Cloud Security Threats

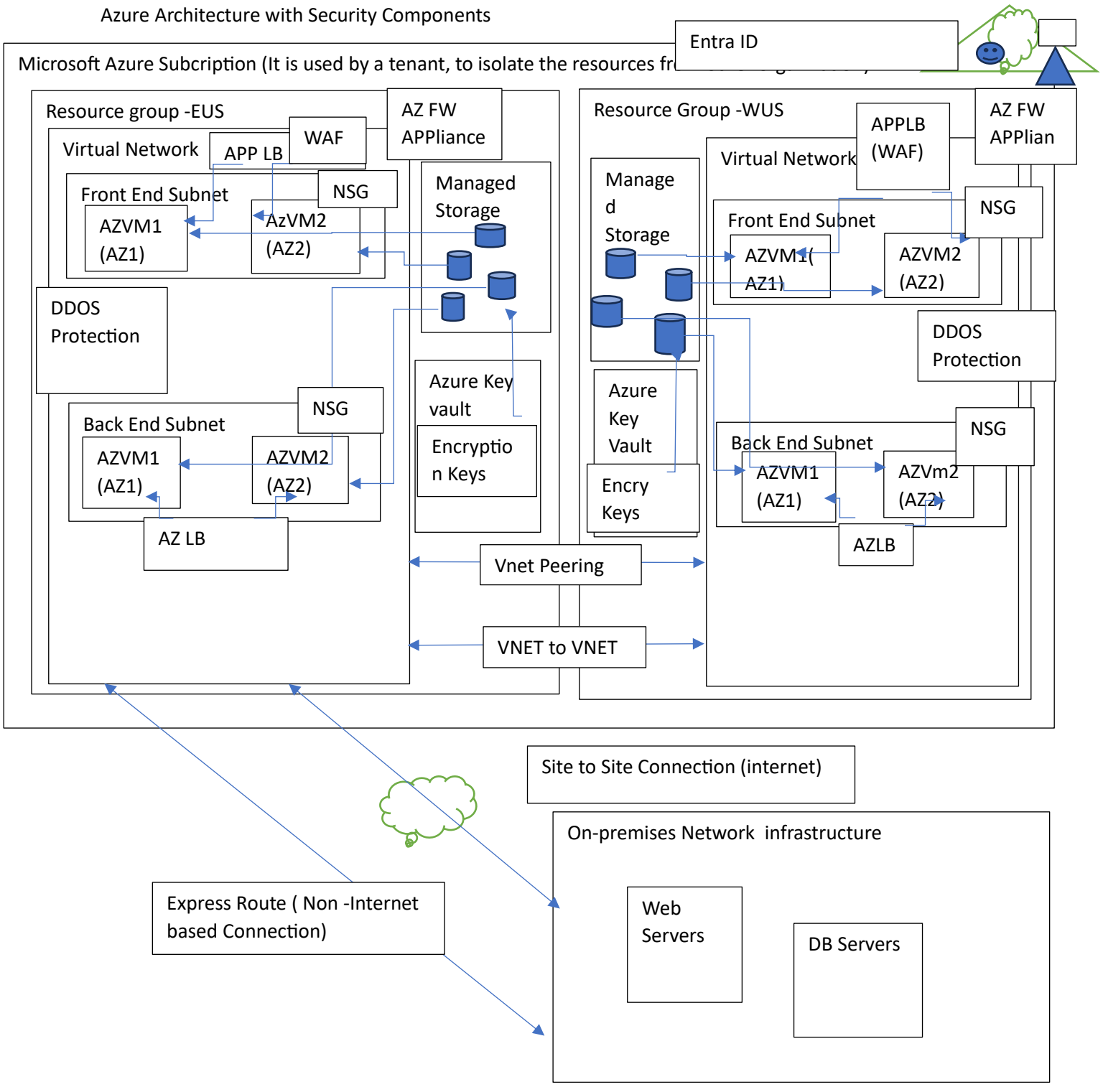
1. Insider threats
    a. Share the credentials
    b. Steal the credentials
    c. Sharing the security sensitive informations
    d. Sharing the documents
    e. Accessing the unwanted web sites
2. Account hijack
3. Exploits (Manually or automatically attacker will deploy the exploits (Malicious Software)
4. Insecure API, gateways, Virtual networks, load Balancers
5. Web application Attack
6. DDOS Attack (Distributed Denial of service attack)
7. Insecure Data at rest and Data in transit
8. Spectra and meltdown

Zero-Trust Security principles

Zero-Trust – Very Any request and Authenticate at all layers of IT Infrastructure in cloud

1. Implement Strong identity security (Insider Threats, Account Hijack, Exploits)
2. Apply Security In all the Infrastructure and platform layers (Virtual Network, gateways, load balancers, Virtual Machines and all) (Web Application attack, DDOS Attack, API and Other Network services attack)
3. Secure data at Rest and Secure Data in transit (data Breach and Data Disk Stealing)
4. Apply Security Best Practices and Monitor security information and Events (increase the security score, Avoid future security problems and we can enhance the Security posture)

Azure Architecture with Security Components



Site to Site Connection (internet)

On-premises Network infrastructure

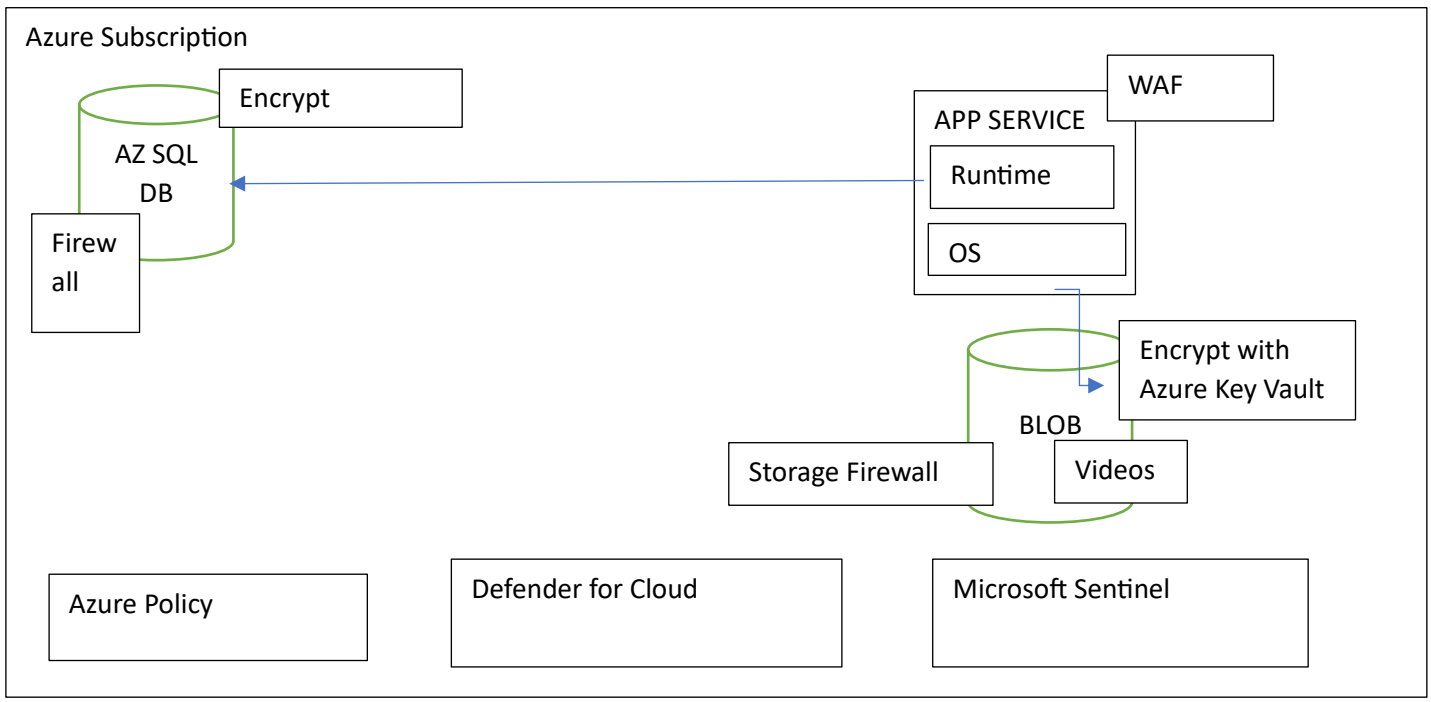
Web
Servers

DB Servers

Express Route (Non -Internet
based Connection)

Key Notes:

1. Azure Subscriptions – Used by a tenant to isolate the resources from other organization
2. Entra ID – It is a Cloud directory service, Used to create, Manage and protect identities
3. Resource Group -Region – It is a Container, to organize the resources based on the region
4. Virtual Network – A Logical Network Infrastructure
5. Front End Subnet – Used to Deploy Internet facing azure vms such as web servers and API
6. Back End Subnet – Used to deploy Non Internet facing Azure VMS Such as DB Servers
7. Azure VMS – A virtual servers or desktops to deploy applications
8. Managed storage – To Create and Manage Azure Virtual Machine disks
9. Azure Load Balancer – To Distribute the load and Failover any TCP/UDP Traffic Between the azure VMS
10. Application Load Balancer – Used to do Load Balancing and failover Web Applications (HTTP and HTTPS)
11. NSG – Network security Group – Used to filter the network traffic at subnet and VM level
12. Web application firewall – To protect web application attack
13. Azure Firewall Appliance – Used protect inbound and outbound virtual network network, application and URL based traffic
14. DDOS Protection service – used to protect the flood of malicious traffic
15. Azure Key Vault – To create encryption keys and Encrypt the managed disk (VM DISK)
16. Vnet Peering – to connect vnets located in different region (NON internet based, Non Encrypted connection (Private connection))
17. VNET to VNET – to Vnets Located in different region (Internetbased Connection, Encrypted connection)
18. Site to site – To Connect on-premises and Azure VNET (Internet based encrypted connection)
19. Express Route – To Connect onpremises and Azure VNET (Non Internet Based private connection and Non Encrypted connection)



Key Notes

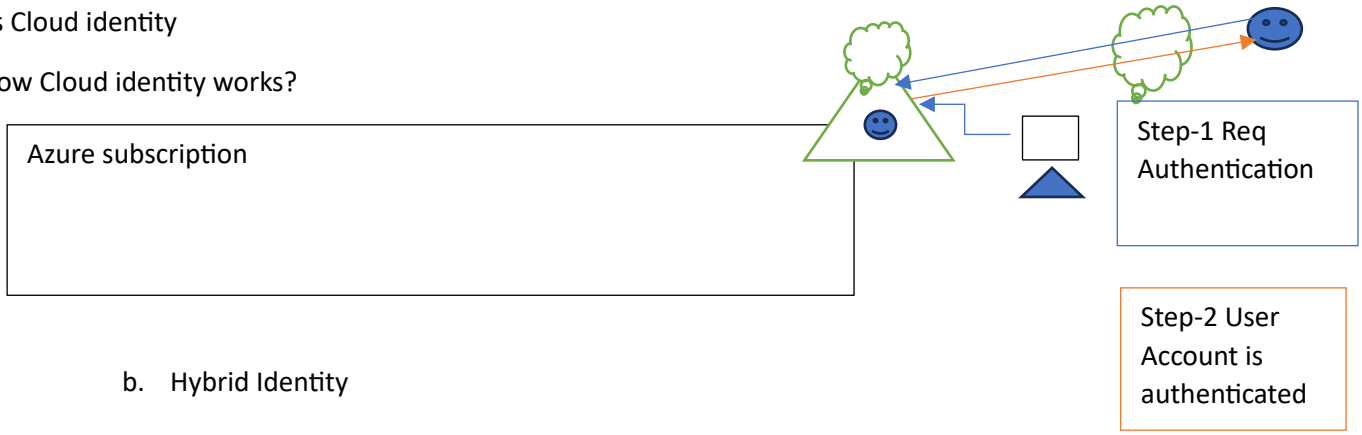
20. App Service – It is a Platform as service, Used to Create, Build and Deploy web app, mobile app, and API
21. Azure SQL DB – To store Structured data
22. Blob Storage – Used to store objects (any files such as text, Videos, images etc)
23. Storage Firewall – To Protect blob storage
24. Azure Policy - Used to Security and Compliance Policy
25. Defender for cloud and sentinel – Used to Check security score, Scurity posture, events, Best practices.

Entra ID

1. It is Cloud Directory service
2. Used to Create, Manage, protect and authenticate the identities
3. Entra ID is Provisioned automatically while creating azure subscription
4. By Default Entra ID is Configured default domain name *.onmicrosoft.com (Eg: Optum.onmicrosoft.com)
5. Entra Id also supports Custom domain name (divya200.testrls.xyz)
6. Entra ID Supports Two types of identities
    a. Cloud Identity

All the identities Created directly in Entra ID Since we don't have on-premises infrastructure is known as Cloud identity

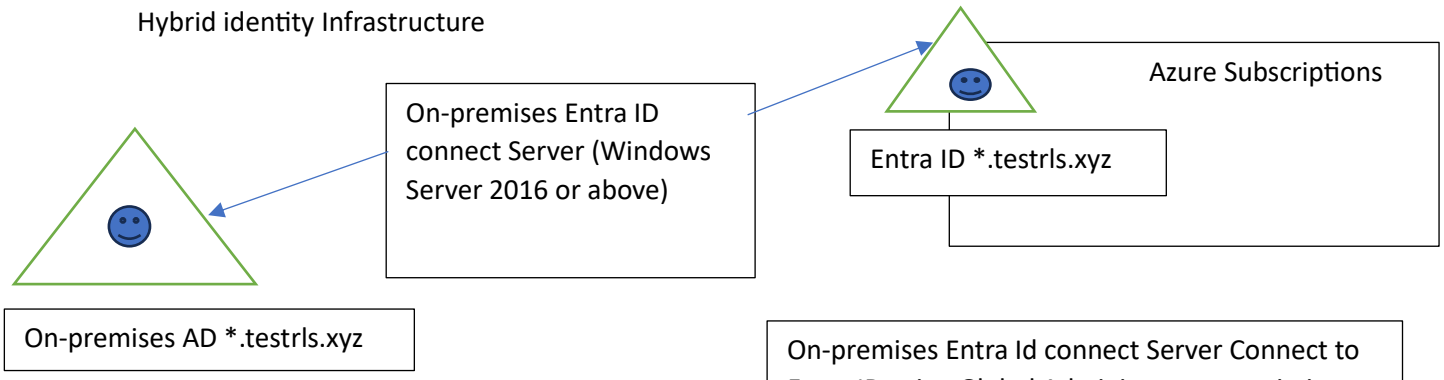
How Cloud identity works?



    b. Hybrid Identity

All identities are created in on-premises and synchronized to Entra ID is known as Hybrid identity to provide single sign-on (Same user account and password to access local apps and azure application)

Hybrid identity Infrastructure



On-premises Entra Id connect Server Connect to Entra ID using Global Administrator permission

On-premises Entra ID connect server to on-premises AD Enterprise administrator credential is used

Hybrid Identity Authentication methods:

1. Password Hash Synchronization
2. Pass-through authentication
3. Federated authentication

Any Identities Protect from password stealing and Password sharing

To Protect from Password stealing, the following policies are used:

MFA – Multifactor Authentication

User will be authenticated using password with mobile and app verification