Cloud Computing NETW1009

Lecture 12

Course Instructor: Dr. – Ing. Maggie Mashaly

GUC
German University in Cairo

Lecture 12: Cloud Security II

What we learned so far..

- Overview on Cloud Security
- Cloud Security Concepts
- Cloud Security Threats

Today's Lecture Outline

- Cloud Security Control Mechanisms
- Security-as-a-Service

Security Mechanisms

Preventive Control

- Avoids a vulnerability being exploited in the cloud environment.

Deterrent control

- Reduces the likelihood of a vulnerability being exploited in a cloud environment by warning the attackers.
- **Example:** Data Center physical security, firewall, hardening, and authentication mechanism

Detective Control

- Security tools must detect the newly provisioned resources and integrate with the existing resources.
- They are used when the preventive controls are failed.
- **Example:** Audit trails and logs

Corrective Control

- The goal is to reduce the after-effects of an attack by restoring the system to its expected state.
- They are used during or after an attack has been detected.
- **Example:** Data restore from backup

Security Mechanisms Classification: Administrative Security

Security mechanisms can be broadly classified into three types

1. Administrative Security

- Includes security and personnel policies or standard procedures
- Includes regulatory compliance, policies, and procedures, contracts and SLAs, background verification of the employees, and trainings

2. Physical security

3. Technical security

Security Mechanisms Classification: Physical Security

Security mechanisms can be broadly classified into three types

1. Administrative security

2. Physical security

3. Technical security

- 24/7/365 onsite security
- Biometric or security badge-based authentication
- Video surveillance cameras to monitor the activity
- Redundant utilities for HVAC systems
- Sensors and alarms to detect unusual activities and fire
- Use metal detection to screen the visitors

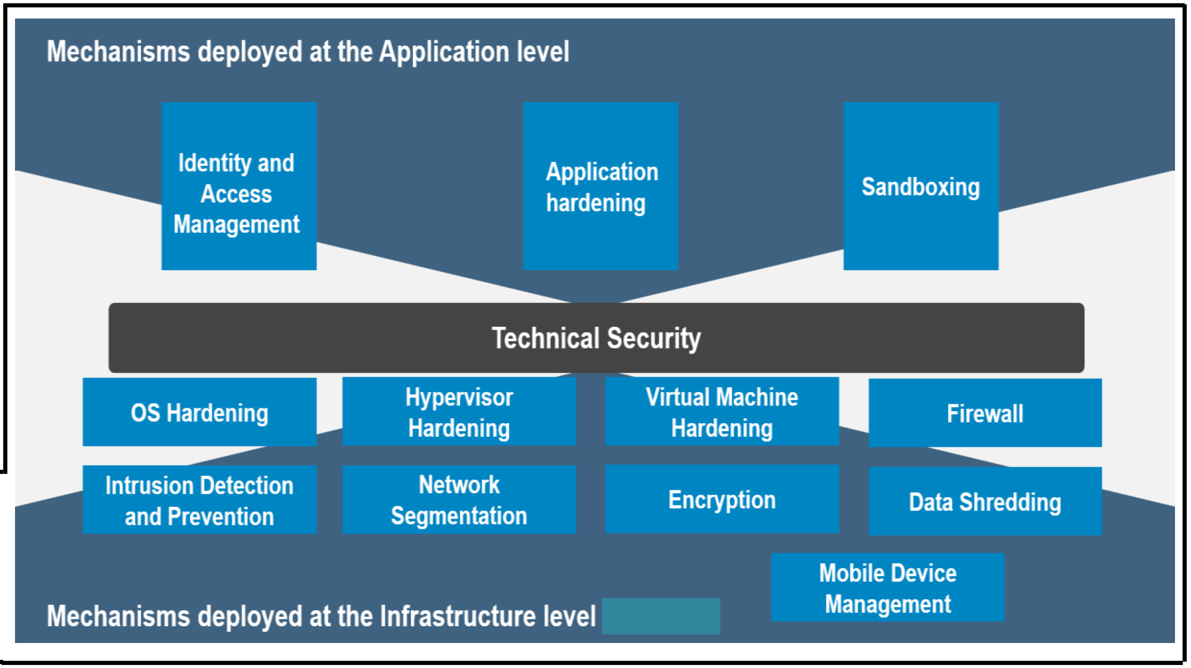
Security Mechanisms Classification: Technical Security

Security mechanisms can be broadly classified into three types

1. Administrative security

2. Physical security

3. Technical security



Mechanisms deployed at the Application level

Identity and Access Management

Application hardening

Sandboxing

Technical Security

OS Hardening

Hypervisor Hardening

Virtual Machine Hardening

Firewall

Intrusion Detection and Prevention

Network Segmentation

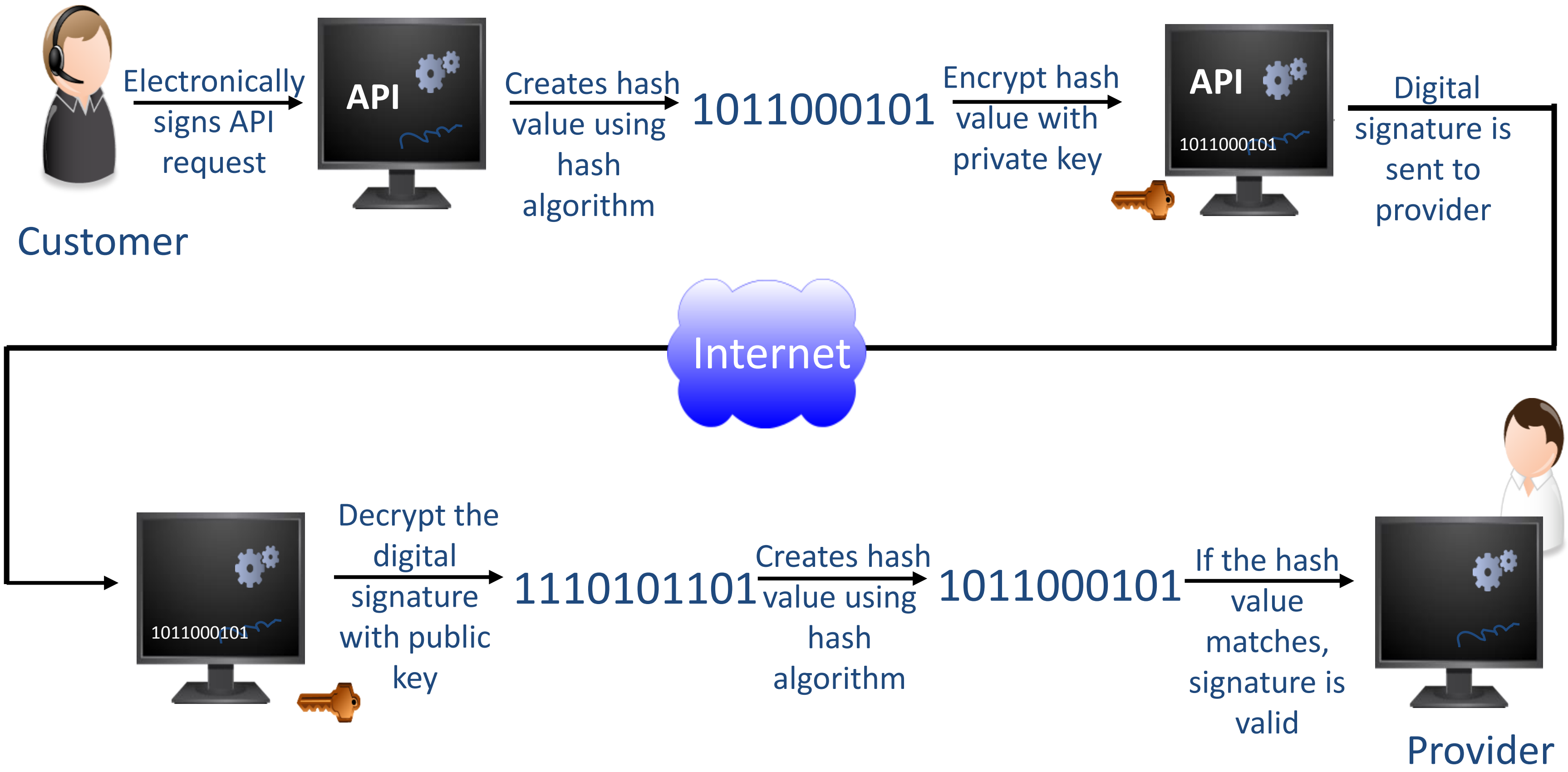
Encryption

Data Shredding

Mobile Device Management

Mechanisms deployed at the Infrastructure level

Identity & Access Management



Customer

Electronically signs API request

API

Creates hash value using hash algorithm

1011000101

Encrypt hash value with private key

API

1011000101

Digital signature is sent to provider

Internet

1011000101

Decrypt the digital signature with public key

1110101101

Creates hash value using hash algorithm

1011000101

If the hash value matches, signature is valid

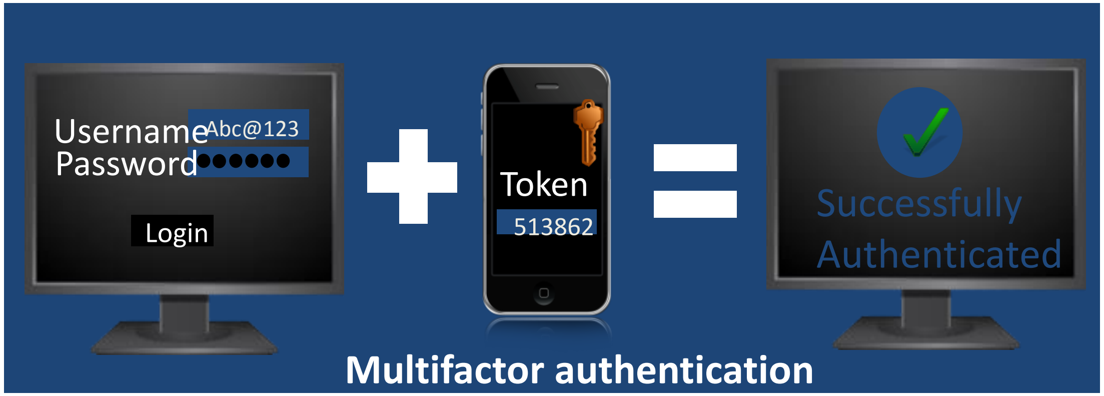
Provider

Digital Signature Certificate Process

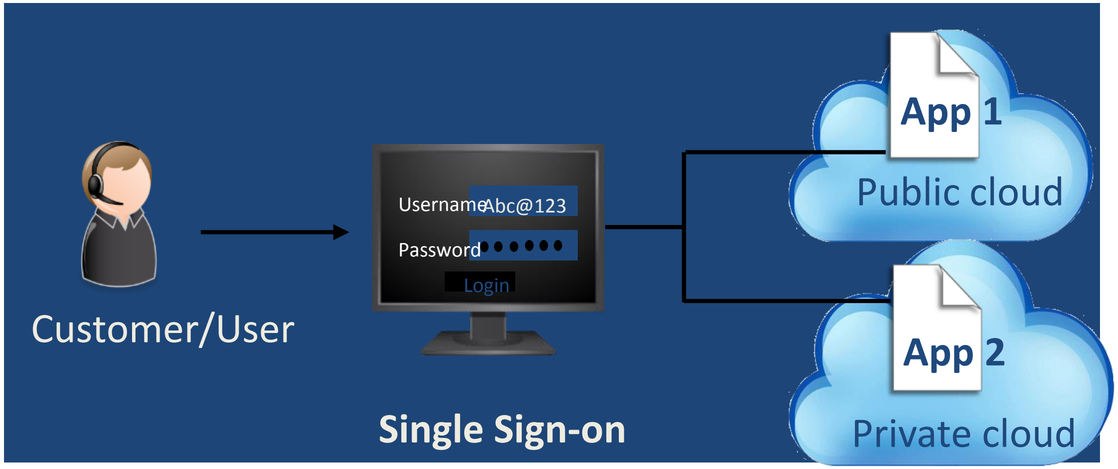
Identity & Access Management

Role-based Access Control

- A secure method of restricting access to the user based on their respective roles.
- Provides a greater degree of control over cloud resources.



Multifactor authentication



Single Sign-on

Application Hardening

Application Hardening

The procedure of applying a collection of techniques and best practices to reduce vulnerabilities in applications

Application hardening checklist

- Identify security policies and procedures
- Consider transmission of credentials over the network
- Implement ACI (Application Centric Infrastructure)
- Secure third party applications and tools
- Install current application updates or patches

Operating System Hardening

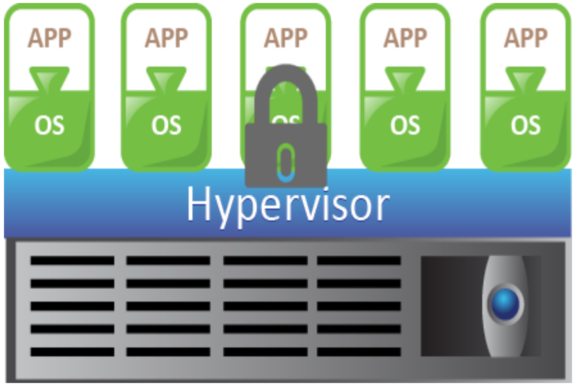
Operating System hardening includes:

- Deletion of unused files and programs
- Installation of current OS
- Configuration of the components following the hardening checklist
- Performing vulnerability scanning and penetration testing

Hypervisor Hardening

Hypervisor hardening includes:

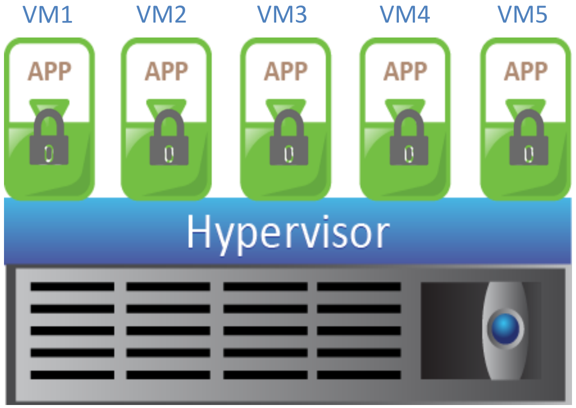
- Separation of management network from the VM network
- Installation of security critical hypervisor updates
- Accessing the management server be restricted to authorized administrators
- Given least privileges to service accounts
- Disabling the services which are not used in everyday operations.



Virtual Machine Hardening

Virtual Machine hardening includes:

- Change the default configuration of the VM
- Disconnection of the virtual components that are not required
- Ensuring that the security mechanisms are enabled, and are up-to-date
- Isolation of the VM network using VLANs
- Creation of the virtual machine from the VM template

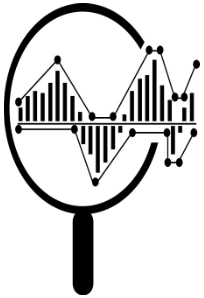


Sandboxing

Sandboxing

Is a mechanism that provides isolation capabilities by packaging the application and data with the infrastructure that it runs on along with the security policies

To test and verify the untrusted applications



To analyze the threats in the environment

To create a uniform environment

Firewall

Traditional Firewall

- Monitors the incoming and the outgoing network traffic
- Filters the traffic based on the defined set of security rules
- Establishes a barrier between the internal network and Internet

Cloud-based Firewall

- Implemented at the network level
- Protects Cloud infrastructure
- Offered in IaaS and PaaS

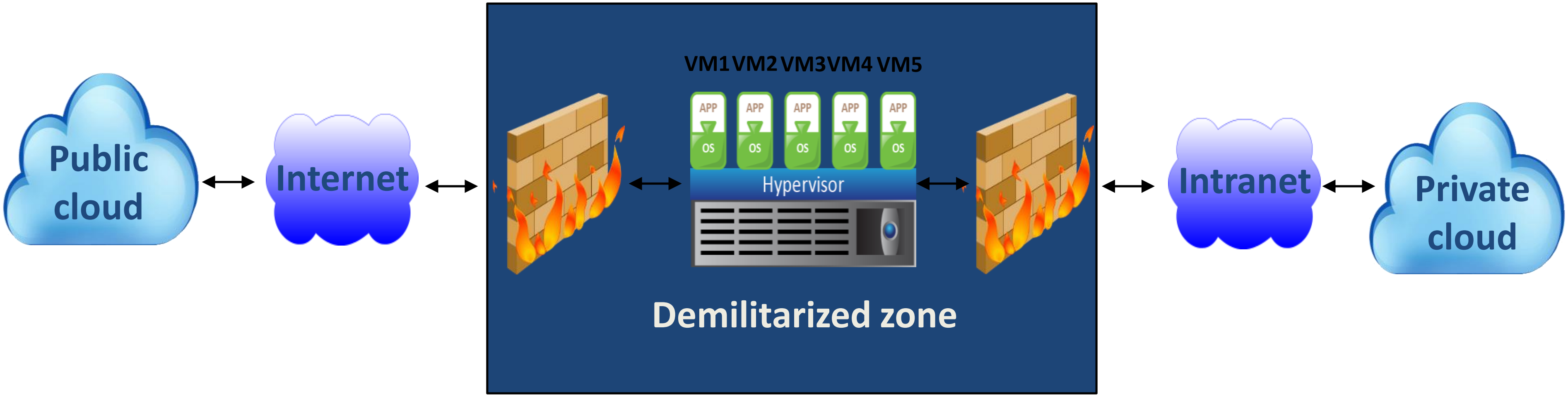
- Implemented at the host level
- Protects consumers infrastructure
- Offered in FWaaS, SaaS, SECaaS

Firewall Use Case: Demilitarized Zones

Secures all the internal resources while still allowing internet-based access only to the selected resources.

VMs that need the Internet access to use the public cloud are placed between two sets of firewalls.

Exposed compute systems or VMs may or may not be allowed to communicate with internal resources.



Demilitarized zone in a Hybrid Cloud Scenario

Intrusion Detection & Prevention Systems

Intrusion Detection System

A security tool that detects the events that can cause exploitation of vulnerabilities in the cloud provider's network or sever

Intrusion Prevention System

A security tool that prevents the events after they have been detected by the IDS

Intrusion Detection systems are classified as:

1. Signature-based
2. Anomaly-based

Intrusion Detection & Prevention Systems

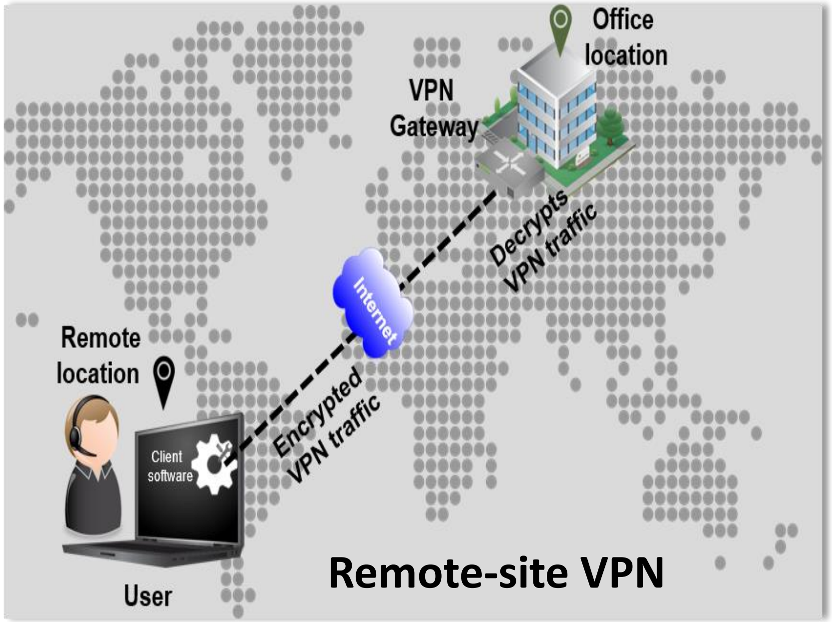
Signature-based IDS

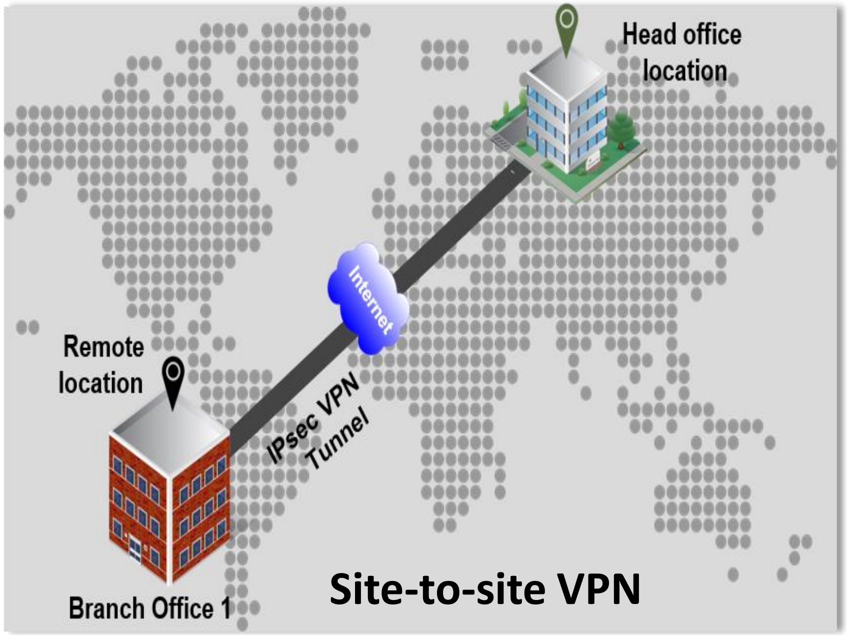
- Compares the signature against observed events by relying on a database that contains known attack patterns or signatures
- Requires constant updates for the database
- Ineffective with unknown attacks and variants of known attacks

Anomaly-based IDS

- Compares the observed events with the normal activities to identify the abnormal patterns
- Has a high risk of false positives
- Effective to detect new and unforeseen vulnerabilities

Network Segmentation





A remote customer initiates a remote VPN connection request using a VPN client software installed on their system.

IPsec protocol creates an encrypted tunnel from provider's site to the customer's site.

Network Segmentation

Network virtualization Implementation methods

Virtual Local Area Network

- Virtual Network created on a physical LAN
- Divide a large LAN into smaller virtual LANs or combine separate LANs into one or more virtual LANs

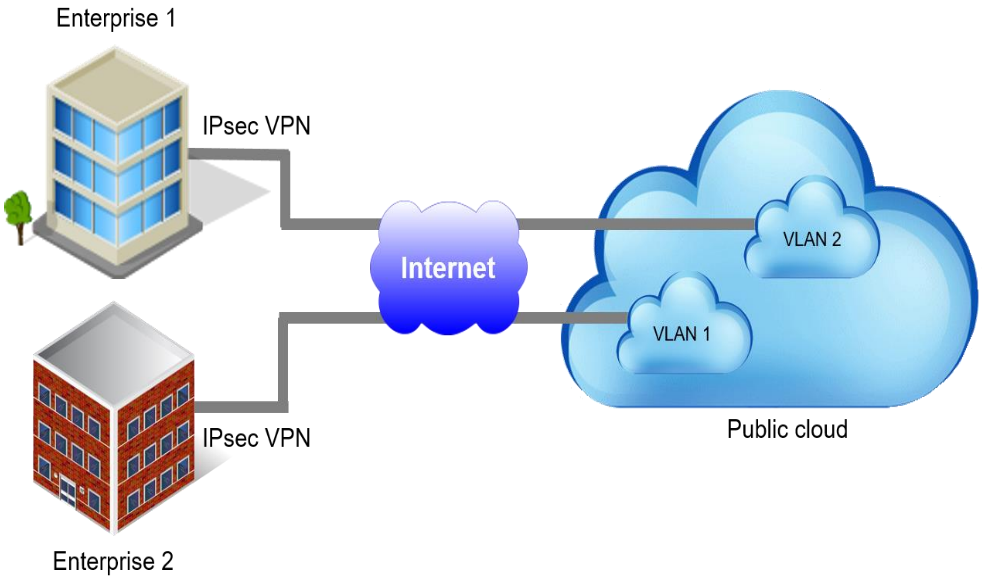
Virtual Storage Area Network

- Virtual network created on a physical SAN
- Builds larger consolidated fabrics and still maintain the required security and isolation between them

VLAN Extension in Hybrid Cloud

- Hybrid Cloud Use Case:
  - Workload Migration
  - Web Application Hosting
  - Application development & testing
  - Disaster recovery

- How it is implemented?
  - Using same IP address, subnet mask, and default gateways as the ones used in their own private data centers



VLAN extension from Enterprise Data Center to Public Cloud

Encryption & SSL

Data Encryption

Data Encryption is a cryptographic technique in which data is encoded and made readable to eavesdropping

Secure Socket Layer

A standard security technology that uses data in-flight encryption to establish a secure connection between a provider’s web server and customer’s browser through Internet.

Data in-flight Encryption

- Process of encrypting the data that is being transferred over a network
- Performed at network level

Data at-rest Encryption

- Process of encrypting the data that is stored on a storage device
- Performed at storage level

Data Shredding

- Data deleted by the customer or a process leaves traces on the system
- Deletes data or residual representations of data
- An attacker may perform unauthorized recovery of consumers' data
- Providers many create multiple copies of consumers data at multiple locations
- Data shredding mechanism should be deployed at all location where the data is stored

BYOD & Mobile Device Management

Bring Your Own Device (BYOD)

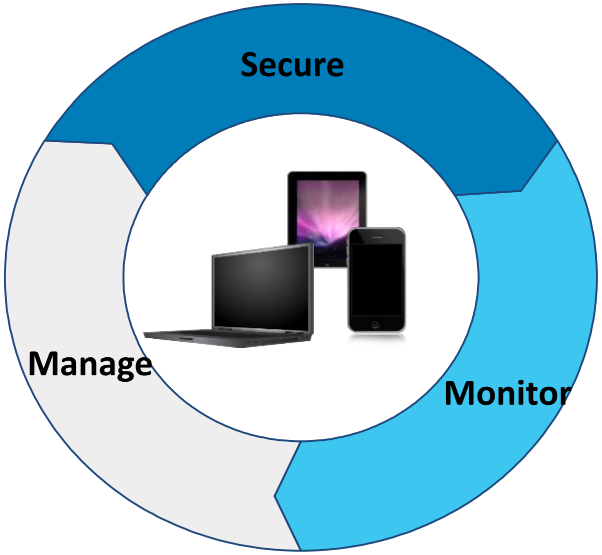
Bring Your Own Device (BYOD) is a policy at workplaces where employees bring their own mobile devices & connect them to the corporate network

Challenges

- BYOD policy at workplaces has created considerations for security and data privacy
- Mobile devices may have varied mobile service providers and varied operating systems

Solution

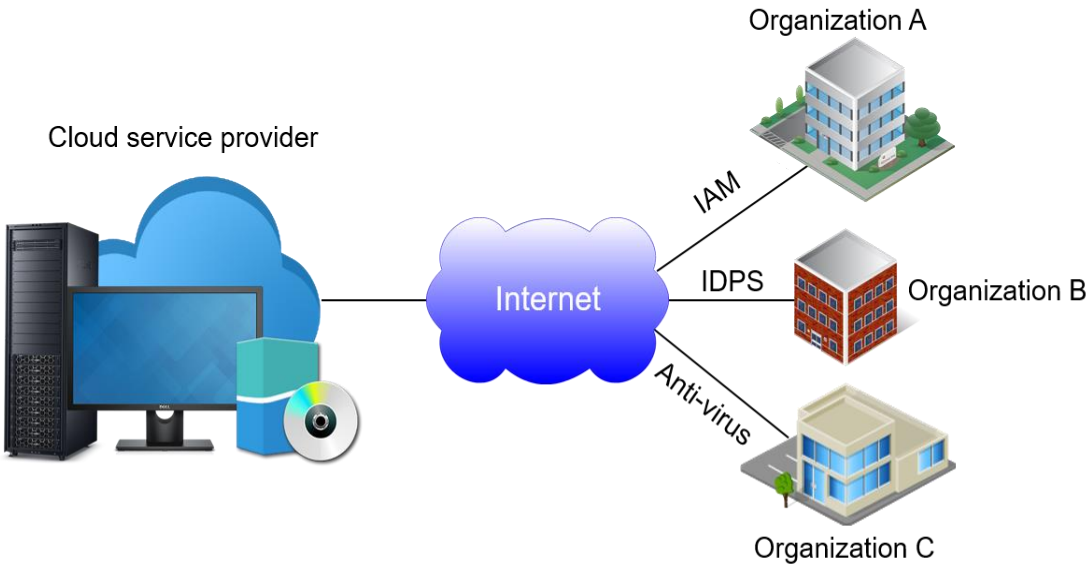
MDM is a security solution to monitor, manage, and secure the employees mobile devices that are being used in the workplace.



Security-as-a-Service

Security-as-a-Service

Is a business model in which a service provider integrates their security services into a corporate infrastructure on a subscription basis that is more cost effective than most individuals or corporates can provide on their own



Cloud service provider delivers various security mechanisms through Cloud - SECaaS

References

- “Cloud Infrastructures and Services - CIS” Course by Dell Technologies
- “Information Storage and Management – ISM” Course by Dell Technologies
- “IT Solutions for Digital Businesses - Virtualization and the Journey to the Modern Digital Workspace” Course by Vmware

For any inquiries e-mail me on:
maggie.ezzat@guc.edu.eg