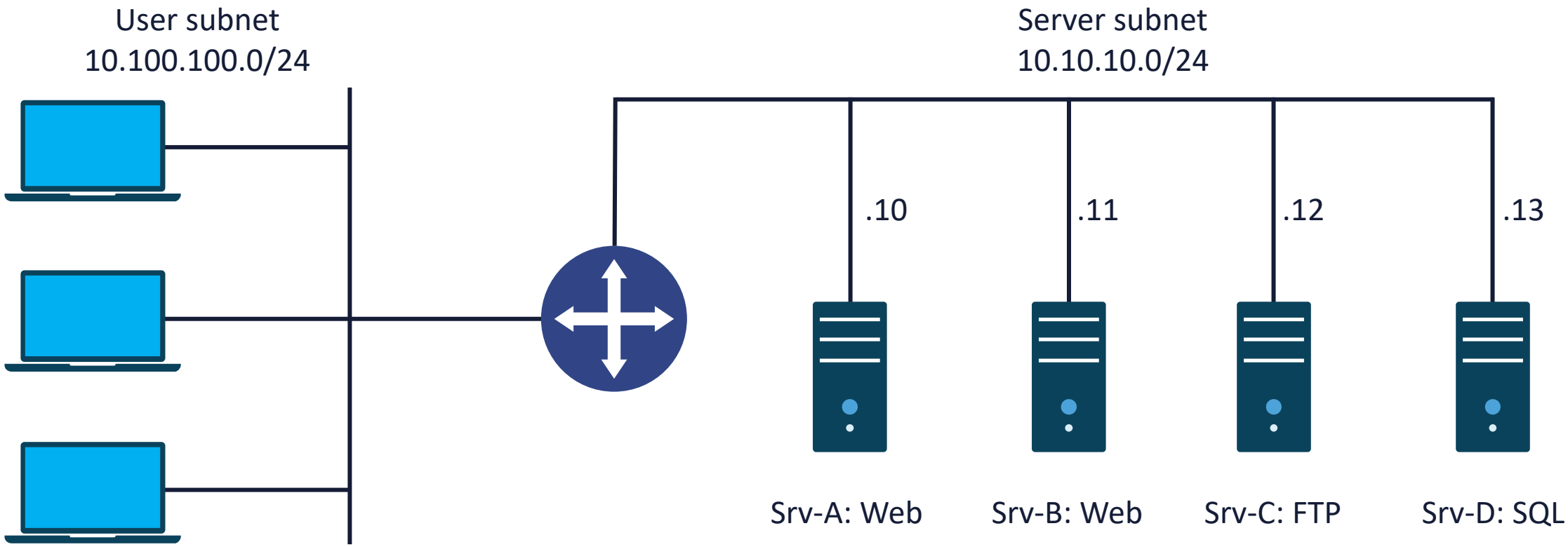
- Extensible Authentication Protocol (EAP) is an authentication framework as opposed to a specific authentication mechanism
- It has evolved over the years from the original Point-to-Point Protocol (PPP)
- It is often used in 802.1X wireless networks and point-to-point connections
- It offers some basic functions and negotiation of authentication methods called EAP methods
- There is typically an original EAP over LAN (EAPOL) exchange before the higher methods are implemented



EXTENSIBLE AUTHENTICATION PROTOCOL

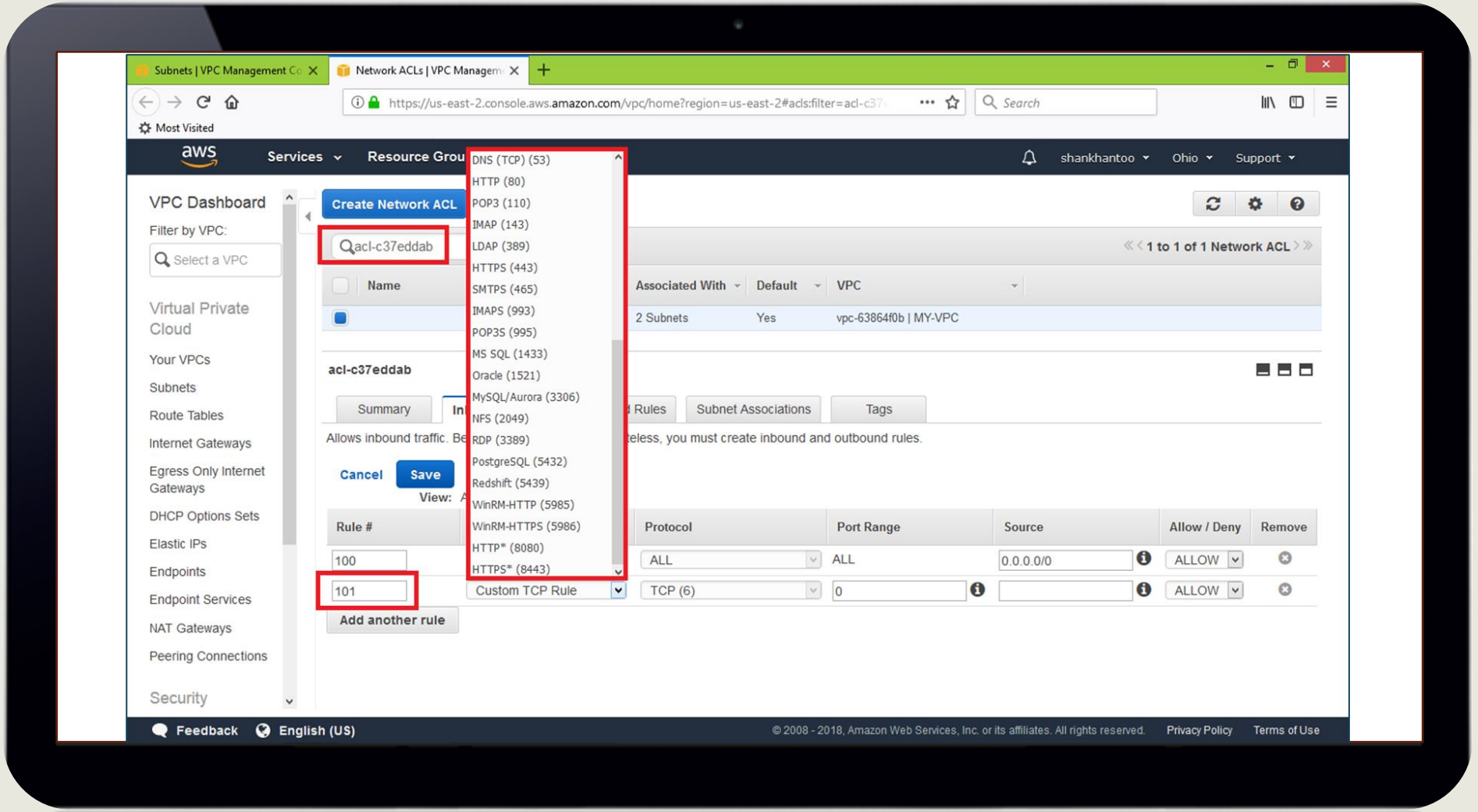
802.1X EAP Types Feature/Benefit	MDS ---- Message Digest 5	TLS ---- Transport Level Security	TTLS ---- Tunneled Transport Level Security	PEAP ---- Protected Transport Level Security	FAST ---- Flexible Authentication via Secure Tunneling
Client-side certificate required	No	Yes	No	No	No (PAC)
Server-side certificate required	No	Yes	Yes	Yes	No (PAC)
Wired Equivalent Privacy (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
Deployment difficulty	Easy	Difficult (because of client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi security	Poor	Very high	High	High	High

ACCESS CONTROL LISTS (ACLS)

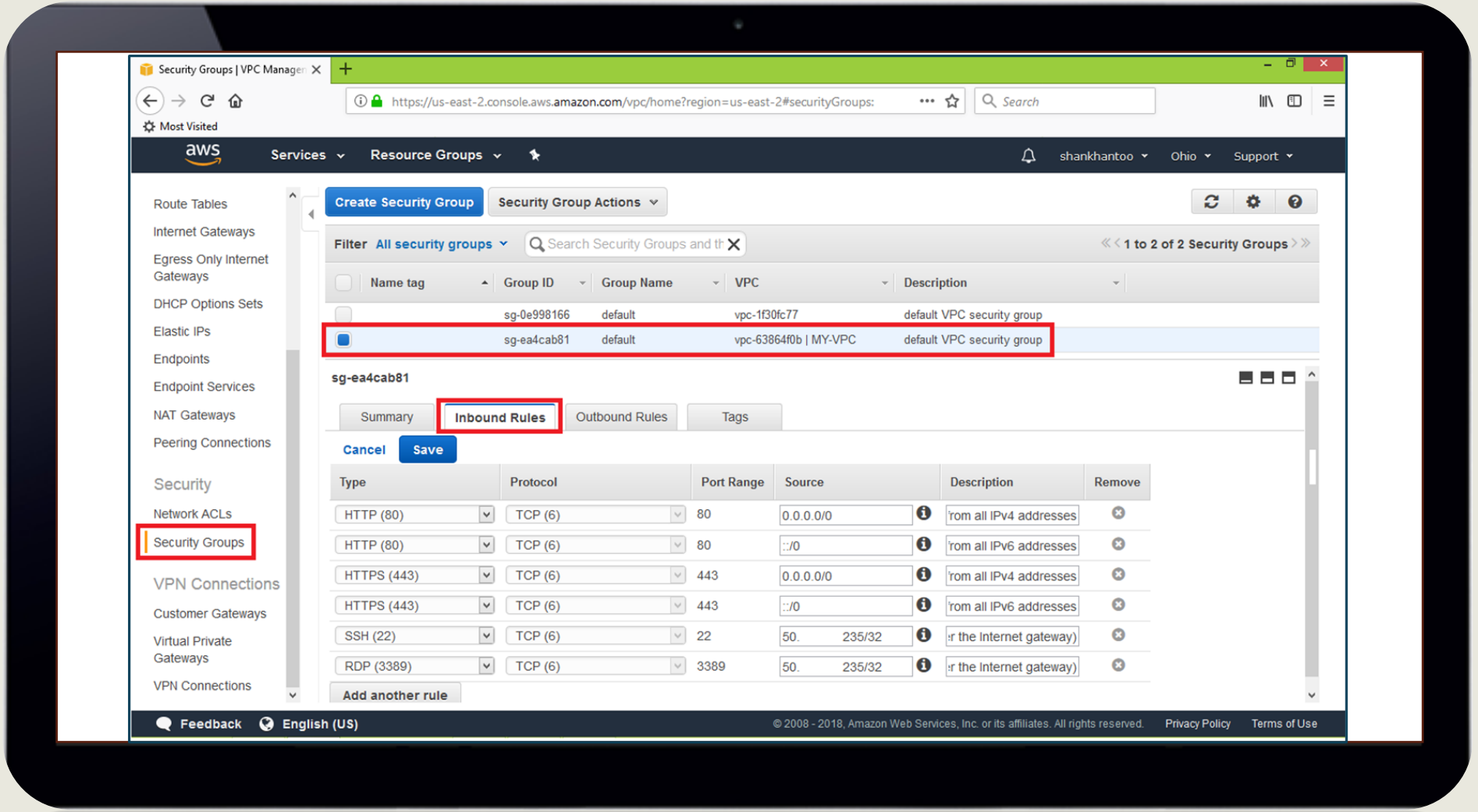



```
access-list 100 permit tcp any 10.10.10.10 eq www
access-list 100 permit tcp any 10.10.10.10 eq 443
access-list 100 permit tcp any 10.10.10.11 eq www
access-list 100 permit tcp any 10.10.10.11 eq 443
access-list 100 permit tcp any 10.10.10.12 eq ftp
access-list 100 permit tcp any 10.10.10.12 eq ftp-data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

NETWORK ACL (NACL)



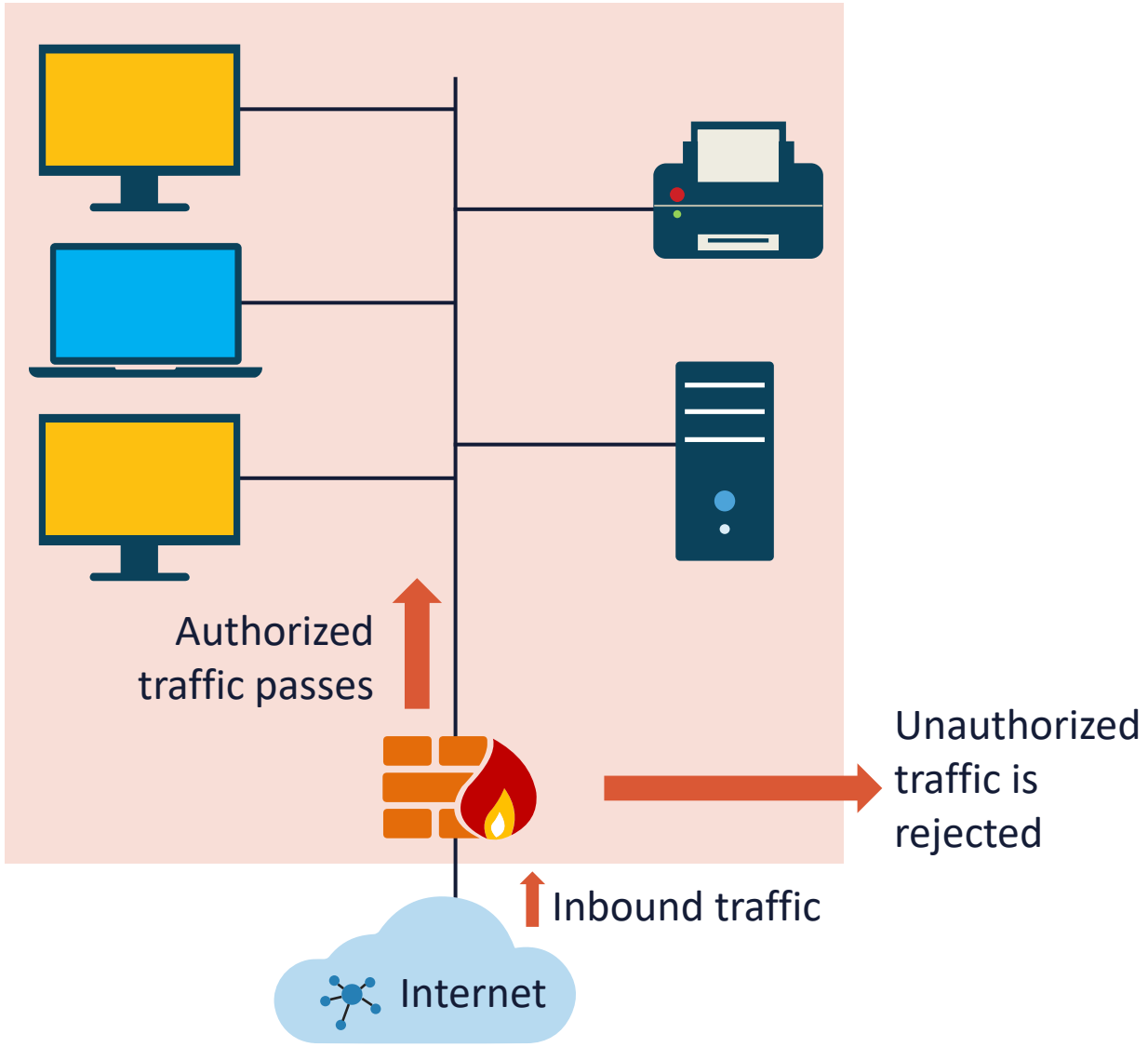
STATEFUL CLOUD-BASED FIREWALL



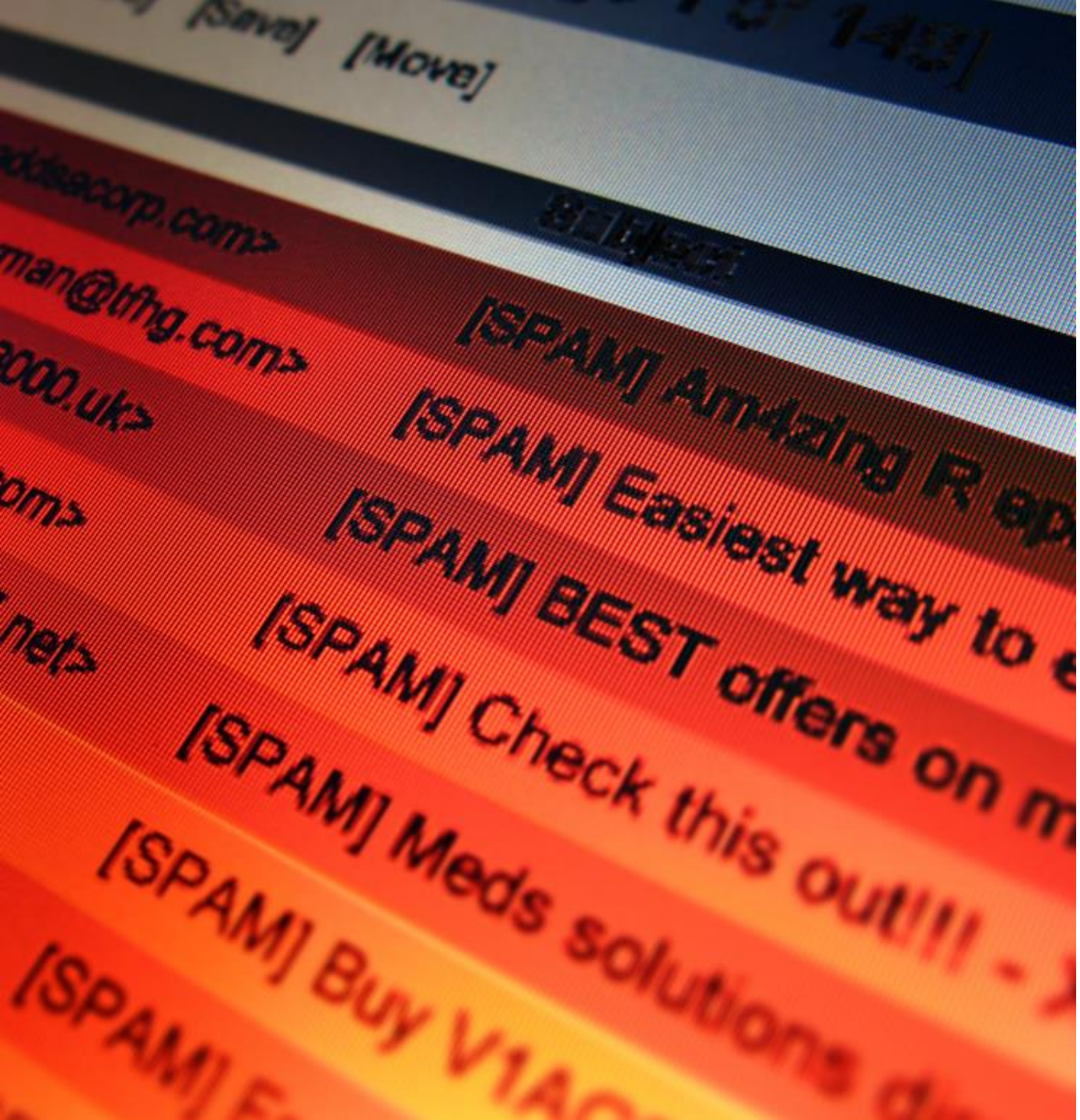
NEXT-GENERATION FIREWALLS

- A firewall is a metaphor representing software and/or hardware controls that can limit the damage spreading from one subnet, virtual local area network (VLAN), zone, or domain to another
- It is typically deployed as a barrier (zone interface point) between an internal (trusted) network and an external (untrusted) network
- They are integrated systems of threat defense functioning at layers 2-7 and can be categorized as network or application firewalls

NEXT-GENERATION FIREWALLS



- Layer 5-7 policies (deep packet inspection)
- Authentication proxy (interactive or transparent
- Identity services for ABAC and advanced identity management
- Integrated IDS/IPS (also cloud-based)
- Content security with URL filtering and data loss prevention (DLP)
- Cloud correlation and integration for advanced malware protection including ML and AI engines
- Botnet filtering for advanced distributed denial-of-service (DDoS) protection
- Unified threat management



UNIFIED THREAT MANAGEMENT

- Most modern networks transmit more than just basic data transit and email traffic
- UTM typically provides multiple security features and services on a single network device
- It can protect email, webmail, fax, voice, conferencing, streaming, peer-to-peer file transfer services, and more
- UTM could be considered the first huge step to evolve into modern next-generation firewall solutions

WEB APPLICATION FIREWALL (WAF)

- Also called a web security gateway (WSG), it is usually an appliance (physical or virtual), server plugin, or virtual firewall running in a hypervisor or cloud deployment
- It protects HTTP and HTTPS (TLS) traffic at layers 5 through 7 of the OSI reference model
- Typically, these rules cover common web attacks, such as cross-site scripting (XSS), request forgeries, and SQL injection
- Typically deployed as dynamically configured WebACLs and Anti-DDoS engines with other threat management services
- The AWS WAF is commonly deployed on an elastic application load balancer, CDN distribution, or API gateway

DEMO: EXAMINING VIRTUAL PRIVATE NETWORKS

In this demo…

we will describe a virtual private network (VPN)

DEMO: EXAMINING IPSEC

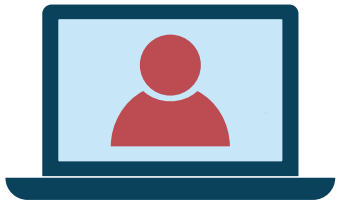
In this demo…

we will describe IP security (IPsec) for IPv4 and IPv6

TRANSPORT LAYER SECURITY (TLS)

- Transport Layer Security (TLS) is the latest iteration of SSL
- TLS is the most ubiquitous certificate-based peer authentication in use on the Internet (HTTPS)
- TLS 1.3 is the most recent published version and should always be used unless the client only supports version 1.2
- It includes a Record protocol and a highly extensible Handshake protocol
- It is also used with SMTP, Lightweight Directory Access Protocol (LDAP), and Post Office Protocol 3 (POP3)
- The only mandatory cipher suite includes RSA for authentication, AES for confidentiality, and SHA for integrity and digital signatures
- Although TCP-based, most servers perform single -packet authentication and mutual TLS instead

TRANSPORT LAYER SECURITY



TLS VPN tunnel

1. User makes a connection to TCP port 443

2. The server response contains server's public key

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

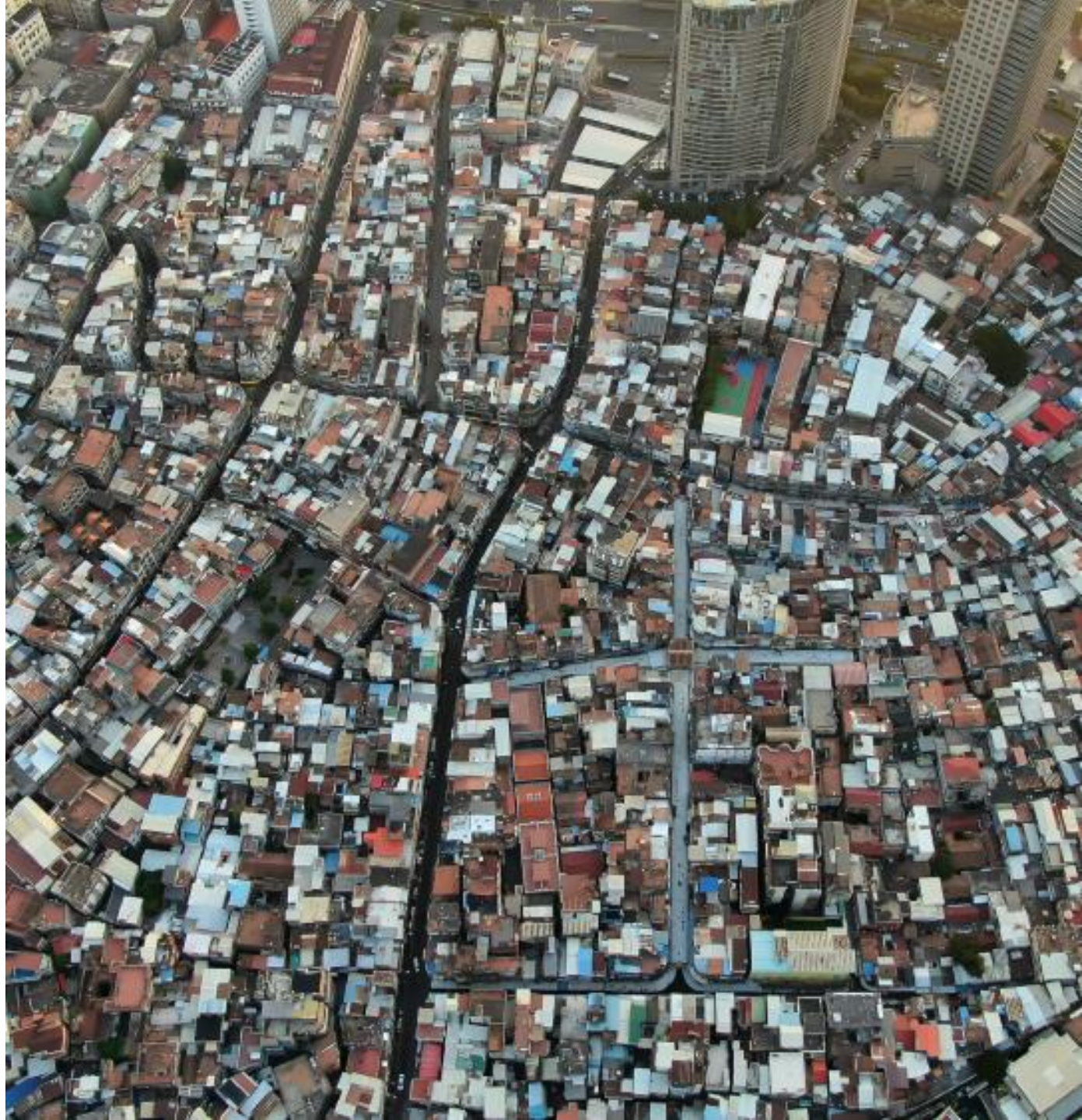
4. User software create a shared-secret key

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

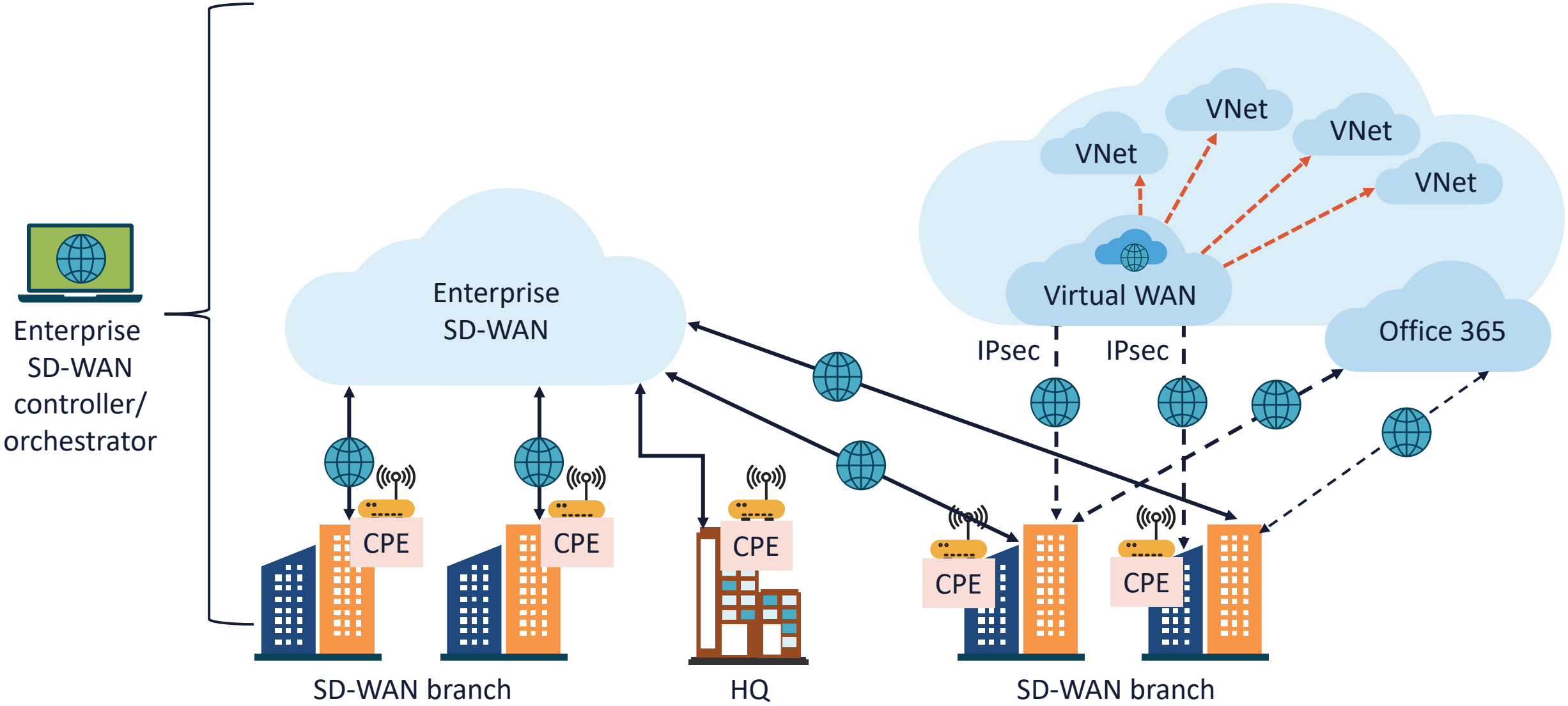
6. Bulk encryption occurs using the shared-secret key with a symmetric encryption algorithm

SD-WAN

- Software-defined wide area network (SD-WAN) is a software-defined networking (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
- SD-WAN incorporates a centralized control function with user-defined application and routing policies to deliver highly secure, robust, application-aware network traffic management
- It is also called SD-MAN for a metropolitan area network fiber deployment



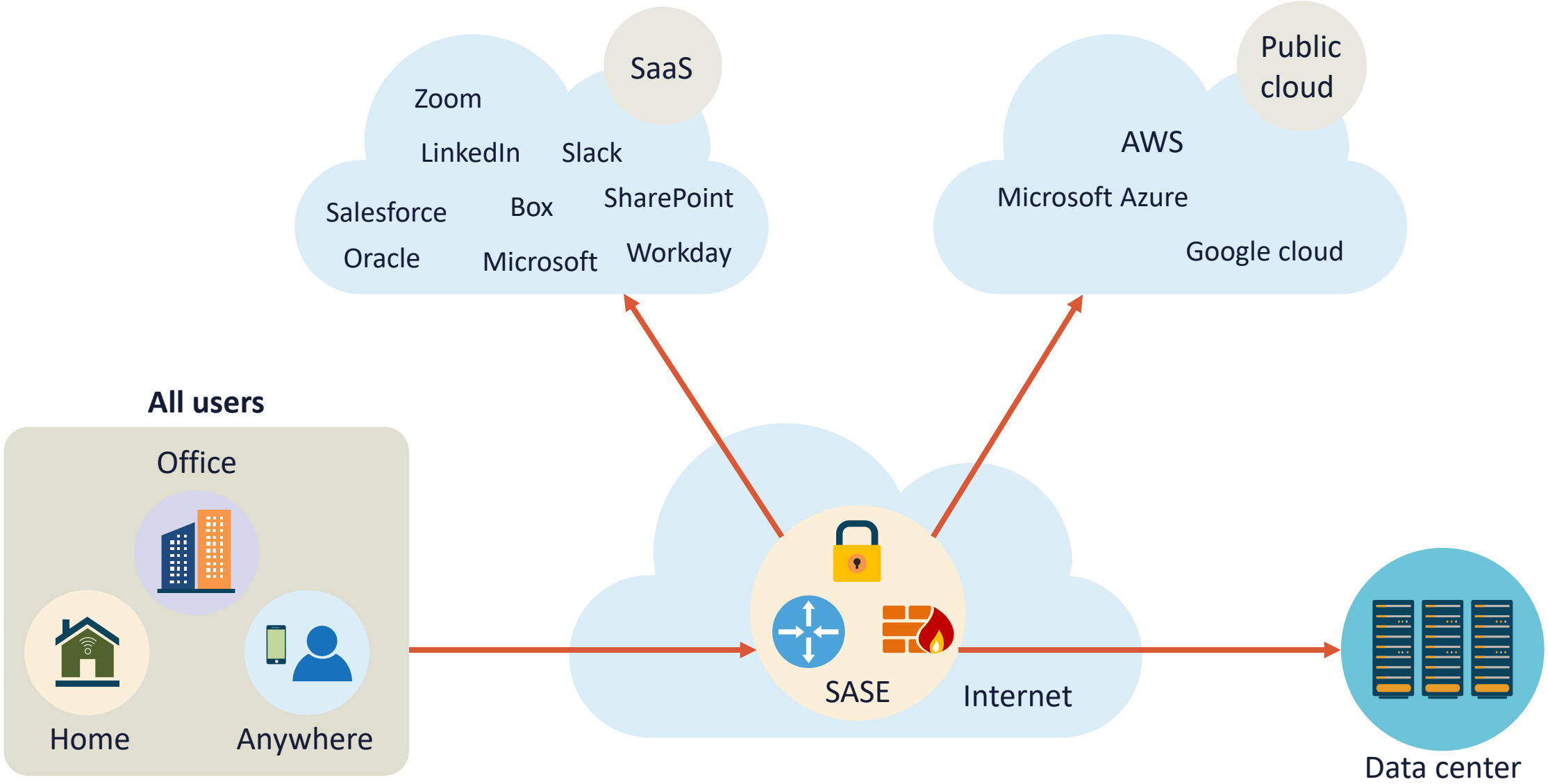
SD-WAN


Enterprise SD-WAN controller/ orchestrator
Enterprise SD-WAN
VNet
VNet
VNet
VNet
Virtual WAN
IPsec
IPsec
Office 365
CPE
CPE
CPE
CPE
CPE
SD-WAN branch
HQ
SD-WAN branch

SECURE ACCESS SERVICE EDGE (SASE)

- Secure access service edge (SASE) is an architecture that delivers converged network and Security as a Service (SaaS) capabilities including SD-WAN and cloud native security functions such as secure web gateways, cloud access security brokers, firewall as-a-service, and zero-trust network access (ZTNA)
- These functions are delivered from the cloud and provided as a service by the SASE vendor such as Cisco Systems or Fortinet

SASE


SaaS
Zoom
LinkedIn
Slack
Salesforce
Box
SharePoint
Oracle
Microsoft
Workday
Public cloud
AWS
Microsoft Azure
Google cloud
All users
Office
Home
Anywhere
SASE
Internet
Data center

DATA PROTECTION CONCEPTS AND STRATEGIES

Objectives

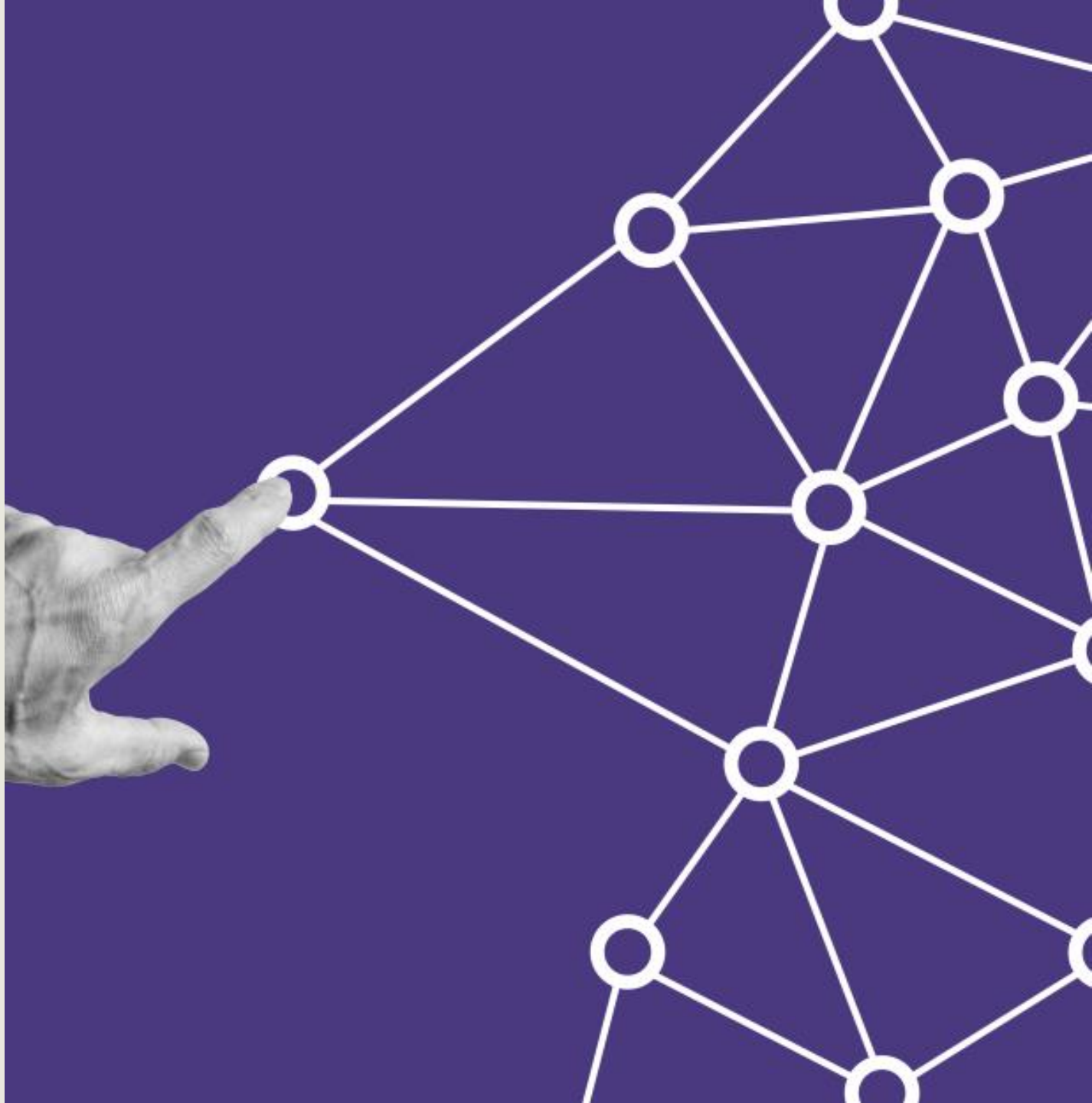
- Discover data states, classification, types, and life cycles
- Examine secure data considerations:
  - Geographic and cultural restrictions
  - Encryption and hashing
  - Masking, obfuscation, and tokenization
  - Segmentation and compartmentalization

DATA STATES: AT REST

- Data at rest is data that has arrived at a destination in a file system, database, or object storage (disk, tape) and is not being accessed or used
- It typically refers to stored data and excludes data that is moving across a network or is temporarily in computer memory or Redis cache waiting to be read or updated
- Data at rest is data that is not dynamically moving from device to device or network to network

DATA STATES: IN TRANSIT

- Data in transit is being packet forwarded or switched over a wireless or wired network in a unicast, broadcast, multicast, or anycast fashion
- Examples include:
  - Wired Ethernet
  - Cable (DOCSIS)
  - Fiber optic
  - 802.11 wireless
  - Cellular
  - Satellite
  - Personal area networking using RFID, Bluetooth, Infrared, Zigbee, and more



DATA STATES: IN USE

- This is active data undergoing processing, translation, analysis, change, or other manipulation
- Examples include:
  - Data in system RAM memory
  - CPU registers
  - Caches and buffers
  - Data in Memcached or Redis clusters
  - Database transactions
  - Cloud-based file or code being modified in real-time by one or more users

DATA CLASSIFICATIONS: GOVERNMENT AND MILITARY

- Sensitivity is based upon a calculation of the damage to privacy and security that an exposure of the information would cause
- **The US has three levels of classification: Confidential, Secret, and Top Secret**
- If one holds a Top Secret security clearance, they are allowed to handle information up to the level of Top Secret, including Secret and Confidential information
- If one holds a Secret clearance, they may only handle Secret and Confidential classified information – not Top Secret

DATA CLASSIFICATIONS: PUBLIC AND COMMERCIAL

- There are five common categories used for data classification in various business and commercial sectors:
  - Public data
  - Private data
  - Internal data
  - Confidential data
  - Restricted data

DATA CLASSIFICATIONS

PUBLIC

Public data may be important, but it is accessible to the public

Since this data is openly shared, it is the lowest level

PRIVATE

Private data requires a greater level of security than public data

It should not be available for public access and is often protected through common security measures such as passwords

INTERNAL

Internal data is usually limited to employees only and often has different security requirements that affect who can access it and how it can be used

DATA CLASSIFICATIONS

CONFIDENTIAL

This information should only be accessed by a limited audience that has obtained proper authorization using strict identity management

RESTRICTED

This classification is reserved for an organization's most sensitive information

Access to this data is strictly controlled to prevent its unauthorized use

DATA TYPES

Regulated data

Information that its use and protection is dictated by a government agency or third-party agreements

Trade secrets

Any practice or process of a company that is generally not known outside of the company

Intellectual property

Creations of the mind, such as inventions, literary and artistic works, designs and symbols, names, and images used in commerce

Personal health information (PHI)

The demographic information, medical histories, test and lab results, mental health conditions, insurance information, and other data

DATA TYPES

Personally identifiable information (PII)

Any representation of data that allows the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means

Legal information

Involves the careful reading about specific clauses or stipulations that does not constitute "advice"

Financial data

Quantitative information used by organizations to make financial decisions and data concerning a company's financial health and performance

Human and non-human readable

Some human-readable formats, such as PDF, are not machine-readable as they are not structured or semi-structured (JSON, YAML) data

THE DATA LIFE CYCLE

THE CREATE PHASE

- Data is either generated from scratch, inputted, acquired, purchased, or modified into another format
- The data owner, stewards, and custodians (if applicable) are identified in this earliest phase
- Other key activities of phase one include:
  - Data discovery
  - Data categorization
  - Data classification
  - Data mapping
  - Data labeling (tagging)

THE STORE PHASE

- The data is put onto a volume (block), object (blob), or file storage system or into one of several types of database systems
- This phase relates to the **optional** transactional, near-term usage data as opposed to long-term cold data storage
- Activities of this phase can also occur simultaneously when the data is generated in phase one
- Protection of data at rest and data in transit will often occur in this phase unless default encryption is implemented in the Create phase

THE USE PHASE

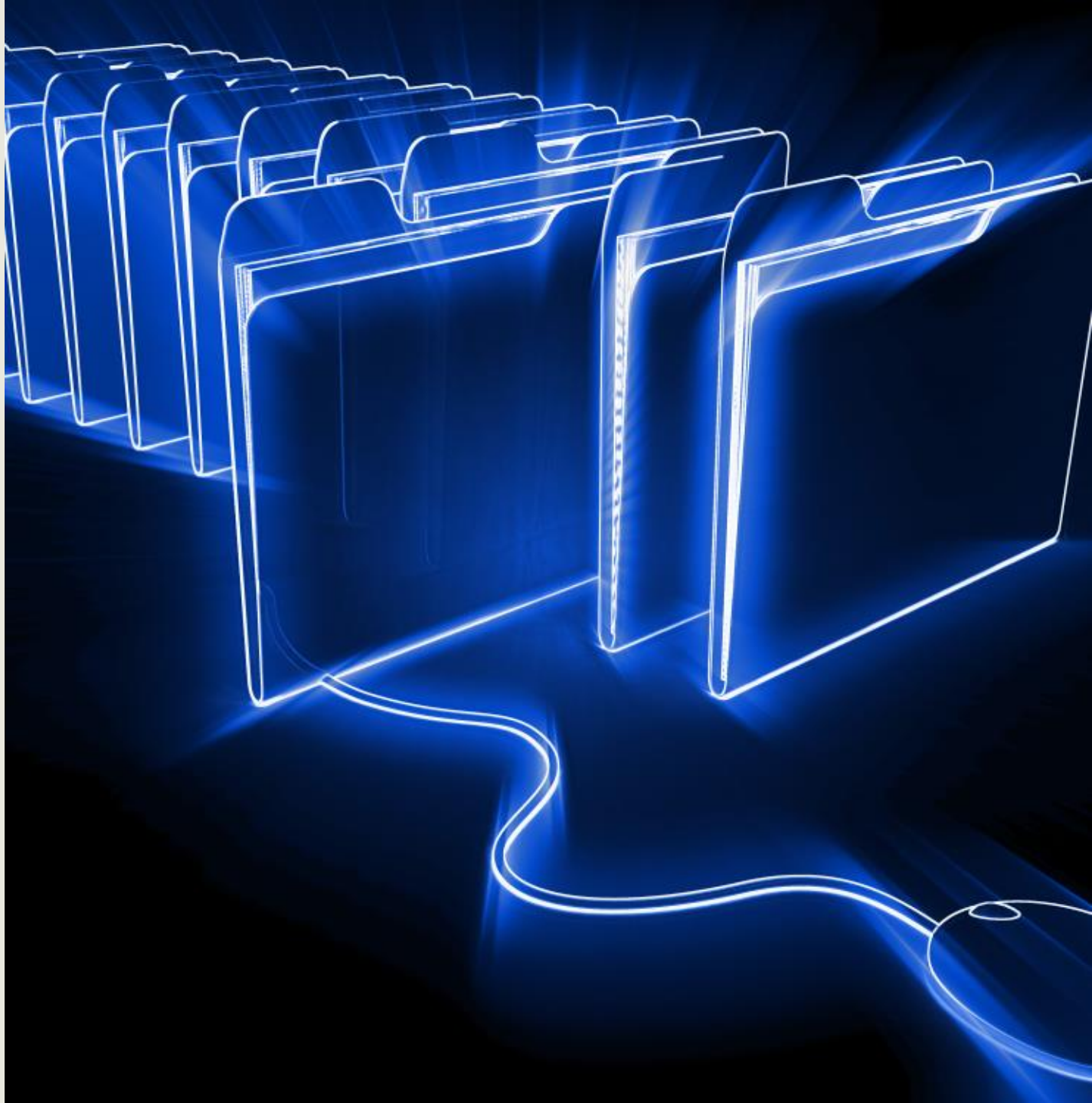
- In this **mandatory** phase, data is utilized by people, applications, services, and tools as well as being changed from the original state
- This is where raw data becomes information, then knowledge, then wisdom
- If data is used remotely then protection mechanisms must be in place (virtual private network (VPN), secure endpoints, digitally signed application protocol interface (API) calls)
- The systems that "use" the data must be secured as well; for example, endpoint detection and response (EDR) or host-based intrusion prevention system (IPS) agents (Palo Alto Cortex XDR)

THE SHARE PHASE

- In this **optional** phase, data is visible, analyzed, and apportioned among users, systems, and applications
- Data can be shared in a client-server, peer-to-peer, or distributed manner
  - Global collaboration and sharing of data introduces obvious risks and lack of control
- Most of the control used in the previous phases will be implemented here in phase four (such as information rights management (IRM) and data loss prevention (DLP) services)
- Stringent Identity and Access Management (IAM) and/or Identity Management (IdM) should be used to enforce the least privilege

THE ARCHIVE PHASE

- In this **optional** phase, data is stored for the long-term and removed from active usage
- Archiving is based on regulations, governance policies, and/or best practices
- Stringent cryptography will be introduced for data at rest – as in AES-GCM-256 AEAD solutions
- Archiving is often automated and based on Intelligent Tiering or Storage Gateway management over a high-speed connection to cloud providers
- Costs are based on retrieval options



THE DESTROY PHASE

- Data is no longer accessible or usable based on lifetime, utility, policy, governance, and/or regulations
- The organization should have their own established methods for disposal of data and media, often using military grade programs or physical destruction such as crushers and furnaces
- Although data can be disposed of using a variety of methods, when storing data at a cloud provider, crypto-shredding (cryptographic erasure) is the only practical and comprehensive solution

SECURING DATA: GEOGRAPHIC AND CULTURAL RESTRICTIONS

- A major value proposition of cloud computing and content distribution is the ability to store and share data to edge locations all over the world
- When storing or sharing data and content, all local laws and regulations must be considered and obeyed
- Attention must be paid to the right of privacy in different countries, as well as the presence or absence of a data protection law
  - There may be import/export laws or mandates such as General Data Protection Regulation (GDPR) data privacy in play

SECURING DATA: GEOGRAPHIC AND CULTURAL RESTRICTIONS

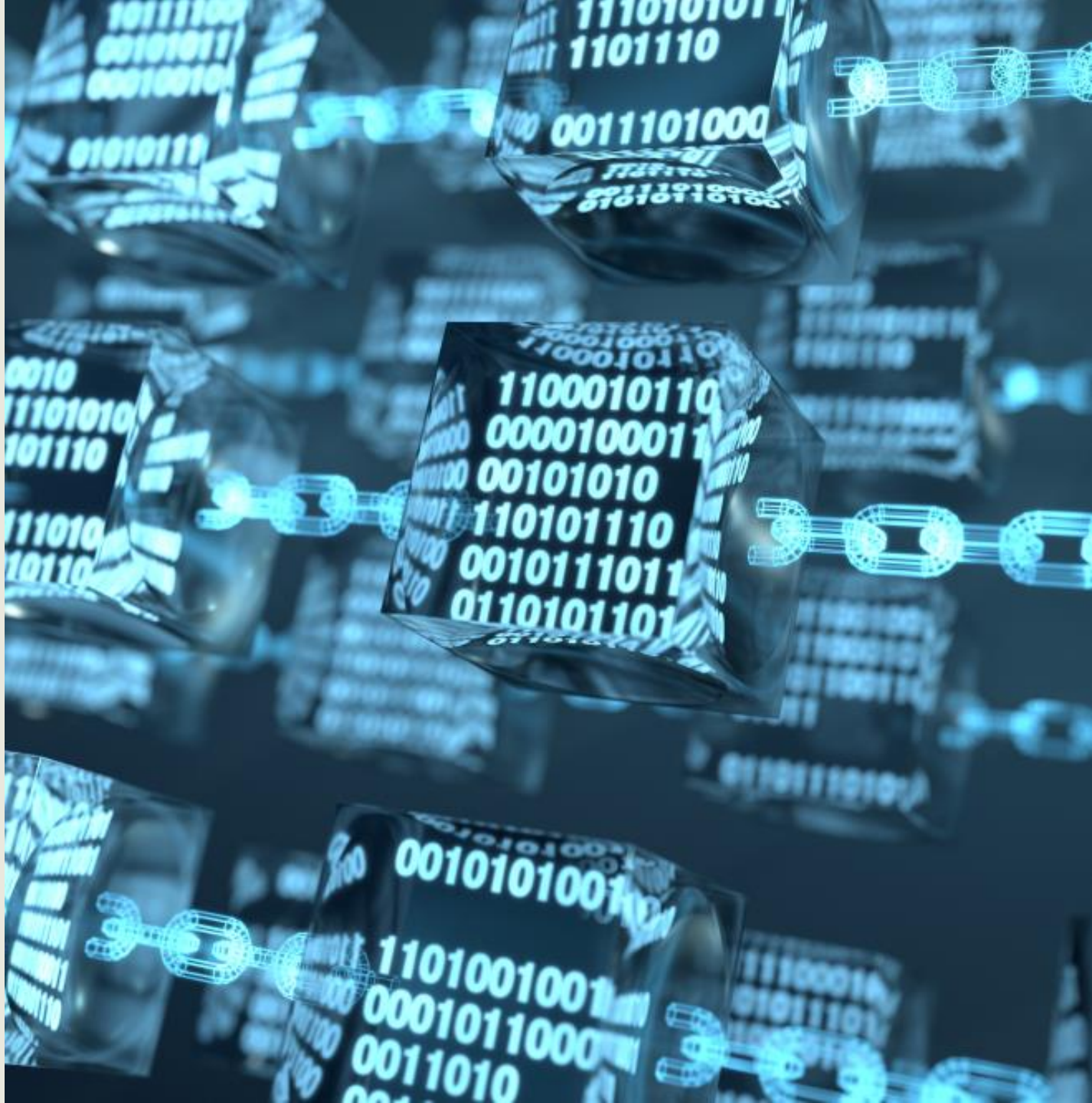
- It is a best practice to choose a safe country where the government is politically stable
- A data center should not be deployed in a location that has the potential for instability
- Data analysts and architects should consider the potential lower costs of raw materials, labor, energy costs, and taxation
- Cultural and religious norms and sensitivities must also be considered for the storage of data and the dissemination of content

SECURING DATA: CRYPTOGRAPHIC HASHING

- By hashing the data before storing it in a database, one can prevent unauthorized parties from reading or changing it without knowing the original data or the hashing algorithm
- It is common for systems like directory services to hash the passwords of users so that they can be verified without exposing the plain text
- Examples of trustworthy hashing algorithms for securing sensitive data in a database include SHA-256, SHA-512, bcrypt, scrypt, and PBKDF2

SECURING DATA: CRYPTOGRAPHIC HASHING

- Choose a hashing algorithm that meets all policy requirements and that is supported by tools and utilities
- Generate a salt for each data input that is hashed with a built-in function or library
- Hash the data input and salt with the chosen algorithm
  - It is essential to use the same hashing algorithm and salt for the same data input every time it is hashed
- Employ a secure connection to the data storage or database to offer protection of data-in-transit



SECURING DATA: ENCRYPTION

- Encryption at rest is encryption that is used to help protect data that is stored on a disk (including solid-state drives) or backup media
- All data that is stored by an organization, whether on-premises or in the cloud, should be encrypted at the storage layer using the Advanced Encryption Standard (AES) algorithm, AES-256

SECURING DATA: ENCRYPTION

- The separation of duties and least privilege principles should be applied to all subjects who are authorized to administer encryption policies and key management
- It is critical to remember that many drives that store data are removable and portable
  - Data at rest can also reside on removable memory cards
- A common solution for many organizations is to employ hardware security modules (HSMs), CloudHSM, and micro HSM on memory cards

SECURING DATA: OBFUSCATION

- Obfuscation is a generic term that applies to any mechanism that makes data less decipherable
- The goal is to render data unreadable or to hide aspects of personally identifiable, personal health, or corporate intellectual property information
  - "Obscuring" is a concept where static or dynamic techniques are used on the original data or a representational data set
  - "Shuffling" is a term that describes utilizing characters from the same data set to further present the data
  - "Randomization" is when all or some of the data is replaced with indiscriminate characters

SECURING DATA: MASKING

- Data masking often involves using characters like "X" to hide some or all data
- Example is to only display the last four digits of:
  - Social security number
  - Credit card number
  - National ID number
  - Bank account number
  - Username or email address
- Masking is considered a suboptimal data obfuscation method since it is subject to inference

SECURING DATA: TOKENIZATION

- Tokenization involves sending sensitive data through an API call (or batch file) to a system or cloud provider service that replaces the data with non-sensitive, pseudorandom placeholders called tokens
- Unlike encrypted data, the tokenized data is irreversible and unintelligible
- The practice involves two distinct databases
  - One with the actual sensitive data
  - One with tokens mapped to each chunk of data

TOKENIZATION

Sensitive data held by government

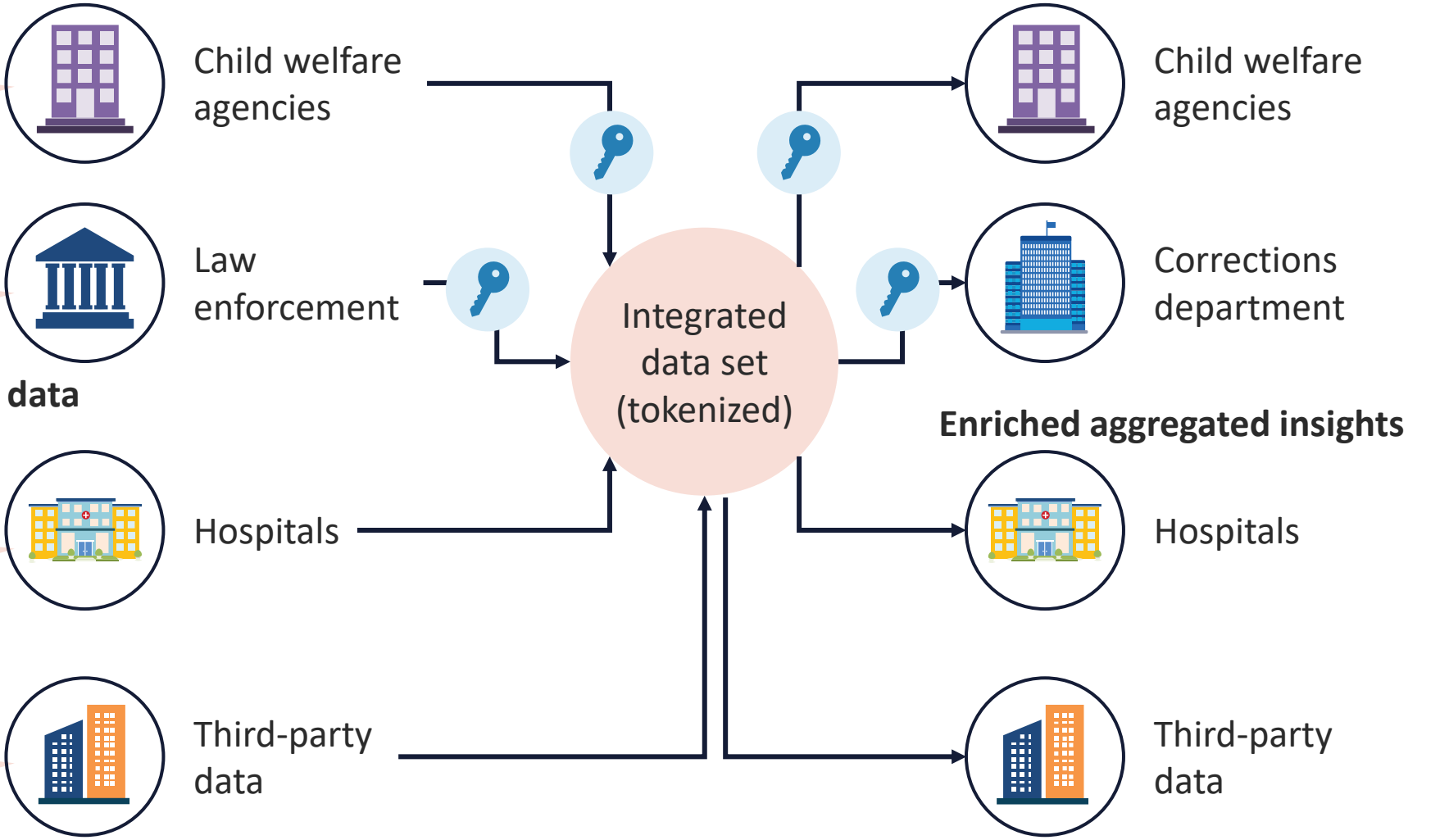
- Substance use in families
- Treatment cost and effectiveness

- Arrest and parole information
- Geographical crime data

Non-sensitive publicly available data

- Aggregated treatments data
- Aggregated prescriptions data

- Marketing data
- Spending and insurance information



SECURING DATA: SEGMENTATION

- Data segmentation is a process of dividing and organizing data and information into defined groups to enable:
  - Handling
  - Labeling
  - Sorting
  - Viewing
  - Securing
- Segmented data offers a team or group with segregated, clear, actionable information

SECURING DATA: SEGMENTATION

- Data segmentation involves grouping data into at least two subsets, although more separations may be necessary on a large network with sensitive data
- Data should be grouped based on:
  - Use cases
  - Types of information
  - Sensitivity levels
  - Separation of duties policies
  - Level of authority for access to that type of information

SECURING DATA: COMPARTMENTALIZATION

- Compartmentalization is regarded as a very powerful way to protect personal information
- It involves limiting access to information to only those people or organizations who need it to perform a certain task
- Originating in the military with classified information, the concept can be further understood with another military term: "managing the blast radius"
- Compartmentalization is equally about:
  - Spreading the risk so if there is any impact (breach), the damage is limited
  - Lowering the effect of recovery efforts