Azure Security Technologies (AZ-500)

Types of Cloud Security Threats

1. Insider threats
   1. Share credentials
   2. Steal credentials
   3. Share sensitive information
   4. Sharing docs
   5. Accessing unwanted websites
2. Account hijack
3. Exploits (Manual/Automatic attacker will deploy malicious code)
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 principals - Verify any request and authenticate at all layers of IT Infra in cloud

|  |  |
| --- | --- |
| Implement | Avoids |
| Strong Identity Security | Insider Threats, Account Hijack, Exploits |
| Apply Security in all the infrastructure and platform layers (VNet, Gateway, LBs, VMs etc) | Web App, DDoS, API and other network attacks |
| Secure data at rest and transit | data breach and data disk stealing |
| Apply Security Best Practices and Monitor security information and events | Increase security score, avoid future security problems, enhance security posture |

Azure Architecture with Security Components

Microsoft Azure Subscription (It is used by a tenant, to isolate the resources from other org)

WAF

Az FW Appliance

NSG

NSG

Az LB

App LB

AZVM1(AZ1)

AZVM2(AZ2)

AZVM2(AZ2)

AZVM1(AZ1)

Front End Subnet

Back End Subnet

Managed Storage

Virtual Network

Resource Group - EUS

DDoS Protection

Azure Key Vault

Encryption Keys

Traffic -> Virtual Network (AZ FW Appliance) -> Subnet(NSG) -> App LB(WAF) -> VM(NSG) -> Az LB ->Backend Subnet(NSG) -> VM(NSG)

FW Appliance – Network filtering, Application filtering and URL filtering

NSG - protocol level filtering

Microsoft Azure Subscription (It is used by a tenant, to isolate the resources from other org)

Az FW Appliance

NSG

NSG

Az LB

App LB(WAF)

AZVM1(AZ1)

AZVM2(AZ2)

AZVM2(AZ2)

AZVM1(AZ1)

Front End Subnet

Back End Subnet

Managed Storage

Virtual Network

Resource Group - EUS

DDoS Protection

Azure Key Vault

Encryption Keys

VNET to VNET

VNET Peering

Microsoft Azure Subscription (It is used by a tenant, to isolate the resources from other org)

Az FW Appliance

NSG

NSG

Az LB

App LB(WAF)

AZVM1(AZ1)

AZVM2(AZ2)

AZVM2(AZ2)

AZVM1(AZ1)

Front End Subnet

Back End Subnet

Managed Storage

Virtual Network

Resource Group - WUS

DDoS Protection

Azure Key Vault

Encryption Keys

VNET to VNET – travels through internet, IPSec protocol, needs encryption

VNET Peering – azure backbone, no encryption needed

DB Servers

Web Servers

Site to Site Connection (Internet)

Express Route (Non-Internet)

On-Prem network infrastructure

Cloud

Key Notes:

1. Azure Subscription – used by tenant to isolate resources from other orgs
2. Entra ID – Cloud directory service used to create, manage and protect identities
3. RG-Region – It is a container to organize the resources based on the region
4. VNet – A Logical Network Infra
5. Front End Subnet – Used to deploy Internet facing azure VMs such as web services and API
6. Backend Subnet – Used to deploy non internet facing servers(Azure VMs Ex. DB Servers)
7. Azure VMS – Virtual servers or desktops to deploy applications
8. Managed Storage – To create and manage azure VM 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 load balance and failover web applications (http & https)
11. NSG – 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 to protect inbound and outbound VNet 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 – connect VNets located in different region(Non internet based, non encrypted connection(Private Connection))
17. VNET to VNET – Connect VNETs located in different region(Internet based, encrypted)
18. Site to Site – Connect on-prem and azure VNET (Internet based encrypted connection)
19. ExpressRoute – To connect on-prem and azure VNET (Non Internet based private connection and non encrypted)

Encrypt with Azure Key Vault

Encrypt with Azure Key Vault

App Service

BLOB

AZ SQL DB

Runtime

OS

DB Firewall

Storage Firewall

Videos

Microsoft Sentinel

Defender for Cloud

Azure Policy

Key Note:

1. App Service – It is a Platform as Service used to create build and deploy web application, Web App, Mobile App and API
2. Azure SQL DB – To store structured Data
3. Blob Storage – Used to store objects (any files Ex. Text, videos, images etc.)
4. Storage Firewall – To protect blob storage
5. Azure Policy – Used to security and compliance policy
6. Defender for cloud and Sentinel – Used to check security store, Security Posture, events, best practices

Entra ID

1. Cloud Directory Service
2. Used to Create, Manage, protect and authenticate the identities
3. Entra IS is provisioned automatically while creating azure subscription
4. By default, configured with a default domain name \*.onmicrosoft.com
5. Supports custom domain name
6. Supports two types of Identities
   1. Cloud Identity – created directly in Entra ID

Azure Subscription

Step-2 User Account is authenticated

Step-1 Req Authentication

* 1. Hybrid Identity – created on-prem and synchronized to Entra ID(Same account and password to access local and cloud apps. SSO)

Hybrid Identity Infra

On-prem Entra ID connect Server (Windows Server 2016 or above

Azure Subscriptions

Entra ID \*.testrls.xyz

On-prem AD \*.testrls.xyz

On-prem Entra ID connect Server to On-prem AD Enterprise Admin permission

On-prem Entra ID connect Server Connect to Entra ID using Global Admin permission

Hybrid Identity Authentication Methods:

1. Password Hash Sync
2. Pass-through
3. Federated

Protect Identities from password stealing and sharing

Policies

MFA – User will be authenticated using password with mobile and app verification

Day2

To prevent identities to share the password, we must enable the following policy

* Conditional access policy

Using this policy we can allow or block users to login based on the conditions

Eg: Do not allow users to login from anywhere except the corporate IP address 80.80.80.80/32

To apply conditional access policy the following requirement are needed

1. Entra ID Premium license
2. Entra ID Mobility + security e5 license

Hybrid Identity Authentication Methods

1. PHS – Password Hash Synchronisation

All the identities are synchronized from on-prem AD(Domain Controller) to Entra ID with passwords

Step-1 Req auth UN and PWD

Entra ID connect Server

How it works

Step-2 Authenticated

Authentication method: PHS

Password Sync: Enabled

Entra ID

On-prem AD

Problem:

Storing password in Entra id

Adv:

SingleSignOn

1. PTA – Pass Through Authentication

All the identities are synchronized from on-prem AD to Entra id without password

Step-1 Req auth UN and PWD

Step-2 Entra ID will receive the credentials and encrypt the creds and place cred in password queue

Entra ID connect Server

How it works

Step-3 PTA agent will poll encrypted creds and decrypt the creds

Authentication method: PTA

Step-4 PTA agent will connect to on-prem AD and request to validate creds

Password Sync: Disabled

Step-5 On-prem AD validates creds. If correct will issue success else failure token to PTA Agent

Entra ID

PTA Agent

On-prem AD

Step-6 PTA agent issue success token to Entra ID

Step-7 User is Authenticated

Password Stealing – MFA

? - Conditional Access

Password spray attack, account hijack – user risk

? - signIn Risk

NSG – Network Security Group

Virtual Firewall

Used to filter network inbound/outbound traffic

Supports any TCP and UDP protocols(port no 0-65535)

Supports Allow and Deny rules

NSG rules are processed based on Priority. If conflict, lower priority will take higher precedence

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rule Name | Priority | Protocol | Service | Port No | Action |
| Rule1 | 100 | TCP | RDP | 3389 | Allow |
| Rule2 | 200 | TCP | RDP | 3389 | Deny |

NSG rules associated with Azure VMs and Subnets

By default

deny all inbound external traffic

allow all outbound external traffic

Exercise1: If NSG is not associated with any Azure VMs and Subnet what is the security level?

Security Level: fully blocked

NSG

Vnet

Subnet

NSG

AZVMS

Azure Firewall Appliance

Vnet

AzureFirewallSubnet

NSG

Subnet

Azfirewallapp100

NSG

AZVMS(webserver100)

NAT Rule Collection (allows inbound traffic for the respective protocols and Services)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| NAT rule Collection100 |  |  |  |  |  |  |  |
| Rule name | Source Type | Source | Protocol | Des Port | Destination | Translated Address | Translated Port |
| RDPRule100 | Ipaddress | \* | TCP | Firewall RDP PortNo(3389) | Firewall Associated Public IP Address | Private IP address of Azure VM (Web Server) | Azure VMS (webserver Port for RDP-3389) |

1 firewall for each vnet

[Friday 4:14 pm] Sundar-Trainer

1. Read all the key notes
2. Do the practice of all the components
3. Read the Model Questions from measureup.com
4. Create a Free trial account and explore all the  components
5. Read FAQ from Docs.Microsoft.com

like 4

[Friday 4:14 pm] Sundar-Trainer

[Sundararajan.s@poutlook.com](mailto:Sundararajan.s@poutlook.com)

[Friday 4:14 pm] Sundar-Trainer

9791107115