10.1 Cloud computing and deployment models

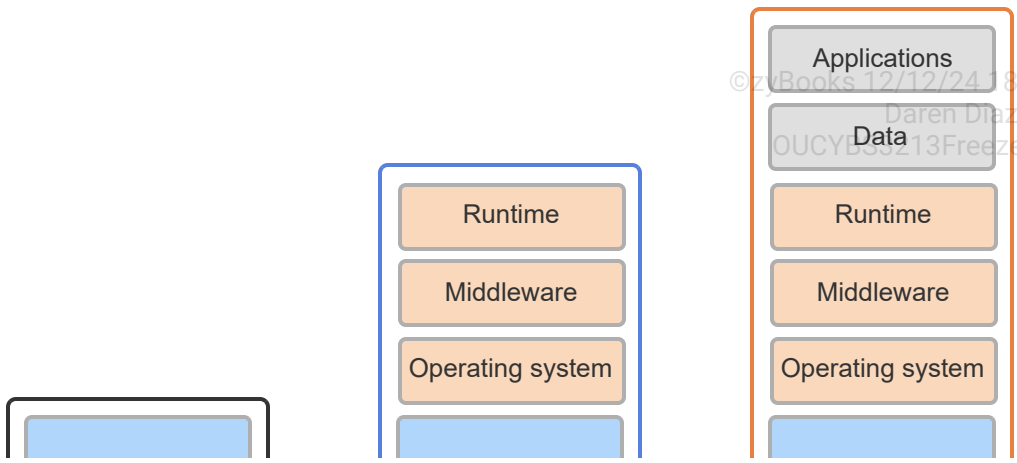
Cloud computing

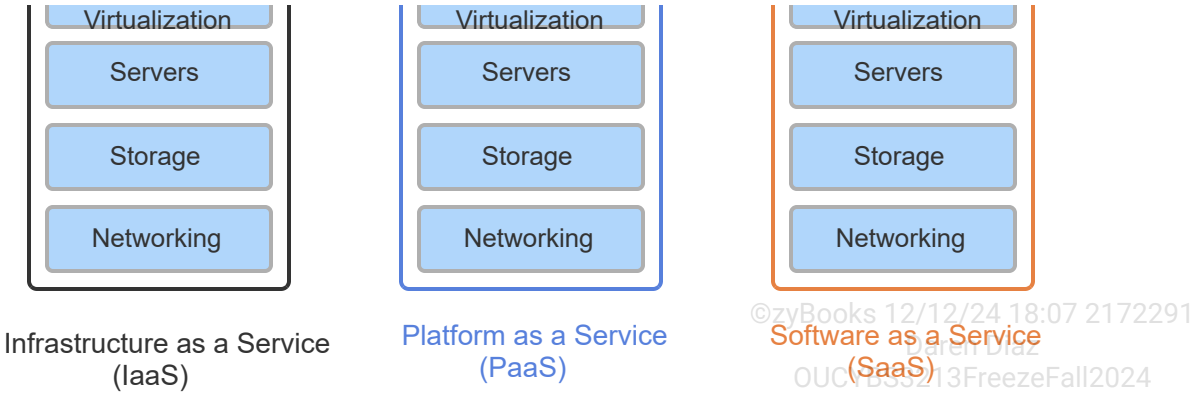
Cloud computing is a computing model where IT resources are offered on-demand over the Internet. A ***cloud service provider***, or ***cloud provider***, is an entity that offers cloud computing. Ex: Microsoft is a cloud service provider that offers the Azure cloud computing service over the Internet. Three cloud computing models exist:

- ***Infrastructure as a Service (IaaS)*** is a cloud computing model that offers infrastructure components on-demand. Infrastructure components include networking, storage, servers, and virtualization. Ex: Google Compute Engine (GCE) is the IaaS component of Google Cloud Platform (GCP).
- ***Platform as a Service (PaaS)*** is a cloud computing model that offers hardware and software tools for application development and deployment. PaaS includes networking, storage, servers, and virtualization, as well as operating system, middleware, and runtime components. Ex: Google App Engine is a PaaS offered by Google for developing and hosting web applications in Google-managed data centers.
- ***Software as a Service (SaaS)*** is a cloud computing model that offers a software application over the Internet. A SaaS provider manages access to applications and data, and is responsible for application security, availability, and performance. Ex: Gmail is a SaaS email service by Google.

Anything as a Service (XaaS) is a term referring to products, tools, and technologies that are offered as a service over the Internet. Ex: A Communications as a Service (CaaS) cloud provider may offer Voice over IP (VoIP) and video conferencing services over the Internet.

PARTICIPATION ACTIVITY 10.1.1: Cloud computing models.





Animation content:

Static image: A box labeled "Infrastructure as a Service (IaaS)" contains blue boxes labeled "Virtualization", "Servers", "Storage", and "Networking". A box labeled "Platform as a Service (PaaS)" contains the blue boxes from IaaS. PaaS also contains orange boxes labeled "Runtime", "Middleware", and "Operating system". A box labeled "Software as a Service (SaaS)" contains the blue boxes from IaaS and the orange boxes from PaaS. SaaS also includes gray boxes labeled "Applications" and "Data".

Animation captions:

1. Infrastructure as a service (IaaS) offers networking, storage, servers, and virtualization.
2. In addition to the components offered by IaaS, Platform as a Service (PaaS) offers operating system, middleware, and runtime components.
3. Software as a service (SaaS) offers software applications over the Internet. SaaS includes IaaS and PaaS components.

PARTICIPATION ACTIVITY 10.1.2: Cloud computing models.

How to use this tool

SaaS IaaS PaaS

	A cloud provider offers an inventory management application over the Internet

	A cloud provider offers infrastructure components, but not software tools necessary for application development
	A cloud provider offers all the components necessary to build applications

Reset

PARTICIPATION ACTIVITY 10.1.3: Cloud computing models.

Select the cloud computing model in each scenario.

1) A cloud provider is responsible for the security, availability, and performance of an enterprise resource planning (ERP) application offered by the cloud provider.
   - IaaS
   - PaaS
   - SaaS

2) A cloud provider offers Windows Server 2022, software libraries, and runtime components, but not software applications.
   - IaaS
   - PaaS
   - SaaS

3) A cloud provider offers the mySQL database and C++ compilers for application development and deployment.
   - IaaS
   - PaaS
   - SaaS

4) A cloud provider offers a payroll management system.

- IaaS
- PaaS
- SaaS

Cloud deployment models

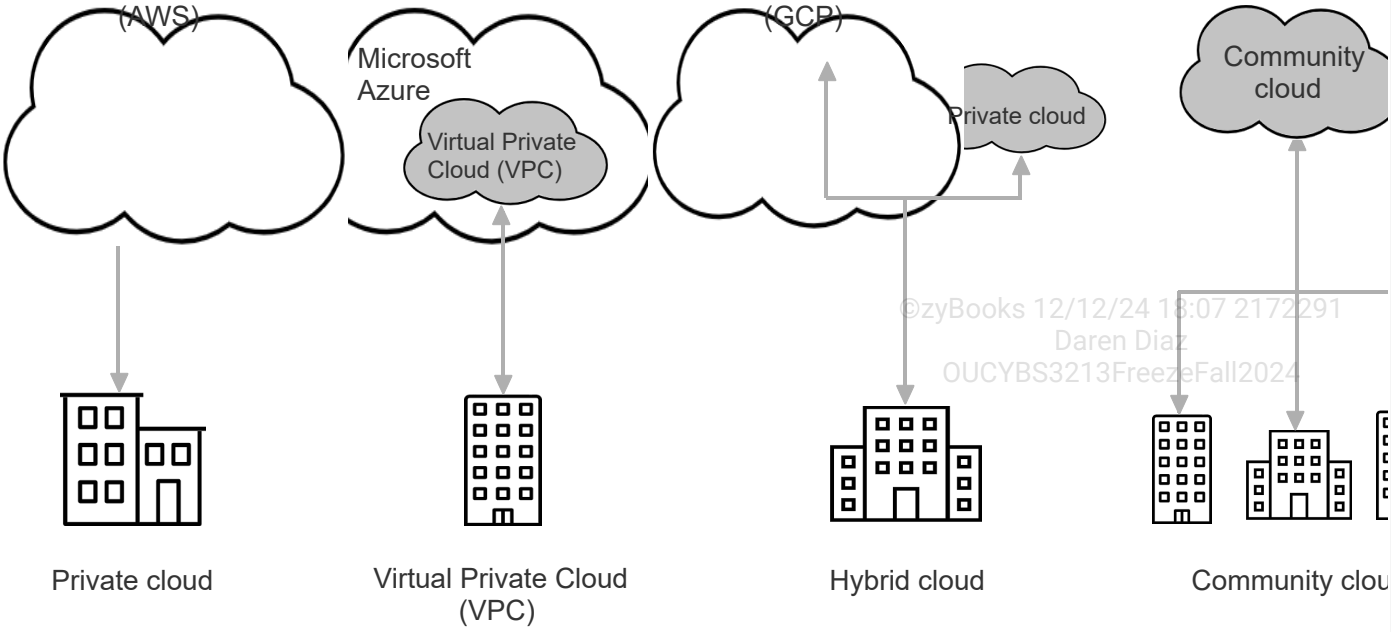
A cloud deployment model identifies the cloud architecture, scalability, ownership, and control, as well as how the cloud services are made available to users. Four cloud deployment models exist:

- A ***public cloud*** is a cloud deployment model where the cloud infrastructure is provisioned for use by the general public. A public cloud exists on the cloud provider's premises and is accessible over the Internet. A public cloud is commonly offered as a pay-per-use service. Ex: Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure are public clouds.
- A ***private cloud*** is a cloud deployment model where the cloud infrastructure is provisioned for exclusive use by a single organization. A private cloud may be managed and operated by the organization that owns the private cloud, or by a third-party. A private cloud may exist on an organization's on-premises infrastructure or off-premises. A ***virtual private cloud (VPC)*** is a private cloud where the cloud infrastructure resides within a public cloud.
- A ***hybrid cloud*** is a cloud deployment model where the cloud infrastructure from private and public clouds are bound together by standardized or proprietary technologies. A hybrid cloud enables the sharing of data and applications between different cloud deployments. Ex: An organization may store sensitive client data on a private cloud and a business intelligence application on a public cloud and interconnect the two using a hybrid cloud.
- A ***community cloud*** is a cloud deployment model where the cloud infrastructure is provisioned for exclusive use by organizations with common computing concerns. A computing concern may be regulatory compliance, performance, and security requirements. A community cloud may be owned, managed, and operated by the organizations in the community, or by a managed service provider (MSP). A community cloud may exist on or off an organizations' premises.

PARTICIPATION ACTIVITY 10.1.4: Cloud deployment models.

Amazon Web Services

Google Cloud Platform



Animation content:

Static image: Representations of five cloud deployment models. The first is "Public cloud" represented by a cloud labeled "Amazon Web Services (AWS)". The second is "Private cloud" represented by a single office building connected to a cloud labeled "Private cloud". The third is "Virtual Private Cloud (VPC)" represented by a single office building connected to a cloud labeled "Virtual Private Cloud (VPC)" within a larger cloud labeled "Microsoft Azure". The fourth is "Hybrid cloud" represented by a single office building connected to a cloud labeled "Google Cloud Platform (GCP)" and another cloud labeled "Private cloud". The fifth is "Community cloud" represented by three office buildings pointing to a single cloud labeled "Community cloud".

Animation captions:

1. A public cloud is provisioned for use by the general public. Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) are public clouds.
2. A private cloud is provisioned for exclusive use by a single organization. A private cloud may be on or off an organization's premises.
3. A virtual private cloud (VPC) is a private cloud where the cloud infrastructure resides within a public cloud.
4. A hybrid cloud binds infrastructure from private and public clouds together by standardized or proprietary technologies.
5. A community cloud is provisioned for exclusive use by organizations with common computing concerns.

PARTICIPATION ACTIVITY

10.1.5: Cloud deployment models.

How to use this tool

Community cloud | **Private cloud** | **Virtual private cloud** | **Hybrid cloud** | **Public**

	Cloud infrastructure can only be used by the cloud owner
	Cloud infrastructure can be used on a pay-per-use basis by the general public
	Cloud infrastructure consisting of public and private clouds
	Cloud infrastructure resides within a public cloud and can only be used by a single organization
	Cloud infrastructure can only be used by organizations with common computing concerns

Reset

PARTICIPATION ACTIVITY 10.1.6: Cloud deployment models.

Select the cloud deployment model in each scenario

1) Several health care organizations create a cloud infrastructure to comply with the requirements of the health insurance portability and accountability act (HIPAA) on personal medical records.
   - ○ Public
   - ○ Private
   - ○ Community

- Hybrid

2) An organization creates a cloud infrastructure on the organization's premises for exclusive use by the organization's employees.
   - Public
   - Private
   - Community
   - Hybrid

3) An organization creates a cloud infrastructure to use a marketing application offered on a public cloud with the organization's client data stored on the organization's private cloud.
   - Public
   - Private
   - Community
   - Hybrid

4) An organization accesses cloud resources the organization does not own as a pay-per-use service.
   - Public
   - Private
   - Community
   - Hybrid

Fog and edge computing

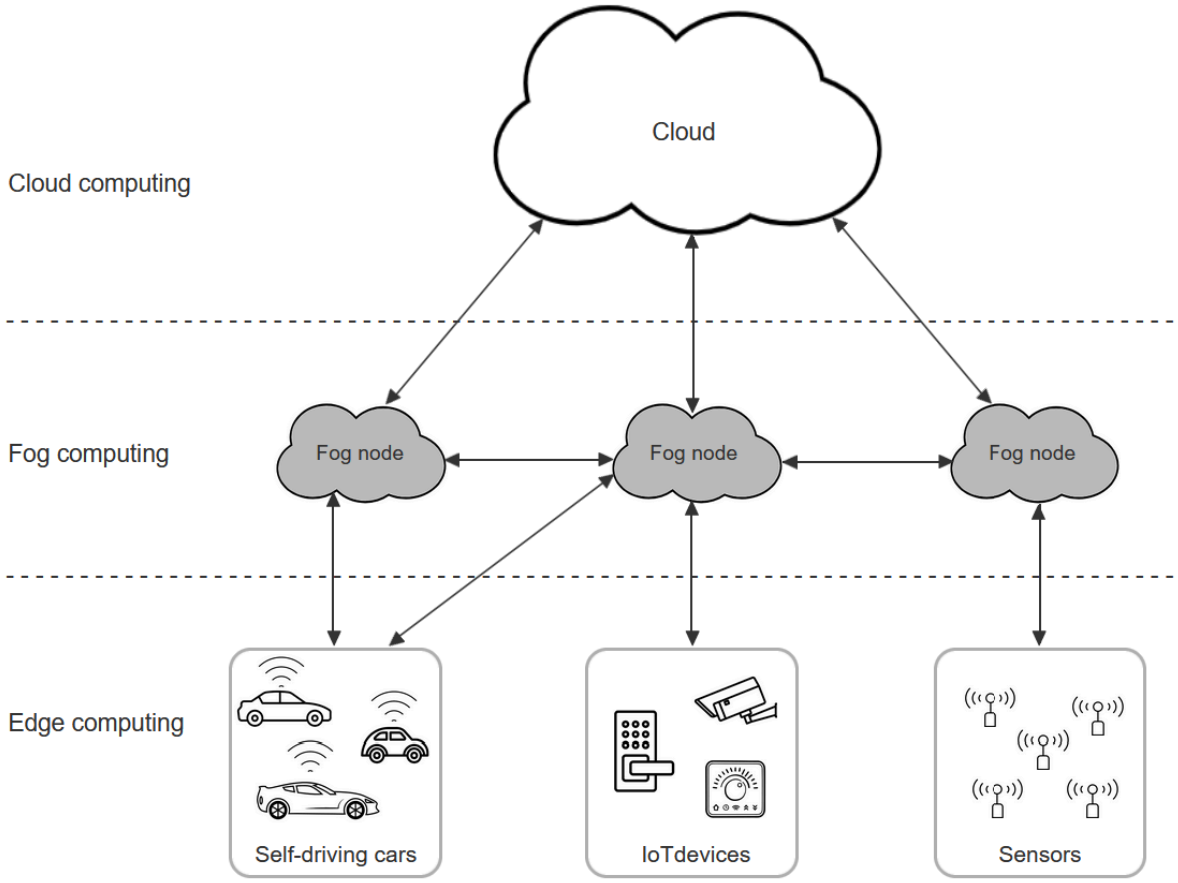
Fog computing, also known as ***fog networking***, or ***fogging***, is a decentralized computing infrastructure that extends the cloud through the placement of nodes between the cloud and end devices. A ***node***, or ***fog node***, is a non-end device with computing, storage, and network connectivity. Fog nodes reduce cloud latency (the delay in sending and receiving data to and from the cloud) by processing data near the end devices, enabling near real-time decision making. In fog computing, data is sent to the cloud only for storage and long-term analytics.

Edge computing is a computing model where most of the data processing is performed at end devices. Edge computing minimizes the need to send data to a node or the cloud, thereby increasing

application responsiveness, reducing bandwidth usage, and improving latency. Ex: Edge computing is used in the manufacturing industry for monitoring and detecting production errors using sensors and performing real-time analytics for improving product quality.

Different computing models may be used to address an application's requirements. Ex: A self-driving car uses on-board devices to analyze real-time data for car navigation (edge computing), and uses fog nodes for low-latency data exchange with nearby cars to ensure safe driving (fog computing). Fog nodes send data to the cloud for long-term analytics aimed at improving car maintenance or tracking car usage (cloud computing).

Figure 10.1.1: Cloud, fog, and edge computing.



PARTICIPATION ACTIVITY 10.1.7: Fog and edge computing.

1) How does fog computing reduce cloud latency?

- By using powerful processors at each fog node

- By performing most data processing at end devices
- By placing fog nodes near to end devices

2) In which computing model is most of the data processing performed at the end devices?
   - Cloud
   - Fog
   - Edge

3) Which computing model is better suited for an application that analyzes the impact of weather on crops over several years?
   - Cloud
   - Fog
   - Edge

4) A smart grid uses smart meters to match electricity supply with demand in near real-time. How can fog computing be used in a smart grid?
   - Fog nodes can collect and send meter data to the cloud for near real-time electricity supply adjustments and billing
   - Fog nodes can collect meter data, adjust electricity supply in coordination with other fog nodes in near real-time, and perform billing operations
   - Fog nodes can collect meter data, adjust electricity supply in coordination with other fog nodes in near real-time, and send usage data for billing to the cloud

©zyBooks 12/12/24 18:07 2172291
Daren Diaz
OUCYBS3213FreezeFall2024

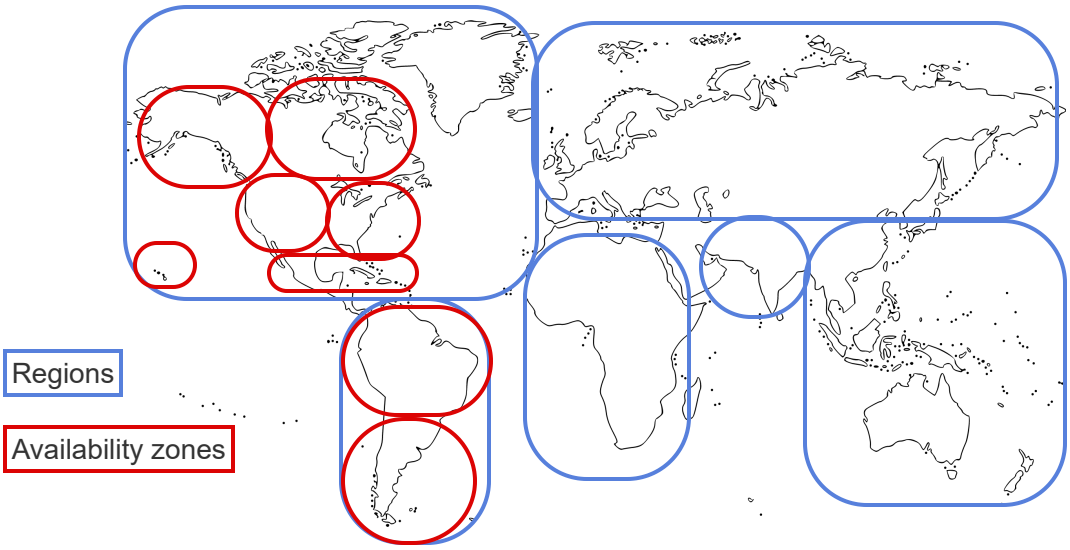
Cloud regions and availability zones

A cloud resource is a physical device located in a cloud service provider's data centers. Cloud service providers organize data center locations and cloud resource availability into regions and zones:

- A ***region*** is the physical location of a cloud service provider's cluster of data centers. Ex: Amazon Web Services (AWS) has over 20 regions, including North America, South America, Europe, China, Asia Pacific, South Africa, and the Middle East.
- An ***availability zone (AZ)***, or ***zone***, is a smaller group of data centers within a region. Ex: AWS has over 80 AZs, including Ohio (North America), Rio de Janeiro (South America), Cape Town (South Africa), London (Europe), Bahrain (Middle East), and Beijing (China).

Different regions offer different services in terms of performance, cost, and latency. Each region is isolated from other regions for fault tolerance and service stability. Each region's availability zones are built with fault tolerance and disaster recovery solutions. No single data center is shared between availability zones.

PARTICIPATION ACTIVITY 10.1.8: Cloud regions and availability zones.



Animation content:

Static image: A world map split into regions indicated by blue boxes. The regions shown include North America, South America, Europe and Northern Asia, Africa, Southeast Asia, and Southwest Asia and Australia. Availability zones are indicated by red circles within the North America and South America regions. Availability zones in North America include Hawaii, Alaska and Western Canada, Eastern Canada, the Western United States, the Eastern United States, and Central America. Availability zones in South America include the northern half of South America and the southern half of South America.

Animation captions:

1. A region is the physical location of a cluster of data centers. A cloud service provider may use a continental map as a reference when defining regions.
2. Availability zones are smaller data center groups within a region. A zone's data centers have increased redundancy and connectivity to meet customer demand within a region.

PARTICIPATION ACTIVITY 10.1.9: Cloud regions and availability zones.

1) Which is a physical device located in a cloud service provider's data center?
   - Guest machine
   - Hypervisor
   - Cloud resource

2) Which term describes a cloud service provider's cluster of data centers?
   - LAN
   - Region
   - Availability zone

3) What is a smaller group of data centers within a region known as?
   - AZ
   - DMZ
   - Security zone

4) Which security control is provided by region isolation?
   - Disaster recovery
   - Service stability
   - Encryption

Multi-cloud systems

*A **multi-cloud system** is a network architecture that integrates cloud services from multiple providers to meet diverse requirements for performance, reliability, and cost-effectiveness. A multi-cloud system allows an organization to avoid vendor lock-in, enhance disaster recovery capabilities, and optimize workload deployment based on the*

strengths of each cloud provider. By distributing assets across different clouds, multi-cloud environments can also increase resilience against service outages and regional disruptions.

CHALLENGE ACTIVITY | 10.1.1: Cloud computing and deployment models.

581480.4344582.qx3zqy7

Start

Select the cloud computing model described in each scenario.

Pick Enables customers to manage the applications, operating systems, and data

Pick Offers a Human Resource Management (HRM) solution as a service which stream recruiting, onboarding, and benefits administration

Pick Provides the scalable resources needed to process and analyze large datasets

Pick Provides a platform for developers to build, test, and deploy applications quickly an

1 2 3

Check Next

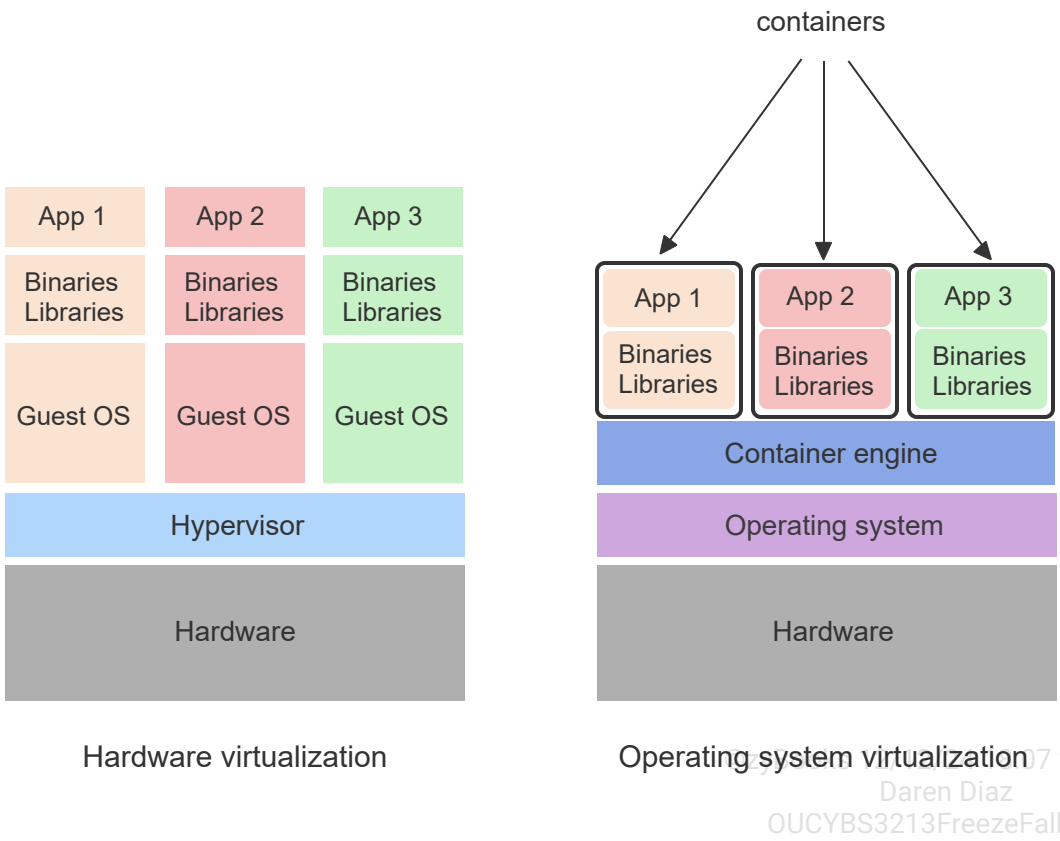
10.2 Containers, serverless, and microservices architectures

Containers

A ***container*** is a package of software that has all the necessary elements to run an application, including code, libraries, system tools, and configurations. A container decouples an application from the underlying hardware. A container can run on any environment. Ex: Virtual machines, physical servers, on-premises data centers, and public clouds. A ***container engine*** is a program that manages the execution of containers. Ex: Dockers is a container engine.

Unlike a virtual machine that virtualizes the hardware, a container engine virtualizes the operating system. Compared to a virtual machine, a container is lightweight and efficient because the container does not need to boot an operating system or load any libraries. A container is defined for a specific operating system. Ex: A containerized Windows application can only run on Windows.

PARTICIPATION ACTIVITY 10.2.1: Containers.



Hardware virtualization

Operating system virtualization

Animation content:

Static image: The left side is a representation of hardware virtualization. The bottom is a gray rectangle labeled "Hardware". A blue rectangle labeled "Hypervisor" sits on top of the hardware. Three boxes, each labeled "Guest OS", sit on top of the hypervisor in a single row. The next row is

three boxes labeled "Binaries, Libraries" on top of each Guest OS. The top row shows boxes labeled "App 1", "App 2", and "App 3". The right side is a representation of operating system virtualization. The bottom is a gray rectangle labeled "Hardware". A purple rectangle labeled "Operating system" sits on top of the hardware. A dark blue rectangle labeled "Container engine" sits on top of the operating system. Three containers sit on top of the container engine in a single row. The left container has boxes labeled "App 1" and "Binaries, Libraries". The middle container has boxes labeled "App 2" and "Binaries, Libraries". The right container has boxes labeled "App 3" and "Binaries, Libraries".

Animation captions:

1. In hardware virtualization, a hypervisor presents the guest operating systems with a virtual operating platform. A hypervisor manages the execution of the guest operating systems.
2. Each application uses the guest operating system's services, run-time libraries, and other environment-specific components to run.
3. In operating system virtualization, one operating system allows the existence of multiple isolated user space instances.
4. A container engine manages the execution of containers on the same operating system. Containers have no dependencies on the underlying hardware (containers are decoupled from the hardware).

PARTICIPATION ACTIVITY 10.2.2: Containers.

1) Which issue may be resolved by a containerized Python application?

- Running a Python application on a server that does not have enough memory
- Running a Python application with an older version of the Python interpreter
- Running a Python application programmed for Windows, in Linux.

2) How does a container enable a legacy application relying on an old C library to run in any environment?

- By modifying the legacy application to run without the old C library

- By removing the legacy application's dependencies on the old C library
- By packaging the old C library with the legacy application

3) A containerized application runs faster than the same application on a virtual machine because _____.

- a containerized application runs on a dedicated machine
- a virtual machine may not have all the required libraries to run the application
- hardware emulation is not used to run a containerized application

Serverless and microservices architecture

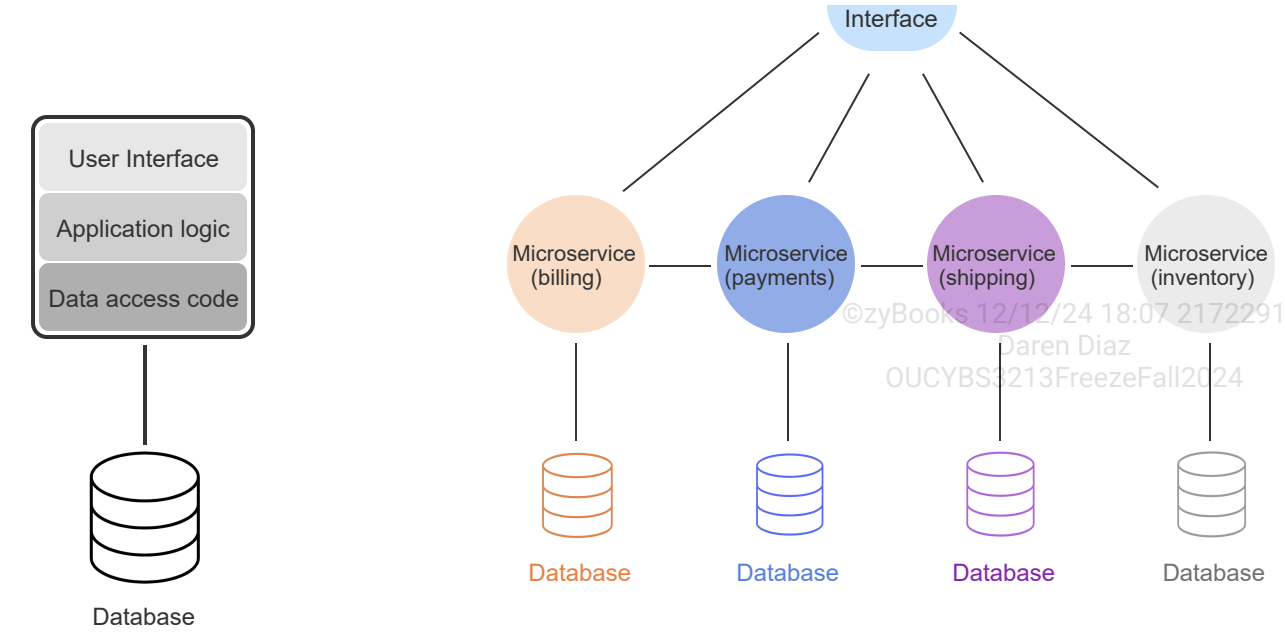
Containers support modern development and application patterns such as serverless and microservices architectures. ***Serverless***, also known as ***serverless architecture***, is a cloud computing model that automatically provisions and scales computing resources. Serverless architecture delegates all management responsibilities such as provisioning, scheduling, and scaling of the cloud infrastructure to the cloud provider. Ex: Amazon Web Services (AWS) Lambda, Microsoft Azure Functions, and Google Cloud Functions are serverless cloud services.

Microservices, also known as ***microservices architecture***, is a software design approach that breaks up an application into smaller, independently deployable components or services. Microservices have a technology stack, inclusive of database and data models, and communicate with each other using APIs. Microservices enable automated, iterative delivery methodologies such as continuous integration/continuous deployment (CI/CD) or DevOps.

Microservices are typically deployed inside containers and are used in real-time data processing applications. Ex: A traffic control or e-banking system that operates in real-time benefits from highly available, lightweight, and scalable microservices.

PARTICIPATION ACTIVITY 10.2.3: Microservices architecture.

User



Monolithic architecture

Microservices architecture

Animation content:

Static image: The left side shows a representation of monolithic architecture. A database is connected to a box containing "User Interface", "Application logic", and "Data access code". The right side shows a representation of microservices architecture. Four databases each connect to a different circle. The circles are labeled "Microservice (billing)", "Microservice (payments)", "Microservice (shipping)", and "Microservice (inventory)". Connections are shown between the microservices. Each microservice circle connects to a single circle labeled "User Interface".

Animation captions:

1. A monolithic application combines the user interface, data access code, and application logic into a single program. Ex: A monolithic e-commerce application is self-contained.
2. In microservices architecture, an application is broken up into smaller services (microservices). Each microservice implements a specific application function. Ex: Billing, payments, shipping, and inventory.
3. Each microservice uses a separate, independent database.
4. Microservices communicate with each other and with the user interface using APIs.

PARTICIPATION ACTIVITY 10.2.4: Serverless and microservices architecture.

1) In which cloud computing model is a cloud provider responsible for scaling computing resources?

- Microservices
- IaaS
- Serverless

2) Which is true for an application based on monolithic architecture?

- The smaller components of the monolithic application use messages to communicate with each other.
- The monolithic application is more scalable than a microservices-based application.
- The monolithic application is built as a single unit.

3) A microservices-based application can be updated without disrupting the entire application because _____.

- application functions operate as one large service
- multiple application instances run at the same time
- application functions operate as independent services

Platform diversity

Platform diversity *refers to the strategic deployment of different application components across various execution environments optimized for specific tasks. Container platforms provide scalability and isolation, serverless architectures offer cost efficiency and dynamic scaling, and microservices on diverse infrastructures enhance performance and resilience. Deploying each application component in the most suitable environment improves system efficiency, reduces platform-specific vulnerabilities, and leads to a more robust and reliable application.*

10.3 Virtualization

Virtualization

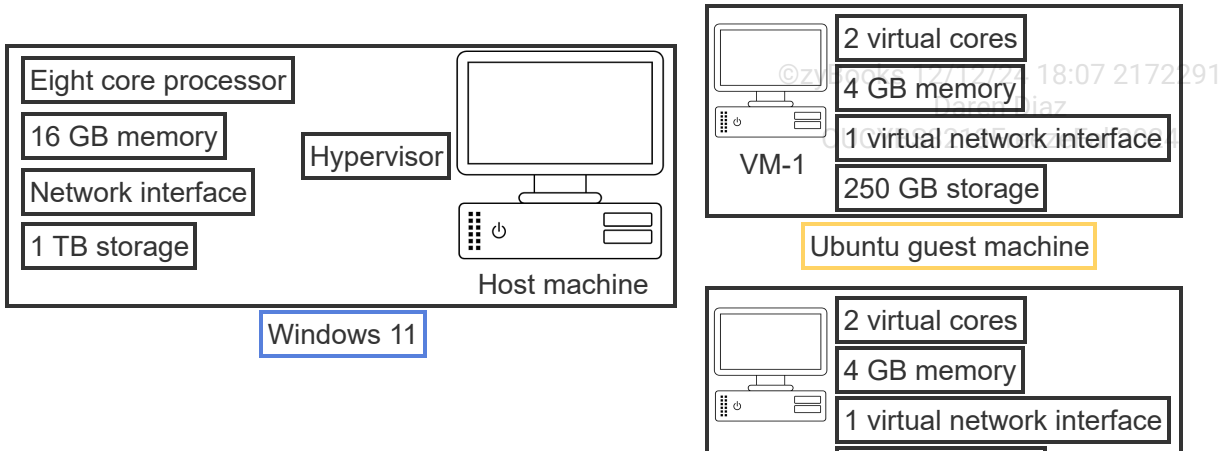
Virtualization is the use of software to create a simulated, or virtual, version of a physical computing resource. Virtualization is the foundation of cloud computing. Virtualization allows for more efficient utilization of physical computer hardware through the creation of virtual machines. A ***virtual machine (VM)*** is the virtualization of a computer system.

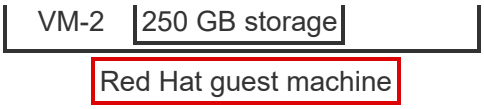
A VM consists of three components:

- A ***hypervisor***, also known as ***virtual machine monitor (VMM)***, is the software or firmware used to virtualize a host machine's hardware platform.
- A ***host machine*** is the machine used by a hypervisor to create a guest machine.
- A ***guest machine*** is a VM running on a host machine.

A guest machine runs an operating system (OS) and is logically isolated from a host machine. ***Logical isolation*** is a virtualization feature enabling a guest machine to behave like an independent machine. Logical isolation enables a host machine to run multiple guest machines with OS-specific software. Ex: A computer running Microsoft Windows 11 may host an Ubuntu Linux VM to run Ubuntu-based software on the hosted VM.

PARTICIPATION ACTIVITY 10.3.1: Virtualization.





Animation content:

Static image: A box labeled "Windows 11" contains a host machine with an eight core processor, 16 GB of memory, a network interface, 1 TB of storage, and a hypervisor. A box labeled "Ubuntu guest machine" contains VM-1 with 2 virtual cores, 4 GB of memory, 1 virtual network interface, and 250 GB of storage. A box labeled "Red Hat guest machine" contains VM-2 with 2 virtual cores, 4 GB of memory, 1 virtual network interface, and 250 GB of storage.

Animation captions:

1. A machine's primary hardware elements include a processor, memory, a network interface, and storage. Hardware elements are traditionally intended for a single machine.
2. A hypervisor enables a traditional machine to become a host machine from which a VM can be created. A hypervisor acts as an intermediary between hardware, a host machine, and VMs.
3. A hypervisor divides hardware elements among VMs. A VM becomes a guest machine once an OS is installed. Ex: A Windows 11 host creating an Ubuntu and a Red Hat guest machine.

PARTICIPATION ACTIVITY | 10.3.2: Virtualization.

Match the virtualization component to the component's description.

How to use this tool

Host machine **Guest machine** **VM** **Hypervisor**

	An instance of Ubuntu running on a Windows 11 host.
	A machine with virtual machine software installed.
	The software providing virtualization capabilities to a host machine.

	A machine running on a portion of underlying hardware and appearing as an individual computer system.

Reset

Hypervisor types

Two hypervisor types exist:

- A ***type 1 hypervisor***, also known as ***native*** or ***bare metal***, is a hypervisor running directly on a host machine.
- A ***type 2 hypervisor***, or a ***hosted hypervisor***, is a hypervisor running as an application on an existing operating system.

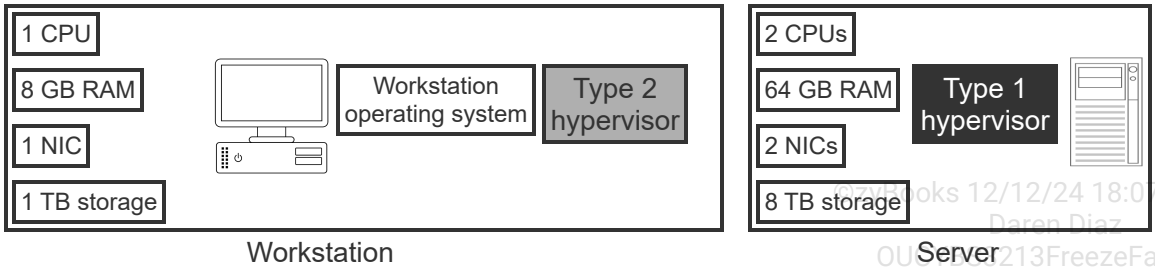
A type 1 hypervisor interacts with the underlying physical resources and replaces the traditional operating system altogether. Ex: Xen, Kernel-based Virtual Machine (KVM), and Windows Server Hyper-V are type 1 hypervisors.

A type 2 hypervisor uses the host operating system to access and coordinate the underlying hardware resources. A guest operating system runs as a process on the host. Ex: Oracle VirtualBox and VMware Player are type 2 hypervisors.

Table 10.3.1: Considerations for choosing a type 1 or a type 2 hypervisor.

Consideration	Type 1	Type 2
Use	A system built for virtualization	Adding virtualization to a traditional computer
Deployment	Server	Workstation
Performance	Better logical isolation for VMs	Adequate logical isolation for VMs
Cost	More expensive than type 2	Less expensive than type 1

PARTICIPATION ACTIVITY 10.3.3: Virtualization.



Animation content:

Static image: A box labeled "Workstation" contains 1 CPU, 8 GB RAM, 1 NIC, and 1 TB storage. A box labeled "Workstation operating system" and a box labeled "Type 2 hypervisor" are inside the Workstation box. A box labeled "Server" contains 2 CPUs, 64 GB RAM, 2 NICs, and 8 TB storage. A box labeled "Type 1 hypervisor" is inside the Server box.

Animation captions:

1. Both a workstation and a server consist of the same hardware elements. A server usually has more processing power, memory, and storage than a workstation.
2. A workstation or server can use either hypervisor type. However, type 2 is intended for a workstation with an existing operating system.
3. A type 1 hypervisor is commonly installed on a server because of a server's powerful hardware. A type 1 hypervisor interacts directly with hardware without an operating system.

PARTICIPATION ACTIVITY 10.3.4: Virtualization types.

1) Which hypervisor runs directly on a host machine?

- Type 1
- Type 2
- Type 3

2) Which hypervisor type is KVM?

- Type 1
- Hosted
- Type 2

3) Which hypervisor type uses a host's operating system to access underlying hardware?

- Bare metal
- SaaS
- Hosted

4) Which hypervisor type is VirtualBox?

- Public
- Bare metal
- Type 2

Virtualization exploits

Virtualization is subject to both traditional and virtualization-specific exploits. Ex: Malware is a traditional exploit that can infect both a host machine and a guest machine. VM escape and VM sprawl are two virtualization-specific exploits.

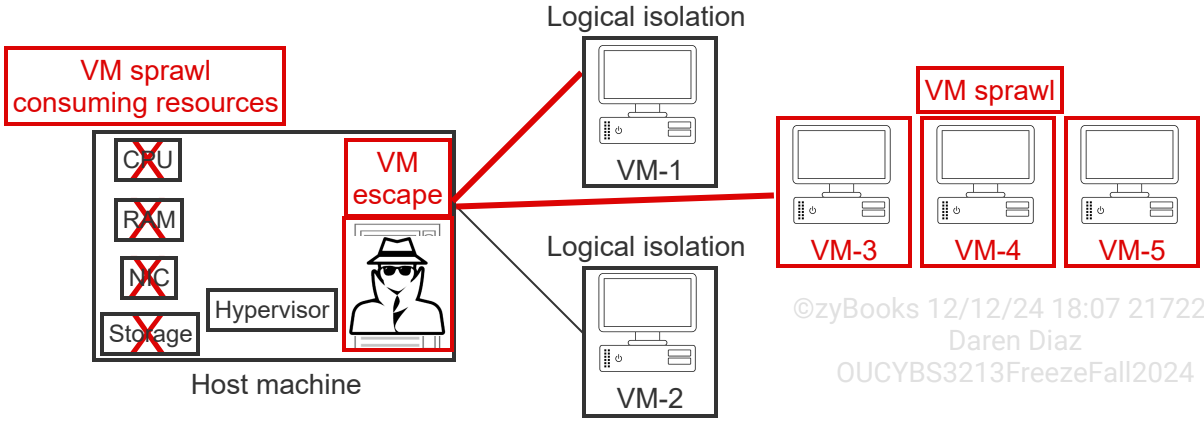
VM escape is a virtualization exploit where a process escapes a guest machine's logical isolation to interact with a host machine. An attacker uses VM escape to further exploit a host machine. Ex: An attacker can create, delete, or modify guest machines if a VM escape exploit is successful.

VM sprawl, or ***virtualization sprawl***, is a virtualization exploit where an attacker creates a VM amount that consumes available resources. An attacker can use VM escape to engage in VM sprawl on a host machine.

Resource reuse in virtual environments refers to the sharing of resources such as memory, I/O devices, or system components between the host machine and guest VMs or between multiple VMs. Resource sharing improves efficiency but can pose security risks without proper isolation, allowing a compromised VM to access or manipulate resources of other VMs or the host machine. Ex: A vulnerability in a shared memory mechanism could allow an attacker to reuse memory resources and gain access to sensitive data or inject malicious code into other VMs.

Traditional mitigation techniques should be applied to both host machines and guest machines for traditional exploits. Ex: Patch management is applied to both an Ubuntu guest machine and a Windows 11 host machine to mitigate malware. A host machine's VMM should be updated to mitigate virtualization exploits. Virtualization exploits are also mitigated by VM lifecycle management. ***VM lifecycle management*** is a series of procedures where a VM is created, maintained, monitored, and decommissioned when no longer needed.

PARTICIPATION ACTIVITY 10.3.5: Virtualization exploits.



Animation content:

Static image: A host machine connected with boxes representing CPU, RAM, NIC, and storage. The host machine connects to two VMs, called "VM-1" and "VM-2". The connection between the host machine and VM-1 is red, and an attacker with the label "VM escape" is within the host machine box. The attacker connects to a group of three more VMs outlined in red and labeled "VM sprawl". The label "VM sprawl consuming resources" is above the host machine's CPU, RAM, NIC, and storage. Red X's cover the CPU, RAM, NIC, and storage.

Animation captions:

1. A host machine has two guest machines. Both the host machine and guest machines are subject to virtualization exploits.
2. VM-1 is isolated from VM-2 and the host machine. However, VM escape is a virtualization exploit. A program breaks out of a guest VM to gain access to the host machine.
3. VM escape can lead to another virtualization exploit known as VM sprawl. VM sprawl occurs when a VM amount exceeds available resources, similar to a DoS attack.

PARTICIPATION ACTIVITY 10.3.6: Virtualization exploits.

1) What must be installed on an Ubuntu guest machine to remove a security vulnerability?

   - Package
   - App
   - Patch

2) What must be installed on a Windows host machine to address multiple

security vulnerabilities through a single update process?

- Patch
- Service pack
- Hotfix

3) Which virtualization exploit allows an attacker to break out of a VM to access a host machine?

- Computer virus
- VM escape
- VM sprawl

4) Which virtualization exploit increases the VM amount to the point of exceeding available resources?

- VM sprawl
- VM escape
- API attack

5) What is a potential security risk of resource reuse in virtual environments?

- Reduced latency in inter-VM communication
- Increased memory allocation for each VM
- A compromised VM accessing resources of other VMs or the host machine

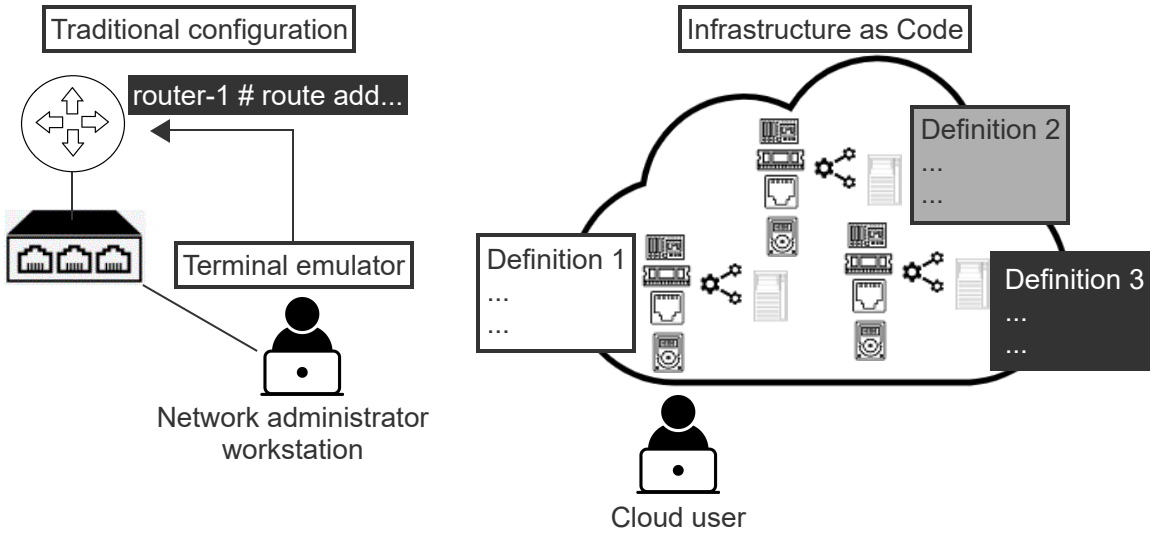
10.4 Software-defined networking

Infrastructure as Code

A cloud network can be configured declaratively based on a programmatic approach. ***Infrastructure as code (IaC)*** is the process of managing and provisioning computer data centers through machine-readable definition files, instead of hardware configuration or interactive configuration tools. The code

in the definition files may use either scripts or declarative definitions to configure infrastructure to a desired state. ***Desired state*** is an IaC feature that declares an infrastructure's final or desired state instead of configuration by a traditional step-by-step approach. IaC-managed infrastructure includes both physical equipment and associated configuration resources. Ex: Amazon Web Services (AWS) CloudFormation is an IaC.

PARTICIPATION ACTIVITY | 10.4.1: Infrastructure as Code.



Animation content:

Static image: The left side shows "Traditional configuration". The traditional configuration shows a network administrator workstation connected to a physical switch. The network administrator uses a terminal emulator to send the command "router-1 # route add..." to the router. The right side shows "Infrastructure as Code". A cloud contains icons representing cloud resources. Three boxes are next to separate groups of resources. The boxes are labeled "Definition 1", "Definition 2", and "Definition 3". A cloud user is outside of the cloud.

Animation captions:

1. Infrastructure is traditionally configured step-by-step using a terminal emulator with a connection to a physical device. Ex: Adding a route to a router's routing table.
2. IaC allows a cloud network to be configured declaratively based on a programmatic approach. A cloud user describes infrastructure's desired state in definition files.
3. Definition files are then pushed to the cloud service provider for automatic assignment to the appropriate cloud resources.

PARTICIPATION ACTIVITY | 10.4.2: Infrastructure as Code.

1) What is used to manage and provision data centers through configuration files rather than hardware configuration?
   - SaaS
   - IaaS
   - IaC

2) What physical resource is manageable by IaC?
   - End-user workstation
   - Virtualized server
   - Bluetooth headset

3) What does IaC use to manage physical resources and associated configuration resources?
   - CLI
   - Terminal emulator
   - Definition files

4) What IaC feature declares infrastructure's final state?
   - Desired state
   - Software versioning
   - Fogging

Overlay networks

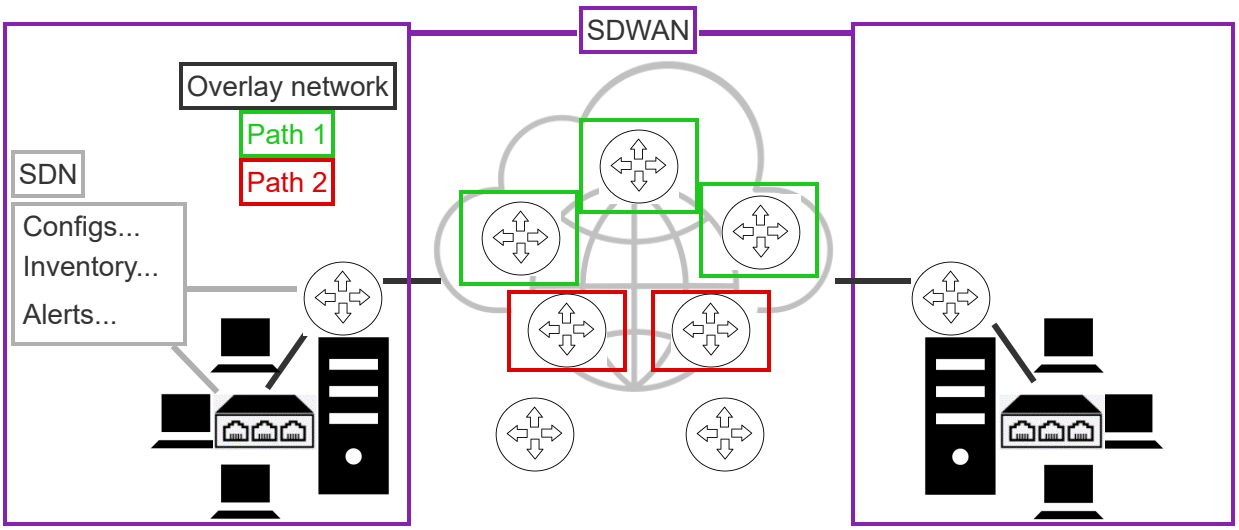
An overlay network is an example of IaC. An ***overlay network*** is a virtual network abstraction layer built on top of an existing physical network infrastructure. Many modern networks leverage at least one overlay network technology to improve network performance without an additional investment in network equipment. ***Software-defined networking (SDN)*** is an overlay network technology that centralizes a network's management and control planes. Centralization allows for more granular traffic management and efficient resource allocation, enabling administrators to dynamically adjust to changing network conditions and demands. Additionally, SDN facilitates the rapid deployment and management of virtualized network functions, enhancing network flexibility and scalability.

A ***software-defined wide area network (SD-WAN)*** is a software-defined network centralizing a multilocation network's management and control planes. SD-WAN enhances secure communication by embedding security features such as encryption, intrusion prevention systems, and firewalls directly into the network's architecture. Such an integration facilitates the enforcement of consistent and automated security policies throughout all locations, thereby ensuring secure access to network resources and protection of data in transit.

Network planes

A network's control, data, and management planes work together for network management and data transmission. The control plane is the network plane that determines how a packet is transmitted. The data plane is the network plane that transmits a packet. The management plane is the network plane that manages nodes.

PARTICIPATION ACTIVITY 10.4.3: Overlay networks.



Animation content:

Two LANs connected by several routers. A list called "Overlay network" shows "Path 1" in green and "Path 2" in red. Three of the routers between the LANs are outlined in green. Two other routers between the LANs are outlined in red. THe left LAN shows a box labeled "SDN" containing "Configs...", "Inventory..." and "Alerts...". The SDN box connects the LAN's switch and router.

Animation captions:

1. A legacy network relies upon basic routing and address tables to transmit data. Using tables reduces a network's ability to accommodate changing network conditions.
2. An overlay network mitigates time-consuming network operations. Ex: An overlay network labels each data packet to find the quickest path to the data packet's destination.
3. SDN streamlines a network's management plane by centralizing each network device's configuration into a single interface.
4. SDWAN is a software-defined network example. A SDWAN extends SDN capabilities into a multilocation network, such as a metropolitan area network (MAN) or wide area network (WAN).

PARTICIPATION ACTIVITY 10.4.4: Overlay network technologies.

1) An overlay network is an example of _____ because an overlay network manages and provisions network components through machine-readable definition files.
   - IaaS
   - PaaS
   - IaC

2) Which network technology improves network performance by overcoming the limitations of a network's physical infrastructure?
   - Logical topology
   - PSN
   - Overlay network

3) Which overlay network technology centralizes a network's management and control planes?
   - Virtual networking
   - SDN
   - VPN

4) Which overlay network utilizes an abstraction layer to centralize a

multilocation network's management plane?

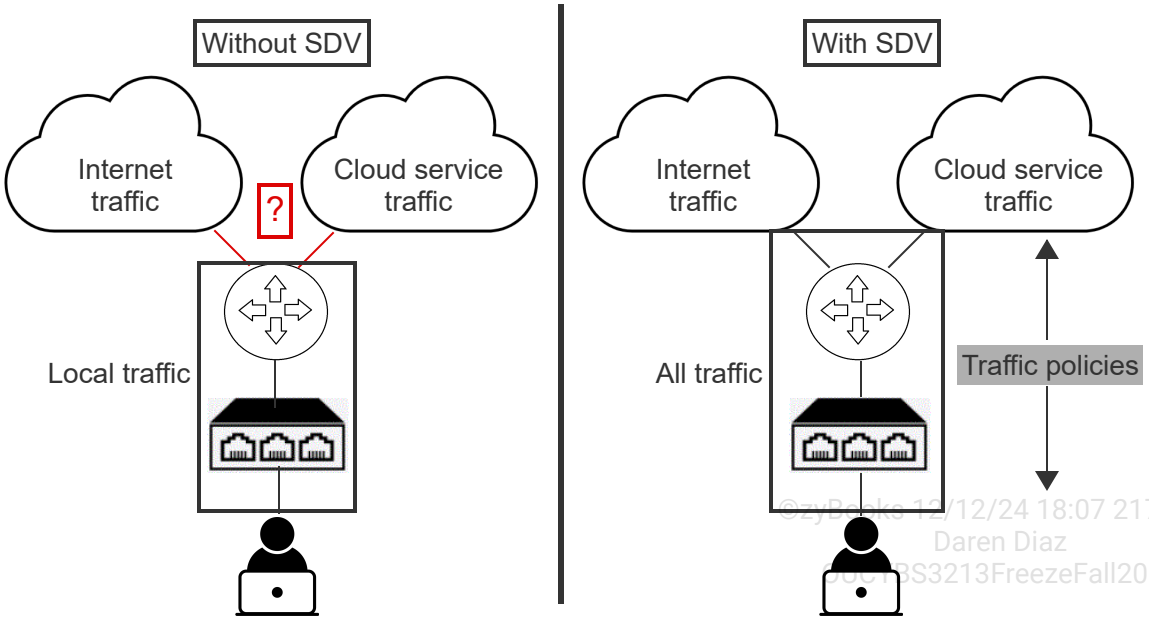
- SDN
- SDWAN
- VLAN

Software-defined visibility and APIs

Software-based tools can be used to monitor network traffic on the cloud, as well as an on-premises network. ***Software-defined visibility (SDV)*** refers to technologies enabling network traffic visibility to any monitoring device regardless of the device's physical location on a network.

A cloud-based application typically uses APIs to integrate with other applications and microservices. API calls should be inspected to prevent an attacker from sending malinformed data in an application's API. Many SDV solutions provide visibility into API calls to SDN components, assess cloud applications for vulnerabilities, and detect features deviating from best practices. Ex: Microsoft Cloud App Security is a tool that evaluates various aspects of a cloud application, including the application's account permissions, auditing, and data scanning.

PARTICIPATION ACTIVITY 10.4.5: Software-defined visibility.



Animation content:

Static figure: Two networks consisting of a user, a switch, a router, and internet connections for normal internet traffic and cloud service traffic. The network on the left does not have SDV and the

network on the right has SDV.
Step 1: Traffic monitoring without SDV lacks seamless visibility into local, Internet, and cloud service traffic. Utilizing multiple monitoring solutions is ineffective and inefficient. The network without SDV appears. A box labeled local traffic appears and indicates only local traffic visibility is possible. The connections for the internet traffic and cloud service traffic are changed from black to red. A question mark appears near the red connections to indicate how a network without SDV lacks visibility into internet and cloud service traffic.

Step 2: Traffic monitoring with SDV provides seamless visibility into all traffic regardless of origin or destination without multiple monitoring solutions. The network with SDV appears. A box labeled all traffic appears and indicates how visibility into all traffic is possible.
Step 3: Seamless visibility into all traffic allows the application of appropriate traffic policies - to/from the local network, to/from the Internet, and to/from a cloud service. A traffic policies text box appears with an up arrow pointing towards the internet and cloud service traffic and a down arrow pointing towards local traffic. The arrows represent how SDV enables the application of traffic policies to incoming and outgoing traffic.

Animation captions:

1. Traffic monitoring without SDV lacks seamless visibility into local, Internet, and cloud service traffic. Utilizing multiple monitoring solutions is ineffective and inefficient.
2. Traffic monitoring with SDV provides seamless visibility into all traffic regardless of origin or destination without multiple monitoring solutions.
3. Seamless visibility into all traffic allows the application of appropriate traffic policies - to/from the local network, to/from the Internet, and to/from a cloud service.

PARTICIPATION ACTIVITY 10.4.6: Software-defined visibility and APIs.

1) Which technology enables network traffic visibility to any monitoring device regardless of physical location?
   - SNMP
   - SFTP
   - SDV

2) Which interface type is used to integrate a cloud resource with an application and a service?
   - CLI
   - API
   - GUI

3) Which attack type targets application entry points?

- API attack
- XSS attack
- Buffer overflow attack

4) Which tool can identify when a cloud-based application feature deviates from industry best practices?

- Overlay network
- Software-defined visibility
- Desired state

10.5 Storage, network, and compute security controls

Compute

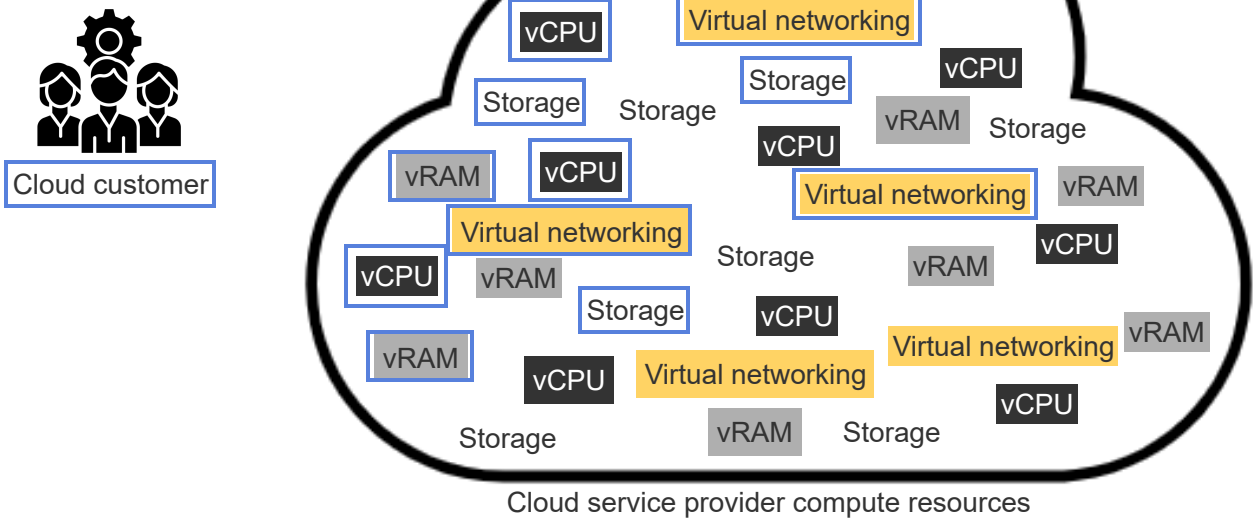
Compute is a term referring to the collective cloud resources required to meet a cloud customer's computational needs. A ***compute resource*** is a measurable quantity of compute power that can be requested, allocated, and consumed in computations. Ex: A Central Processing Unit (CPU), Graphic Processing Unit (GPU), and Random Access Memory (RAM) are compute resources. Four compute resources exist:

- A ***virtual central processing unit (vCPU)*** is a portion of a host machine's CPU made available to a guest machine for virtualization or as part of cloud computing.
- ***Virtual random access memory (vRAM)*** is a portion of a host machine's RAM made available to a guest machine for virtualization or as part of cloud computing.
- ***Virtual networking*** is a computer network made available to a guest machine for virtualization or as part of cloud computing.
- ***Cloud storage*** is a cloud resource where a cloud service provider stores, manages, and operates cloud customer's data.

Dynamic resource allocation (DRA) is the automatic provisioning and deprovisioning of cloud resources based on demand. Dynamic resource allocation makes cloud computing scalable and cost-efficient. Ex: Dynamic resource allocation automatically provisions a retailer's web servers during a

sales event when demand increases and deprovisions the web servers after the sales event when demand decreases. Web servers are dynamically deprovisioned as the number of visitors decreases.

PARTICIPATION ACTIVITY 10.5.1: Cloud resources.



Animation content:

Static image: An icon labeled "Cloud customer" and a cloud labeled "Cloud service provider compute resources". The cloud contains small boxes representing cloud resources: five yellow boxes labeled "Virtual networking", ten black boxes labeled "vCPU", nine gray boxes labeled "vRAM", and nine white boxes labeled "Storage". Blue outlines indicate resources used by the Cloud customer. Three vCPU boxes, three Virtual networking boxes, three vRAM boxes, and three Storage boxes are outline in blue.

Animation captions:

1. A cloud service provider offers compute resources to cloud customers to satisfy computational needs. Processing (vCPU), memory (vRAM), networking, and storage are made available as compute.
2. A cloud customer uses compute resources to satisfy computational needs. Ex: An organization with a cloud-based database needs processing, memory, networking, and storage resources.

PARTICIPATION ACTIVITY 10.5.2: Cloud resources.

1) Which term refers to a collection of cloud resources intended for a customer's computational needs?

- Cloud computing
- AZ
- Compute

2) Which compute type provides processing power for a customer's computational needs?

- vCPU
- Virtual networking
- Cloud storage

3) Which compute type satisfies memory requirements for a cloud-based application?

- vCPU
- vRAM
- VLAN

4) What enables compute to scale automatically based on customer need or service demand?

- DRA
- DNS
- DHCP

Cloud security controls

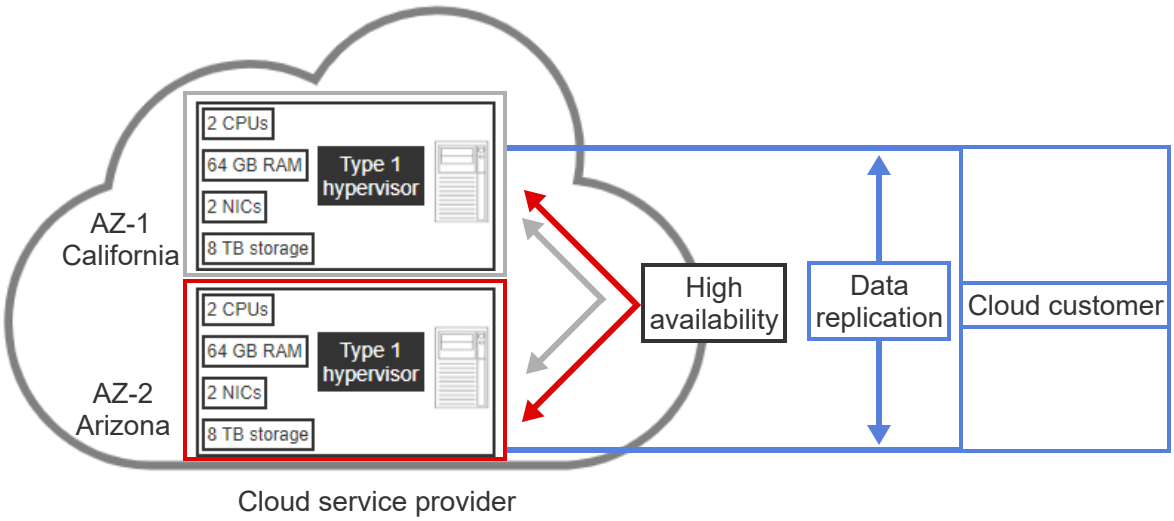
A cloud service provider utilizes several security controls for their cloud services. High availability across zones is provided by interconnecting the zones using high-bandwidth, low-latency, and redundant network links. The physical separation of zones provides disaster recovery by ensuring cloud services are protected against natural and man-made disasters Ex: Earthquakes, tornados, fire, and sabotage.

A cloud resource, such as a virtual machine, is usually associated with a resource policy and a hardware security module. A ***resource policy*** specifies a cloud resource's authorized users, systems, and actions. A ***hardware security module (HSM)*** is a tamper-resistant external device or a plug-in expansion card that provides cryptographic services. A cloud service provider uses an HSM to store a

hardware device's certificate for authentication, cryptographic keys, and passwords. A cloud service provider may offer HSM services to cloud customers to enable secrets management, including the secure storage of encryption keys and passwords.

A cloud resource is also auditable. Auditing helps cloud customers evaluate the effectiveness of implemented security controls and provides the means to demonstrate regulatory compliance.

PARTICIPATION ACTIVITY 10.5.3: Cloud security controls.



Animation content:

Static image: A cloud labeled "Cloud service provider" contains two availability zones, labeled "AZ-1 California" and "AZ-2 Arizona". The label "Cloud customer" is outside the cloud and connects to both availability zones. The label "High availability" is next to the availability zones and has arrows pointing to both availability zones. The label "Data replication" is shown between the Cloud customer's connections to the two availability zones.

Animation captions:

1. Locating AZs in separate locations reduces the likelihood of a single disaster impacting cloud services. Ex: A disaster in California should not impact an AZ located in Arizona.
2. A cloud customer selects compute resources in two different AZs for the customer's own disaster recovery purposes.
3. The cloud service provider uses high-bandwidth, low-latency, and redundant network links for high availability within and among the zones.
4. A cloud customer configures their cloud services with data replication between the two AZs for high availability and fault tolerance purposes.

PARTICIPATION ACTIVITY 10.5.4: Cloud security controls.

1) What security control is provided by the physical separation of availability zones?
   - Data confidentiality
   - Data integrity
   - Disaster recovery

2) Which policy type would define an authorized user for a cloud resource?
   - Resource policy
   - Account policy
   - Password policy

3) Which cloud resource is subject to a resource policy?
   - Hypervisor
   - OS
   - Cloud storage

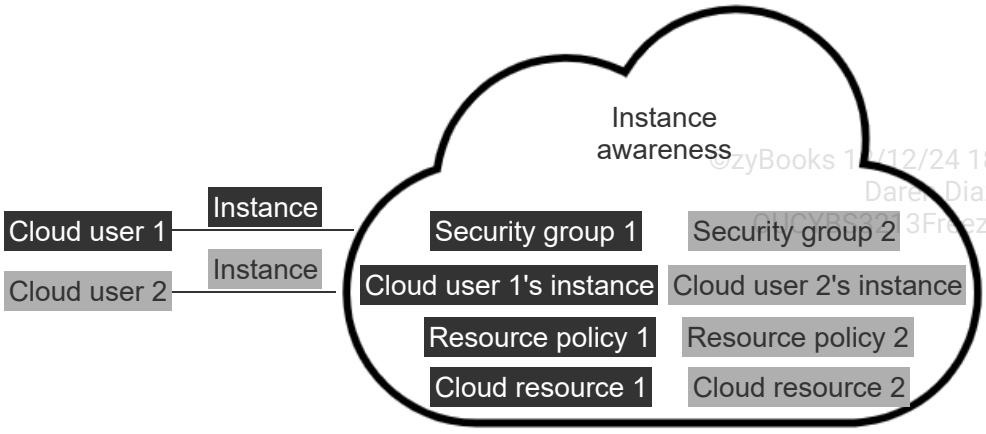
4) Which device is used by a cloud service provider to enable secrets management?
   - Security token
   - HSM
   - OTP

Cloud resource security controls

Cloud resource access is controlled by security groups and instance awareness. A ***security group*** is a security control for associating several cloud users with a resource policy. A security group acts as a virtual firewall for a cloud resource. Ex: A security group is assigned to a resource policy disabling TCP port 23 to prevent a telnet connection to a cloud resource.

An organization may run multiple simultaneous instances of a cloud service. Ex: An organization running several hundred instances of a cloud storage service such as Microsoft OneDrive. ***Instance awareness*** is a tool providing cloud instance recognition to define and apply appropriate resource policies.

PARTICIPATION ACTIVITY 10.5.5: Cloud resource security controls.



Animation content:

A cloud with the label "Instance awareness". The cloud contains two columns of text. The left column text is white on a black background and includes "Security group 1", "Cloud user 1's instance", "Resource policy 1", and "Cloud resource 1". The right column is black with a gray background and includes "Security group 2", "Cloud user 2's instance", "Resource policy 2", and "Cloud resource 2". Outside the cloud, the text "Cloud user 1" is written in white with a black background. "Cloud user 1" connects to the cloud. The text "Instance" is above the connection and written in white text with a black background. Below "Cloud user 1", the text "Cloud user 2" is written in black with a gray background. "Cloud user 2" also connects to the cloud. The text "Instance" is above the connection and written in black with a gray background.

Animation captions:

1. Two cloud users attempt to access cloud resources. Instance awareness recognizes the access attempts.
2. A cloud user's instance is recognized and associated with a security group. A security group is associated with a resource policy to determine a cloud user's access.

PARTICIPATION ACTIVITY 10.5.6: Cloud resource security controls.

1) Which security control associates several cloud users with a resource policy?
   - ○ GPO
   - ○ Security group

- Group account

2) A security group is acting as a _____ when associated with a resource policy configured to block port 23.
   - virtual firewall
   - virtual network
   - virtual machine manager

3) A security group should be associated with a resource policy allowing port _____ to enable a SSH connection to a cloud resource.
   - 20
   - 21
   - 22

4) Which tool identifies multiple occurrences of cloud resource access?
   - Instance awareness
   - Continuous monitoring
   - DLP

Virtual network security controls

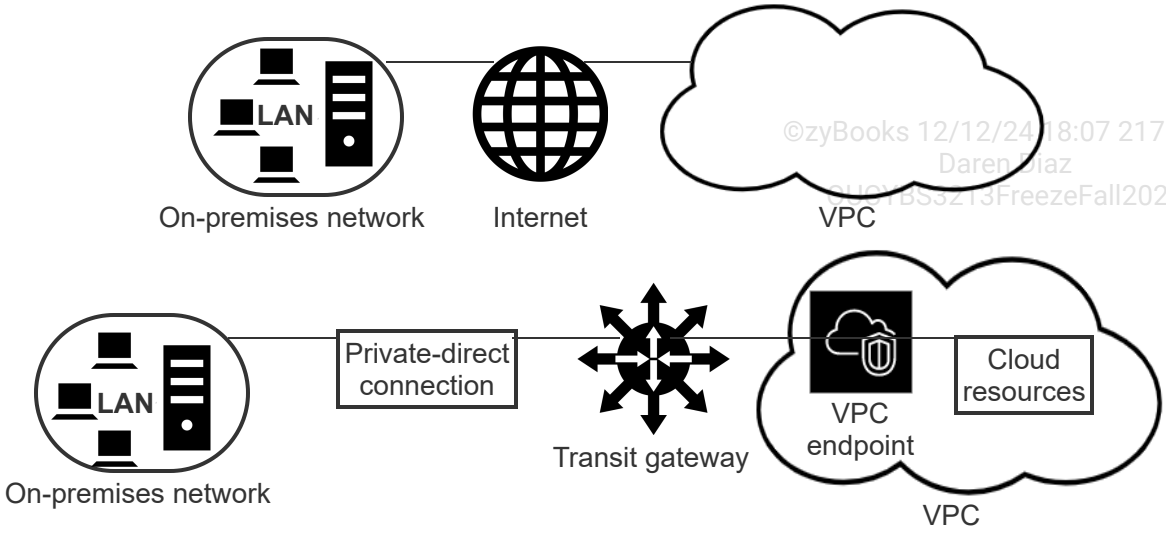
A virtual network uses some of the same security controls as an on-premises network. Ex: A virtual firewall provides the same protections as a physical firewall. Network segmentation is also used within a virtual network. Ex: A virtual network is divided into smaller subnetworks for access control and improved security.

A ***VPC endpoint*** is a virtual device with connectivity to a VPC's instances without requiring public IP addresses. A ***transit gateway*** is a network transit hub interconnecting on-premises networks and VPCs. A cloud customer defines and controls communications between on-premises infrastructure and a cloud provider's network. A transit gateway acts as a virtual router and scales elastically based on traffic volume.

A VPC endpoint and a transit gateway are part of a private-direct connection to a cloud provider. A ***private-direct connection*** is a private connection, rather than an Internet-based connection from an on-premises network to a cloud service provider's VPC. Many cloud service providers offer a VPN add-on for their private-direct connections for enhanced security through encrypted connections.

PARTICIPATION ACTIVITY

10.5.7: Virtual network security controls.



Animation content:

A VPC endpoint and a transit gateway are part of a private-direct connection to a cloud provider. A private-direct connection is a private connection, rather than an Internet-based connection from an on-premises network to a cloud service provider's VPC.

Animation captions:

1. A cloud customer typically connects from an on-premises network to a VPC using on-premises networking devices and the Internet.
2. A cloud customer can work with their cloud service provider to establish a private-direct connection to a VPC for better performance and enhanced security.
3. A transit gateway connects an on-premises network with a VPC. A VPC endpoint is created within a VPC to connect with VPC instances and cloud resources.

PARTICIPATION ACTIVITY 10.5.8: Virtual network security controls.

1) Which security control provides network access control by using subnetworks for a large network?

   - Network segmentation
   - VPN
   - Load balancing

2) What provides a connection from a cloud customer to a VPC without requiring a public IP address?

- VPN endpoint
- VLAN endpoint
- VPC endpoint

3) Which device interconnects an on-premises network with a VPC?

- Transit gateway
- Default gateway
- Media gateway

4) What connection type does a combination of a VPC endpoint and a transit gateway form?

- P2P
- Private-direct
- Client-server

Cloud responsibility matrix

A ***cloud responsibility matrix*** is a visual representation that clarifies the roles and responsibilities of both cloud service providers and cloud customers for various cloud computing models. A cloud responsibility matrix outlines the specific responsibilities of each party, including infrastructure, applications, and security. Ex: In an IaaS model, the cloud provider is responsible for the physical servers, storage, and networking hardware, while the customer manages the operating system, applications, and data.

The division of responsibilities provides operational clarity, minimizing overlaps and gaps that could lead to security vulnerabilities or inefficiencies in cloud service deployment and management. Additionally, allocating tasks streamlines troubleshooting, enhances compliance with regulations, and improves the security and reliability of the cloud environment. Ex: AWS as the cloud provider is responsible for securing the underlying cloud infrastructure, while Netflix as the cloud customer is responsible for securing Netflix applications and data stored on the AWS cloud.

Table 10.5.1: Cloud responsibility matrix.

Responsibility	IaaS	PaaS	SaaS	Examples

Infrastructure	Provider	Provider	Provider	Physical servers, networking hardware
Application & data	Customer	Customer	Provider	Operating system, application software
Security & compliance	Shared	Shared	Provider	Security protocols, compliance audits
Backup & disaster recovery	Shared	Provider	Provider	Data backup solutions, disaster recovery plans
Identity & access management	Shared	Provider	Provider	User authentication, access controls

PARTICIPATION ACTIVITY 10.5.9: Cloud responsibility matrix.

Based on the cloud responsibility matrix, identify the party responsible for each scenario.

1) Physical security of data centers when Dropbox uses Amazon S3 (IaaS) to store user data
   - Amazon
   - Dropbox
   - Shared

2) Operating system patches when Adobe Systems uses Amazon EC2 (IaaS)
   - Amazon
   - Adobe Systems
   - Shared

3) Application updates when Salesforce uses Google App Engine (PaaS)
   - Google
   - Salesforce
   - Shared

4) Disaster recovery planning when Zoom uses Oracle Cloud Infrastructure (OCI) for computing resources (IaaS)

- Oracle
- Zoom
- Shared

5) Database software updates when a financial firm uses Microsoft Azure SQL Database (PaaS)

- Microsoft
- The financial firm
- Shared

6) GDPR compliance when a retail store hosts a website on IBM Cloud's PaaS offering

- IBM
- The retail store
- Shared

Cloud-specific vulnerabilities

Cloud computing environments are vulnerable to various security risks, including resource misconfiguration, insecure APIs, and shared technology vulnerabilities. Improperly configured resources can expose sensitive data, while insecure APIs can be exploited to gain access to cloud service management interfaces. Shared technology risks, such as vulnerabilities in hypervisors and networking hardware, can lead to isolation failures and compromise the security and integrity of cloud resources.

To effectively address the security risks in cloud computing environments, robust security measures must be implemented, including regular security audits, penetration testing, and incident response plans that account for the scalability and distributed nature of cloud resources. As part of such measures, robust API security and stringent access controls can help prevent cloud data breaches, including multi-factor authentication, role-based access control, and regular access reviews to ensure that only authorized personnel interact with sensitive infrastructure and data.

10.6 Cloud security solutions

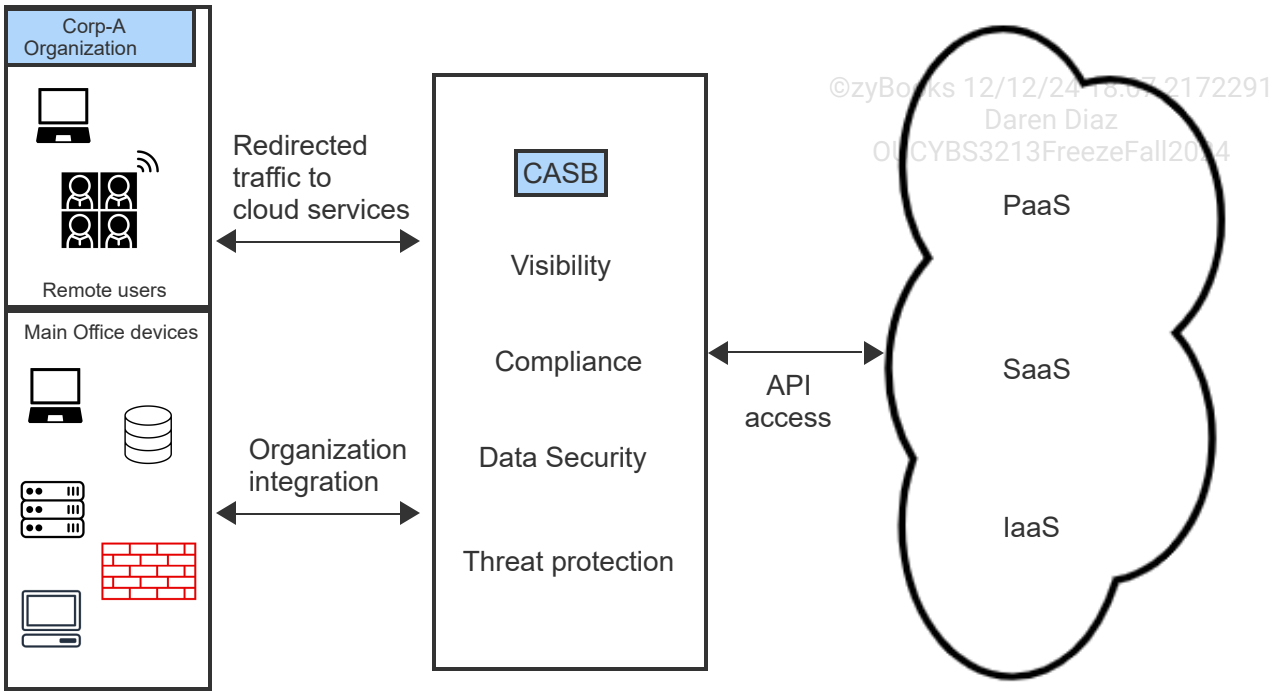
CASB

A ***cloud access security broker (CASB)*** is a software security service, placed between an organization's infrastructure and a cloud service provider's infrastructure, enforcing an organization's security policies when cloud-based resources are accessed. A CASB, deployed in the cloud or on-premises, is a security policy enforcement point. A security policy may include authentication, authorization, encryption, logging, alerting, and malware detection/prevention. Ex: A CASB enforces an organization's cloud data encryption policies on cloud data.

CASB:

- Visibility - Keeps track of how and who is using the cloud services Ex: Records the time and device's IP address when the device accesses the company's database.
- Compliance - Provides control of outside organization data and meets compliance as per regulatory requirements.
- Data security - Monitors and provides access control to data by parameters like location, IP address, browser, OS, and device type.
- Threat protection - Provides alerts when threats are detected.

PARTICIPATION ACTIVITY 10.6.1: CASB Implementation.



Animation content:

Core-A's organizational offices and data centers around the world are similar to most organizations' structure. Office, users, and data centers are shown. A CASB is set in between the organization and the cloud services. Core-A traffic outside the Core-A organization is redirected through the CASB for protection. Also, Core-A inside lan traffic is integrated through the CASB.

Animation captions:

1. Corp-A's infrastructure is comprised of network components located on-site and off-site.
2. A CASB is set in between the organization and the cloud services. Cloud vendors provide services PaaS, SaaS, and IaaS, which form the external cloud layer a CASB connects to.
3. Remote users core traffic is redirected through a CASB to cloud services. The CASB provides multiple types of security policy enforcement.
4. Main office devices access cloud services through a CASB using API access. An API allows applications to communicate with one another.

PARTICIPATION ACTIVITY 10.6.2: CASB.

1) A CASB is a software security service.

- True
- False

2) Throughput is a pillar of a CASB.

- True
- False

3) A CASB is a security policy enforcement point.

- True
- False

SWG, NGFW, and FWaaS

Next generation secure web gateway (SWG) is an on-premise appliance or cloud-based network security service that protects users from web-based threats and enforces corporate acceptable use policies. A SWG operates at the application layer and is deployed between users and the Internet. A SWG performs URL filtering, malware detection, malicious content inspection, data loss prevention (DLP), application control, and filtering Internet-bound traffic functions.

Next generation firewall (NGFW) is an on-premise or cloud hosted network security device providing firewall capabilities beyond a traditional firewall. NGFW, like traditional firewalls, can segment a network into trusted and untrusted zones, which limits attack surfaces, thereby preventing threats spreading beyond a zone. NGFW capabilities include IPS, DPI, threat intelligence, and application control.

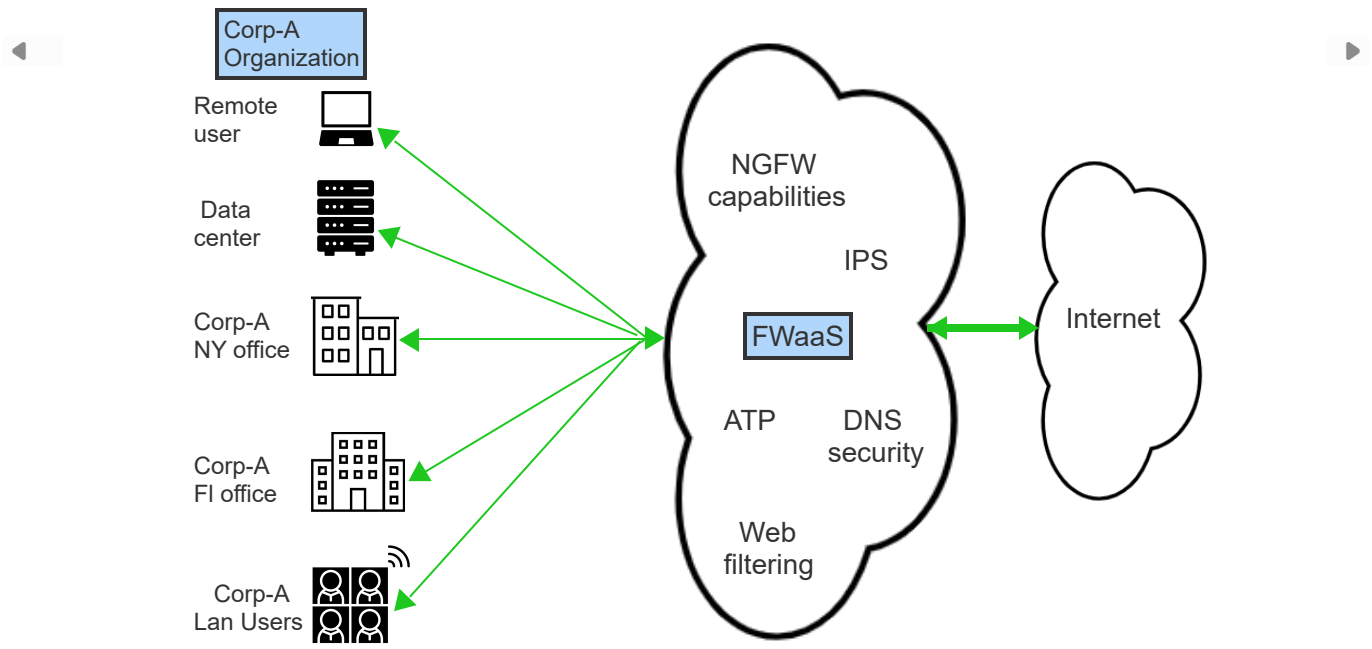
Firewall as a service (FWaaS), also known as a ***cloud firewall***, provides NGFW capabilities, which filters network traffic to safeguard organizations from both inside and outside threats. Similar to an on-premise IT environment, a FWaaS prevents unauthorized access into or out of a virtual network. FWaaS, like SaaS or IaaS, is hosted in the cloud and accessed through the Internet.

Table 10.6.1: Comparing firewall types.

Firewall type	Cost frequency	Cost based on	OSI layer operation	Security model
FWaaS	Monthly	Volume of traffic filtered	1-7	Virtual wall across platforms, infrastructure, and applications

NGFW	Upfront and monthly	Initial equipment costs and employee maintenance/setup costs	1-7	Virtual wall around internal network
Traditional	Upfront and monthly	Initial equipment costs and employee maintenance/setup costs	1-4	Virtual wall around internal network

PARTICIPATION ACTIVITY 10.6.3: FWaaS setup.



Animation content:

Core-A's organizational offices and data centers around the world need to be protected from the internet. Office, users, and data centers are shown. A FWaaS is placed in the cloud between the internet and the Core-A organization. Core-A traffic is funneled through the FWaaS. The FWaaS will provide security functions for the Core-A organization.

Animation captions:

1. Corp-A's organizational offices and data centers around the world must be protected from the internet.
2. A FWaaS is placed in a cloud between the internet and the Corp-A organization.
3. Corp-A traffic is funneled through the FWaaS, providing security between Corp-A and internet resources.

PARTICIPATION ACTIVITY 10.6.4: SWG and FWaaS.

1) A cloud-based or on-premise _____ provides content filtering.
   - NGFW
   - FWaaS
   - SWG

2) _____, a type of NGFW, filters network traffic to safeguard organizations.
   - CASB
   - FWaaS
   - SWG

3) FWaaS operates at what OSI Layer?
   - 3
   - Layers 1 thru 4
   - Layers 1 thru 7

4) Which devices create a virtual wall around an organization's internal network?
   - Traditional firewall and NGFW
   - Traditional firewall and FWaaS
   - NGFW and FWaaS

Cloud-native

Cloud native refers to both platform and infrastructure security, as well as continuous application security. A traditional security approach is to build a perimeter around the infrastructure. ***Cloud-native***

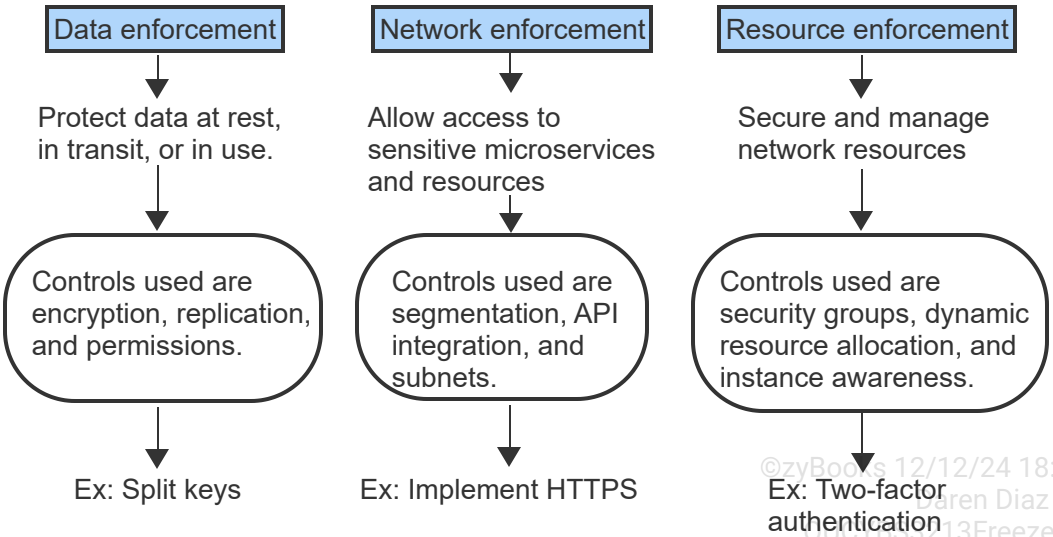
architecture dissolves the perimeter and builds security into the assets. Assets apply to multiple layers, from OS to container to application.

A ***security control*** reduces risks to assets. A ***cloud-native security control*** is inherent to the cloud computing environment, whereas a ***third-party security control*** is a security control available from an external source or exists on-premise.

Cloud-native controls used in securing cloud computing:

- Visibility and audits - Performing audits satisfies compliance and legal requirements. Visibility identifies and logs network access.
- High availability - Create server clusters in different geographical areas for resiliency. Ex: Storm in NE USA causes power loss, servers in California can service needs.
- DevOps process microservices/API's - Security is integrated into the DevOps process ensuring the infrastructure and application are free from vulnerabilities. Two practices of DevOps are microservices, building a single application from a set of small services, and Infrastructure as Code, using the cloud's API driven model features. Secret management is used for management of API keys, database credentials, IAM permissions, SSH keys, and certificates.
- Mitigation - Enforce mitigation on cloud computing's data, network, and compute resources.

PARTICIPATION ACTIVITY 10.6.5: Cloud-native mitigation control enforcement.



Animation content:

When a company moves the network resources to the cloud, the company evaluates the three key areas of security mitigations for cloud computing. Step 1: Data enforcement mitigation protects data at rest, in transit, or in use. Ex: Protect files by splitting keys and store the keys on different

devices. Step 2: Network enforcement mitigation allows access to sensitive microservices and resources. Ex: Use HTTPS everywhere to help protect against phishing. Step 3: Resource enforcement mitigation integrates security into the DevOps process. Ex: Use two-factor authentication to add an extra layer of security.

Animation captions:

1. When a company moves the network resources to the cloud, the company evaluates the three key areas of security mitigations for cloud computing.
2. Data enforcement mitigation protects data at rest, in transit, or in use. Ex: Protect files by splitting keys and store the keys on different devices.
3. Network enforcement mitigation allows access to sensitive microservices and resources. Ex: Use HTTPS everywhere to help protect against phishing.
4. Resource enforcement mitigation integrates security into the DevOps process. Ex: Use two-factor authentication to add an extra layer of security.

PARTICIPATION ACTIVITY 10.6.6: Cloud-native.

1) _____ is achieved by creating clusters, a group of servers acting as a single server.
   - ○ High availability
   - ○ Audit
   - ○ Cloud-native control

2) _____ is used for management of API keys, database credentials, IAM permissions, SSH keys, and certificates.
   - ○ High availability
   - ○ Secret management
   - ○ Visibility and audits

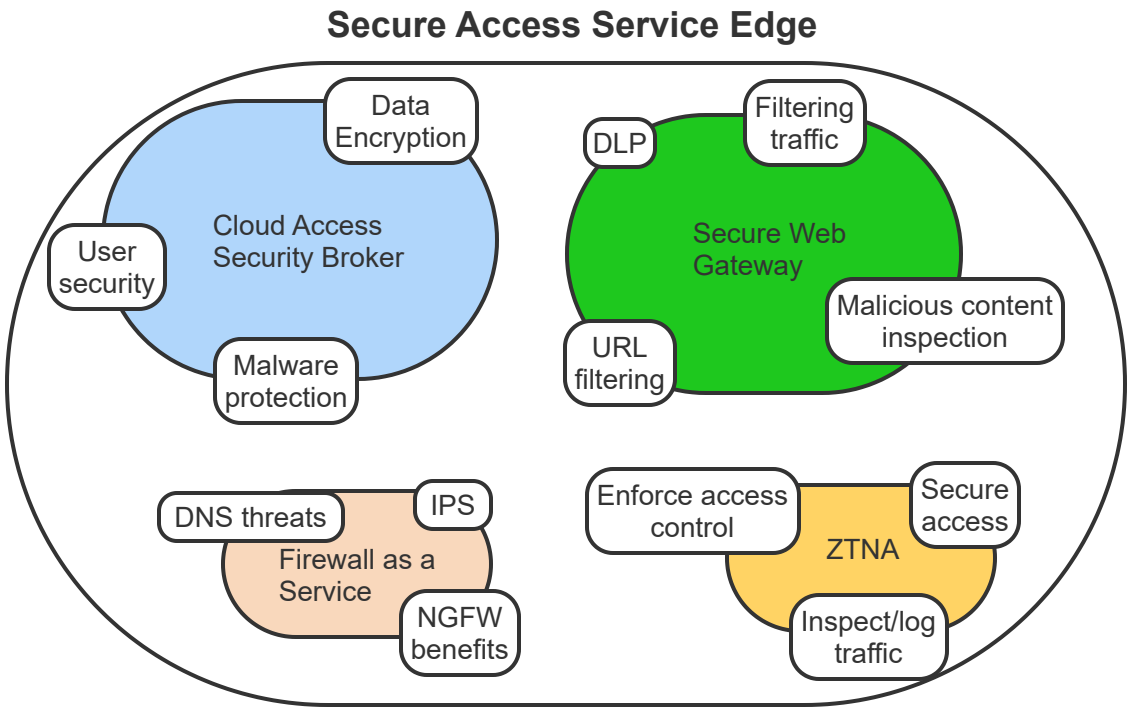
3) Cloud-native architecture _____ perimeter and builds security into the assets.
   - ○ creates
   - ○ extends
   - ○ dissolves

SASE

Secure access service edge (SASE) was developed to combine networking and network security services into a single system. ***Secure access service edge (SASE)*** is the convergence of WANs and network security services into a single cloud service model.

A SASE environment supports multiple cloud security services (Ex: SWG, FWaaS, CASB, DNS security, and DLP) in one cloud-based platform.

PARTICIPATION ACTIVITY 10.6.7: SASE security model architecture.



SASE is a security model combining perimeter and cloud security. SASE provides users the same network services and security controls from any location.

Animation captions:

1. CASB is a main component of SASE. CASB may include authentication, authorization, encryption, logging, alerting, and malware detection/prevention.
2. SGW is another security appliance used by the SASE to protect users from web-based threats and enforce corporate acceptable use policies.
3. A Zero-Trust network access (ZTNA) can be added to the SASE architecture. ZTNA enables employees secure access to all apps, tools, and data from anywhere.
4. FWaaS can be added to SASE. FWaaS has all the capabilities of a NGFW, plus can incorporate an IPS, DLP, secure gateway, ZTNA, and protection against DNS threats.

PARTICIPATION ACTIVITY 10.6.8: SASE.

1) Secure access service edge (SASE) is the convergence of WANs and network security services into multiple cloud service models.
   - True
   - False

2) A SASE environment will allow only one cloud security service.
   - True
   - False

3) CASB is a main component of SASE.
   - True
   - False

4) SASE can contain a FWaaS.
   - True
   - False

5) SASE allows companies to control security from one cloud-based platform.
   - True
   - False

Cloud infrastructure hardening

Cloud infrastructure hardening encompasses a range of technical measures to secure cloud computing environments by minimizing vulnerabilities and reducing the risk of cyber attacks. Such measures include conducting regular vulnerability assessments to identify weaknesses, applying timely security patches to prevent potential exploits, and implementing network segmentation to divide cloud environments into smaller, isolated segments, thereby mitigating the impacts of security incidents. Authentication and authorization protocols are used to control access, and encryption ensures the

confidentiality and integrity of data, both at rest and in transit, across the cloud and the on-premises systems.

CHALLENGE ACTIVITY | 10.6.1: Cloud security solutions.

581480.4344582.qx3zqy7

Start

Which CASB functions contribute to visibility? Select all that apply.

- [ ] Logging all uploads to the cloud
- [ ] Detecting compliance violations
- [ ] Recording an audit trail for user activities
- [ ] Logging all downloads from the cloud
- [ ] Detecting threats from internal users

1 2 3

Check Next

10.7 LAB: Secure virtualization (Walkthrough)

IT-Labs are not printable at this time.

10.8 LAB: Cloud security (Walkthrough)