

Project Summary: Secure Architecture with Azure VNets, NSGs, and Application Gateway

1. Project Title:

Design and Implementation of a Secure Azure Architecture

1.1 Project Prepared and Submitted By: Mr. Jithin Thiruppathi // Email – tjithin21@gmail.com

1.2 Project Submitted To: GUVI Geek Network Private Limited

1.3 Guvi Batch No: Batch: CC1WE-E

1.4 Submitted Date: 07-08-2024

2. Project Description:

Design a secure, scalable architecture using Azure Virtual Networks (VNets), Network Security Groups (NSGs), and Azure Application Gateway. The architecture will support a multi-tier application with a web frontend, business logic layer, and database tier, all hosted in separate VNets. Key features will include advanced load balancing, traffic management, and security.

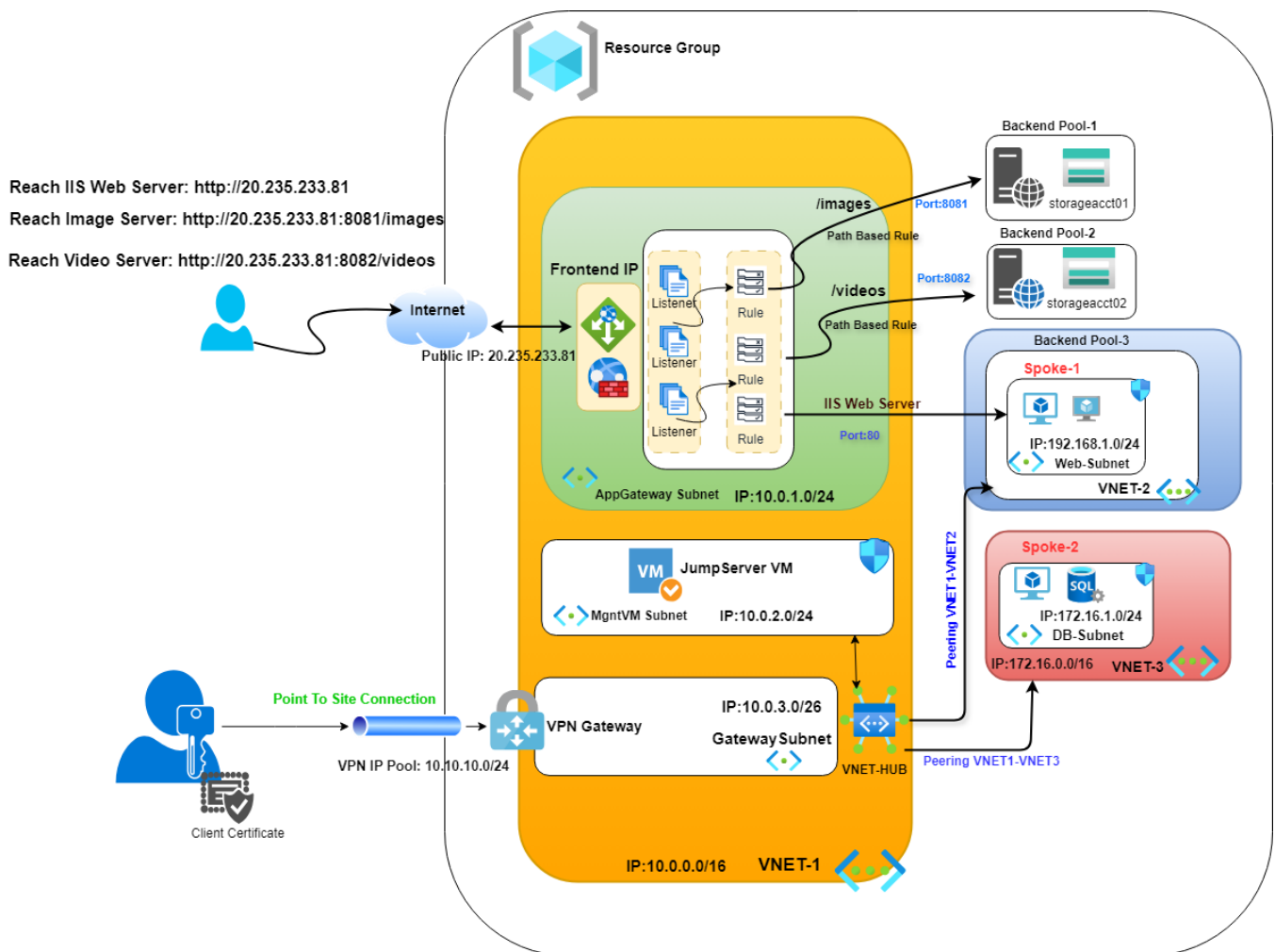
3. Goals and Objectives:

- **Secure Segmentation:** Create separate VNets for each application tier to ensure isolation and security.
- **Traffic Management:** Implement Azure Application Gateway for effective traffic handling, including advanced load balancing features.
- **Enhanced Security:** Configure NSGs and WAF to protect against threats and ensure safe traffic flows.
- **Scalability:** Use auto scaling to dynamically adjust resources based on traffic demand.

4. Architecture Components:

- **Virtual Networks (VNets):**
 - **VNET-1:** Used for Application Gateway, Jump Server, VPN Gateway and VNET-1 act as HUB for internal VNET communication.
 - **VNET-2:** Secure Web Server hosted
 - **VNET-3:** DB server for managing Database secure.
- **Network Security Groups (NSGs):**
 - **Jump Server NSG:** Allows traffic from VPN Gateway tunnel only.
 - **Web Server NSG:** Permits traffic from Web Frontend (VNET-1).
 - **Database NSG:** Restricts access to only the Business Logic VNet.(Private endpoint created for internal access)
- **Azure Application Gateway:**
 - **Health Probes:** Monitor and ensure the health of backend instances.
 - **Path-Based Routing:** Direct traffic based on URL patterns to appropriate backend pools.
 - **Web Application Firewall (WAF):** Protects against common web threats.
 - **Auto scaling:** Auto scaling of Application Gateway as traffic hits.
- **Virtual Network Gateway: P2S**
 - **VPN Gateway:** Secure access to VNets from end user.

5. Architecture Design and Resource Details:



5.1 Application Gateway:

Azure Application Gateway is a web traffic load balancer and application delivery controller that helps manage and secure traffic to your web applications. It operates at the application layer (Layer 7 of the OSI model), which means it can handle traffic based on more complex rules, such as HTTP requests and URL paths.

The key features of Azure Application Gateway in a condensed format:

- **Layer 7 Load Balancing:** Distributes traffic based on URL paths and HTTP headers.
- **Web Application Firewall (WAF):** Protects against web attacks and allows custom rules.
- **SSL Termination:** Handles SSL/TLS encryption and decryption; supports end-to-end SSL.
- **Path-Based Routing:** Routes traffic based on URL paths.
- **Host-Based Routing:** Routes traffic based on domain names.
- **Session Affinity:** Routes requests from the same client to the same backend using cookies.
- **Autoscaling:** Automatically scales instances based on traffic demand.

- **Health Probes:** Monitors backend server health to route traffic only to healthy instances.
- **Multi-Site Hosting:** Supports multiple applications on a single gateway instance.
- **Azure Integration:** Connects with VNets, Azure Monitor, and Azure Security Center

5.2 Virtual Network Gateway:

Azure Virtual Network Gateway is a service that provides connectivity between your Azure Virtual Network (VNet) and other networks. It acts as a bridge for secure communication between your Azure environment and on-premises networks or other Azure VNets.

Key Features

VPN Gateway:

- **Site-to-Site VPN:** Connects on-premises networks to Azure VNets over the internet using IPsec/IKE VPN tunnels.
- **Point-to-Site VPN:** Provides secure, remote access for individual devices to Azure VNets, typically used for remote workers.
- **VNet-to-VNet VPN:** Connects multiple Azure VNets together, either within the same region or across different regions.

ExpressRoute Gateway:

- **ExpressRoute:** Provides a private, high-speed, low-latency connection between your on-premises network and Azure, bypassing the public internet.
- **Global Reach:** Allows you to connect Azure VNets in different regions via ExpressRoute circuits.

In This Project, I used Point to Site VPN connection with to VNET-1

5.3 Jump Server:

A jump server (also known as a jump box or bastion host) is a special-purpose server used to access and manage other servers or systems that are located in a private network. It acts as an intermediary or "gateway" to securely access internal resources from an external network.

In This Project, Jump Server is not exposed to Public network. It can be accessible only via Azure Bastion and VPN Gateway. For reach any other server we need to access via jump server only.

5.4 Static Website // Path Based (Image & Video):

A static website is a type of website where the content remains the same for every visitor and is delivered to users as-is, without any server-side processing or dynamic content generation. Static websites are composed of fixed HTML, CSS, and JavaScript files that are served directly from a web server or a content delivery network (CDN).

In This Project, Created Two storage account and hosted image and video static website and added as backend pool to application gateway for path based routing. Storage account has been access resisted to public and only read accessible via internal vNet.

5.5 Web Server:

A web server is a software or hardware that delivers web pages and other content to users over the internet.

In This Project, I build IIS Web Server in secure Vnet-2 and added to backend pool of application gateway for web traffic.

5.6 Database Server:

A database server is a system that stores and manages data, allowing other applications or users to access and manipulate that data over a network.

Examples:

Relational Databases: MySQL, SQL Server.

NoSQL Databases: MongoDB, Redis.

In This project, I Isolated DB server in VNET-3 and created private endpoint to access the DB.

5.7 HUB & SPOKE:

In Azure, the "hub and spoke" model is a network topology used to manage and organize virtual networks (VNETs) for optimal security, scalability, and management.

- **Hub:** Think of this as the central point or main hub of a network. It holds shared services like firewalls, VPNs, and sometimes shared databases.
- **Spokes:** These are like the branches extending from the hub. Each spoke is a separate network used for different purposes, like development, testing, or production.

How It Works

- **Central Hub:** The hub connects to everything and manages shared resources.
- **Separate Spokes:** Each spoke connects only to the hub, not directly to other spokes. This keeps them isolated from each other.
- **Traffic Flow:** If a spoke needs to talk to another spoke, it goes through the hub. This simplifies the network setup and keeps things organized.

In This Project, VNET-1 act as HUB and VNET-2 and VNET-3 as Spoke. VNET Peering from VNET-1 to VNET-2 & VNET-1 to VNET-3. The VNET-2 & VNET-3 use VNET-1 as gateway to route the traffic.

6. Implementation and Testing of Design:

Configuration Details									
S.No	Resource Name	Type	Associated Network	Network IP Segment	Subnet Name	Subnet IP Details	Public IP / Private IP	Port Opened / Description	Remarks
1	VNET-1 (HUB)	Virtual Network	N/A	10.0.0.0/16	default	10.0.0.0/24			
		Virtual Network			AppGw-Subnet	10.0.1.0/24			
		Virtual Network			MgmtSubnet	10.0.2.0/24			
		Virtual Network			GatewaySubnet	10.0.3.0/26			
2	VNET-2 (SPOKE-1)	Virtual Network	N/A	192.168.0.0/16	default	192.168.0.0/24			
		Virtual Network			Web-Subnet	192.168.1.0/24			
3	VNET-2 (SPOKE-2)	Virtual Network	N/A	192.168.0.0/16	default	172.16.0.0/24			
		Virtual Network			DB-Subnet	172.16.1.0/24			
4	VPN_Gateway	Virtual Network Gateway (P2S)	VNET-1			10.10.10.0/24	74.225.167.116		
5	AppGateway	Application Gateway L7 Load Balancer	VNET-1	N/A	AppGw-Subnet		20.235.233.81 (Public)	HTTP:80, tcp/udp:8080,8081	
	WAF-1	WAF policy							
6	JumpServer	VM	VNET-1		MgmtSubnet	10.0.2.0/24	10.0.2.4 (Private)	RDP-3389 Allowed via VPN only	Used for Managing all VM
7	IIS-Webserver	VM	VNET-2		Web-Subnet	192.168.1.0/24	192.168.1.4 (Private)	RDP-3389 Allowed via JumpServer only, HTTP: 80, HTTPS:443	IIS Web Site Loaded
8	DB-VM	VM	VNET-3		DB-Subnet	172.16.1.0/24	172.16.1.5 (Private)	RDP-3389 Allowed via JumpServer only	SQL DB VM used for manaing DB server (mysqlqldbserver01.datab ase.windows.net)
9	storageaccproject01	Storage account	VNET-1		All Subnet		Accessable only in VNET-1 network		Usede for Static Image Website
10	storageaccproject02	Storage account	VNET-1		All Subnet		Accessable only in VNET-1 network		Used for Static Video Website

6.1 Snapshots & Testing:

- 6.1.2 Application Gateway details and Backend Mapped Details

Configuration: WAF V2 / Auto scale Mode

Backend Pool:

Microsoft Azure

Home > AppGateway

AppGateway | Backend pools

Search backend pools

Name	Rules associated	Targets
AppGw-backend	1	1
Image-Backend	1	1
Video-Backend	1	1

Backend Setting or Http Setting:

Microsoft Azure

Search resources, services, and docs (G+I)

Home > AppGateway

AppGateway | Backend settings

Search

+ Add Backend health Feedback

Search Backend settings

Name	Port	Protocol	Cookie based affinity	Custom probe
Appgwt-httpsetting	80	Http	Disabled	IIS_Probe
Image-httpsetting	443	Https	Disabled	image_probe
Video_httpsetting	443	Https	Disabled	video_probe

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Web application firewall
Backend pools
Backend settings
Frontend IP configurations

Frontend IP:

Microsoft Azure

Search resources, services, and docs (G+I)

Home > AppGateway

AppGateway | Frontend IP configurations

Search

Feedback

Search frontend IP configurations

Type	Status	Name	IP address	Associated listeners
Public	Configured	appGwPublicFrontendIpV4	20.235.233.81 (Appgwt-PubIP)	Appgw_List-0, 2 more
Private	Not configured	-	-	-

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Web application firewall
Backend pools
Backend settings
Frontend IP configurations

WAF Policy associated with Application Gateway:

Microsoft Azure

Search resources, services, and docs (G+I)

Home > Load balancing | Application Gateway > AppGateway | Web application firewall > WAF-1

WAF-1 | Associated application gateways

Associate this WAF policy with a specific application gateway, listener, or route path. A WAF policy can be associated with multiple listeners, route paths, and application gateways. Associating with an application gateway will remove and replace existing WAF policy associations with the selected application gateway. [Learn more about managed rule sets](#)

+ Add association Remove association Refresh

Filter for any field

Association type: all Application Gateway: all Resource Group: all HTTP Listener: all Route Path: all

Association type	Application Gateway	Resource Group	HTTP Listener	Route Path
<input type="checkbox"/>	Application Gateway	MyProject01		
<input type="checkbox"/>	HTTP Listener	MyProject01	AppGW_List-1	

Overview
Activity log
Access control (IAM)
Tags
Settings
Policy settings
Managed rules
Custom rules
Associated application gateways
Sensitive data
Properties

Listener:

Microsoft Azure

Search resources, services, and docs (G+/I)

tjithin21@outlook.com

DEFAULT DIRECTORY (TJITHIN21...

Home > AppGateway

AppGateway | Listeners ☆ ...

Search

Web application firewall

Backend pools

Backend settings

Frontend IP configurations

Private link

SSL settings

Listeners

Rules

Application gateway provides native support for websocket across all gateway sizes. There is no additional configuration required to enable or disable websocket support. If a websocket traffic is received on the Application Gateway, it is automatically directed to the WebSocket enabled backend server using the appropriate backend pool as specified in application gateway rules. [Learn more about listeners and WebSocket support.](#)

Search listeners

Name	Port	Protocol	Frontend IP	Associated rule	Host name
Appgw_List-2	8082	HTTP	Public IPv4	Appgw_Rule-2	> - ...
AppGW_List-1	8081	HTTP	Public IPv4	Appgw_Rule-1	> - ...
Appgw_List-0	80	HTTP	Public IPv4	Appgw_Rule-0	> - ...

SSL Policy

The SSL policy defines the SSL protocol version and available ciphers. Choose from one of the predefined policies or create a custom security policy to match your organizational security requirements. These policies apply to all HTTPS listeners unless they are overridden by listener specific SSL Policy under SSL settings. [Learn more about SSL policy.](#)

Selected SSL Policy: Default (change)

Rules:

Microsoft Azure

Search resources, services, and docs (G+/I)

tjithin21@outlook.com

DEFAULT DIRECTORY (TJITHIN21...

Home > AppGateway

AppGateway | Rules ☆ ...

Search

Web application firewall

Backend pools

Backend settings

Frontend IP configurations

Private link

SSL settings

Listeners

Rules

+ Routing rule

Backend health

Feedback

Search rules

Name	Type	Listener	Priority
Appgw_Rule-0	Basic	Appgw_List-0	1 ...
Appgw_Rule-1	Path-based	AppGW_List-1	2 ...
Appgw_Rule-2	Path-based	Appgw_List-2	3 ...

Health Probes:

Microsoft Azure

Search resources, services, and docs (G+/I)

tjithin21@outlook.com

DEFAULT DIRECTORY (TJITHIN21...

Home > AppGateway

AppGateway | Health probes ☆ ...

Search

Web application firewall

Backend pools

Backend settings

Frontend IP configurations

Private link

SSL settings

Listeners

Rules

Rewrites

Health probes

+ Add

Refresh

Delete

Feedback

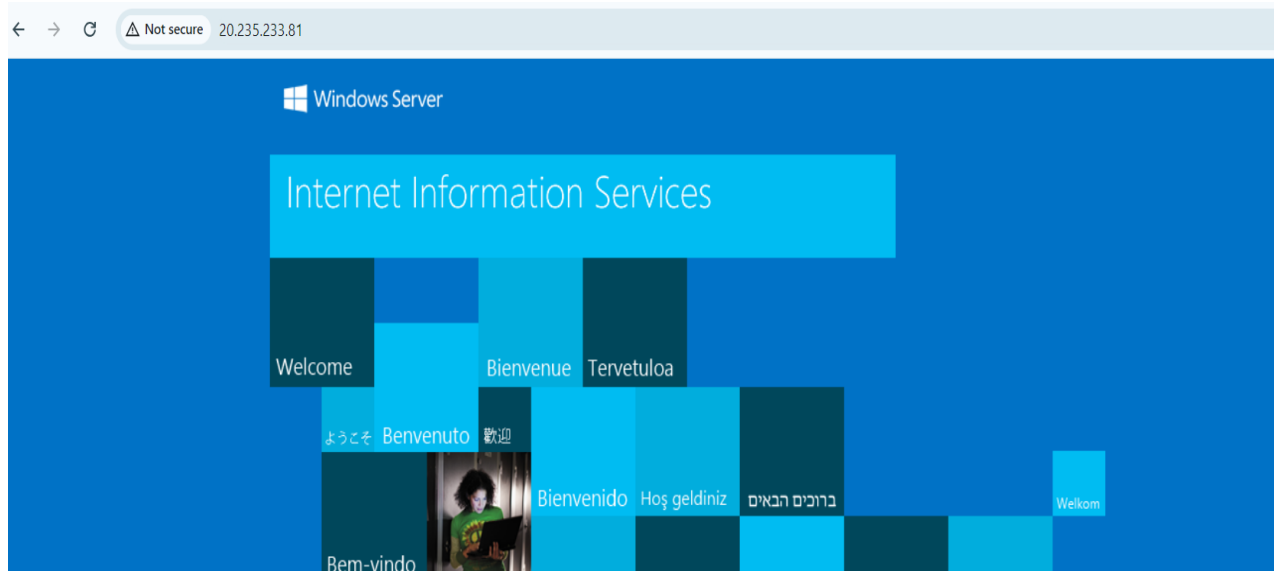
Search probes

Name	Protocol	BackendSettings	Host	Path	Timeout (seconds)
<input type="checkbox"/> IIS_Probe	Http	> 1	192.168.1.4	/	30 ...
<input type="checkbox"/> video_probe	Https	> 1		/videos	30 ...
<input type="checkbox"/> image_probe	Https	> 1		/images	30 ...

Results:

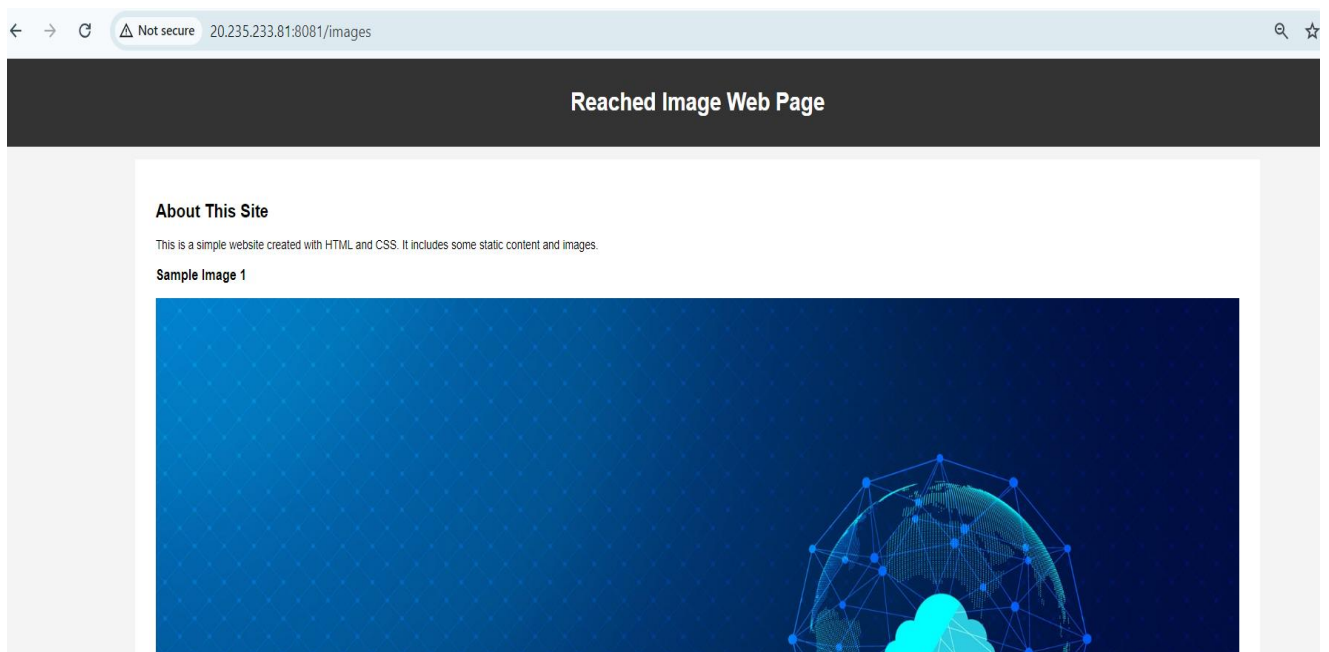
Application Gateway IP: 20.235.233.81

Default Route to IIS Web Server: <http://20.235.233.81/>

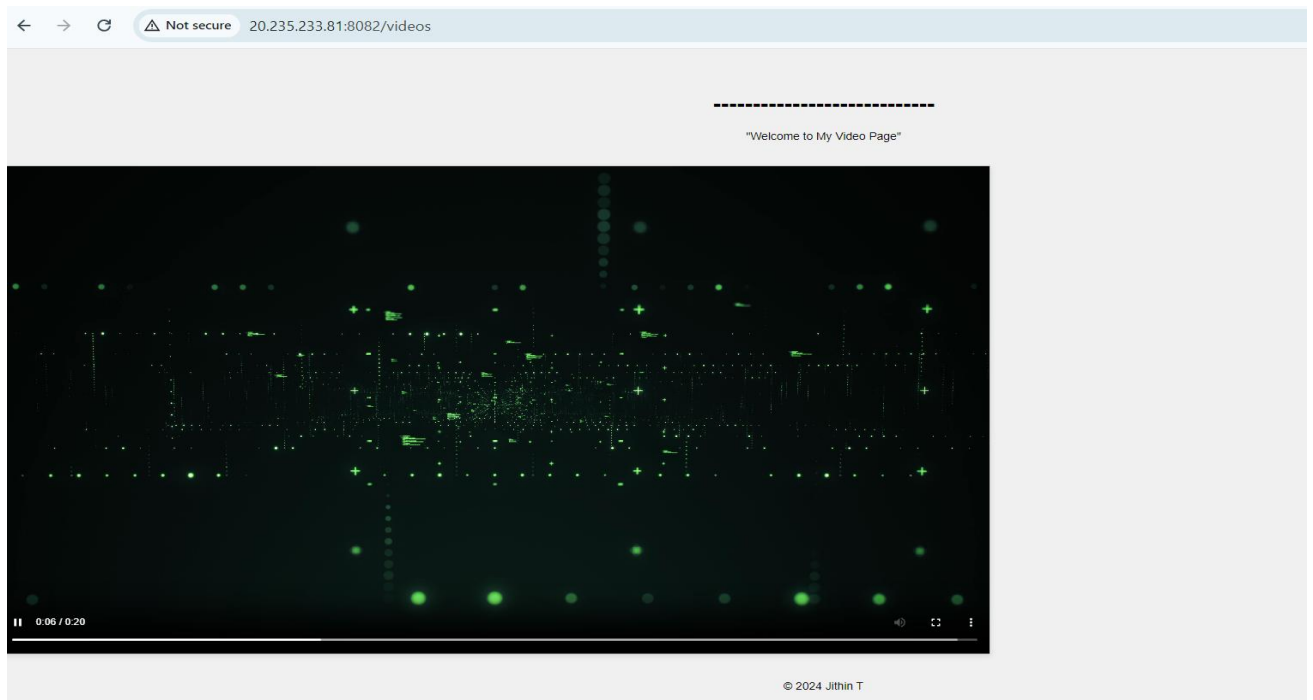


Path based Route:

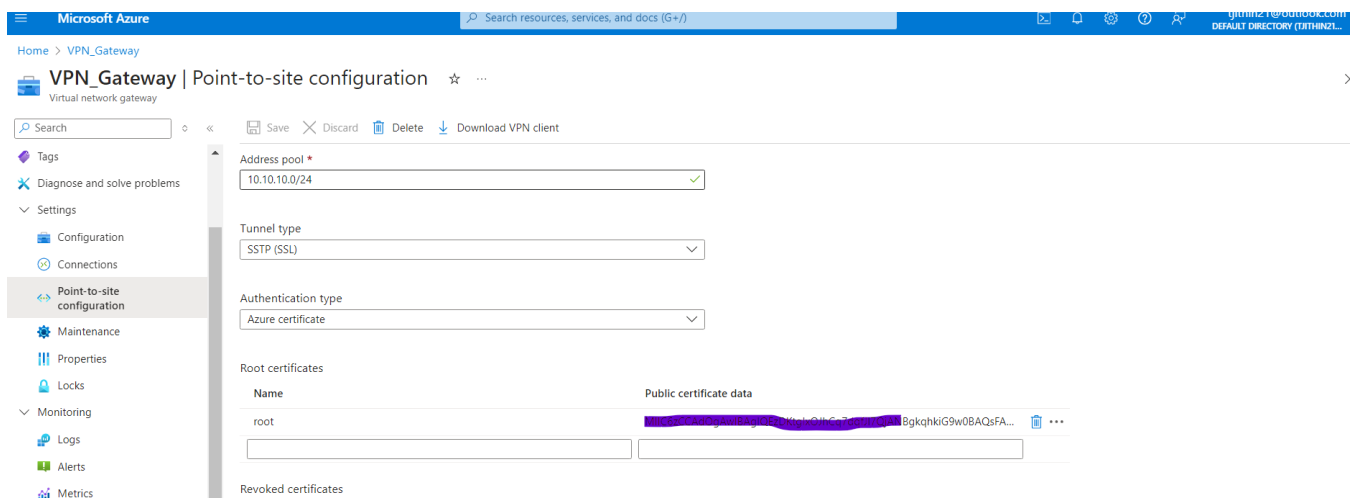
Path: /images → <http://20.235.233.81:8081/images>



Path: /videos → <http://20.235.233.81:8082/videos>



6.1.3 VPN Gateway: Point to Site Configuration:

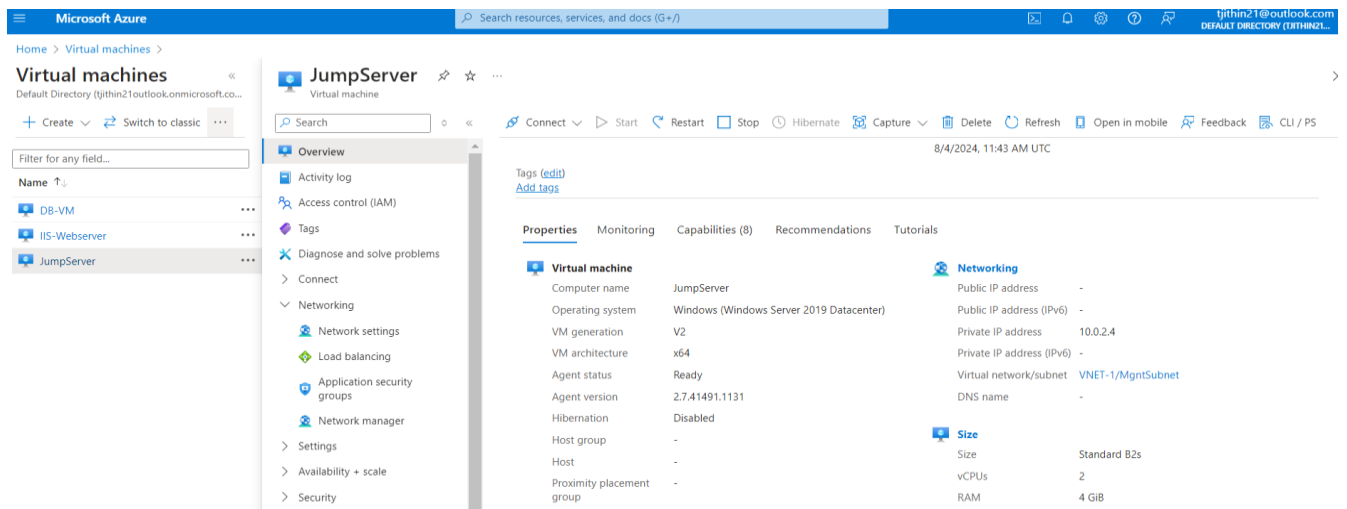


Note: For accessing Azure network, need to install Client Certificate and VPN Client in PC or LAP to get the secured connection. Client certificate and VPN client is uploaded in G Drive.

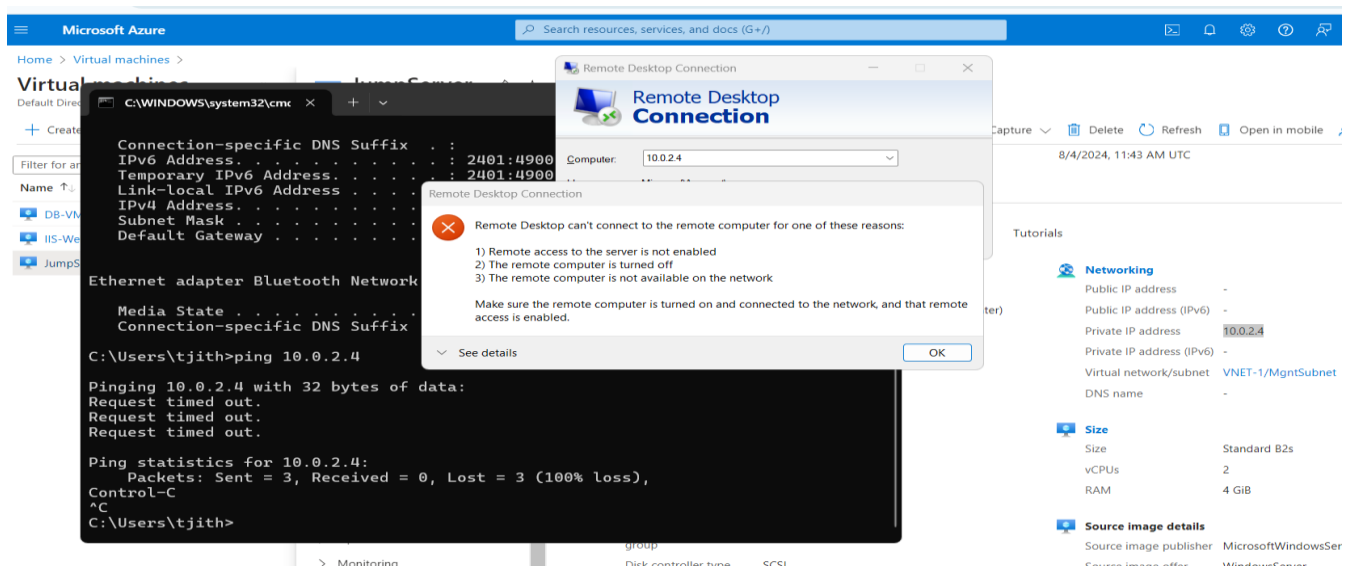
Note: For Installing Client Certificate follow the below mentioned link for ref.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-how-to-vpn-client-install-azure-cert>

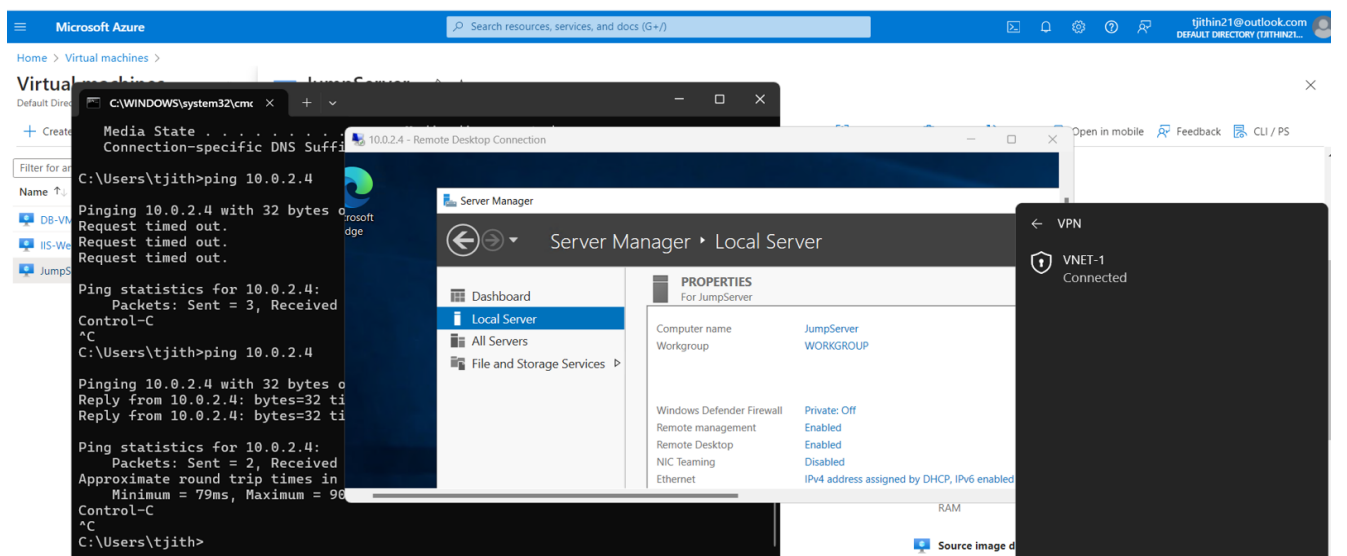
- 6.1.4 Jump Server Configuration:



Ping Test and RDP Fail without VPN Connection:

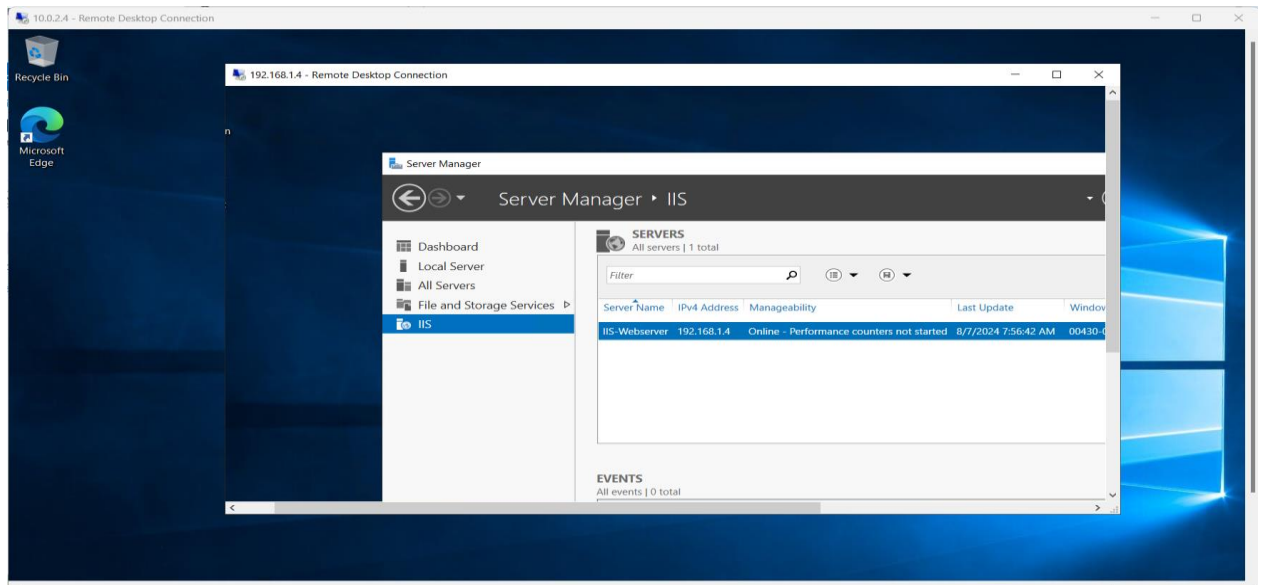


Jump Server can be accessible after connecting VPN: VNET-1

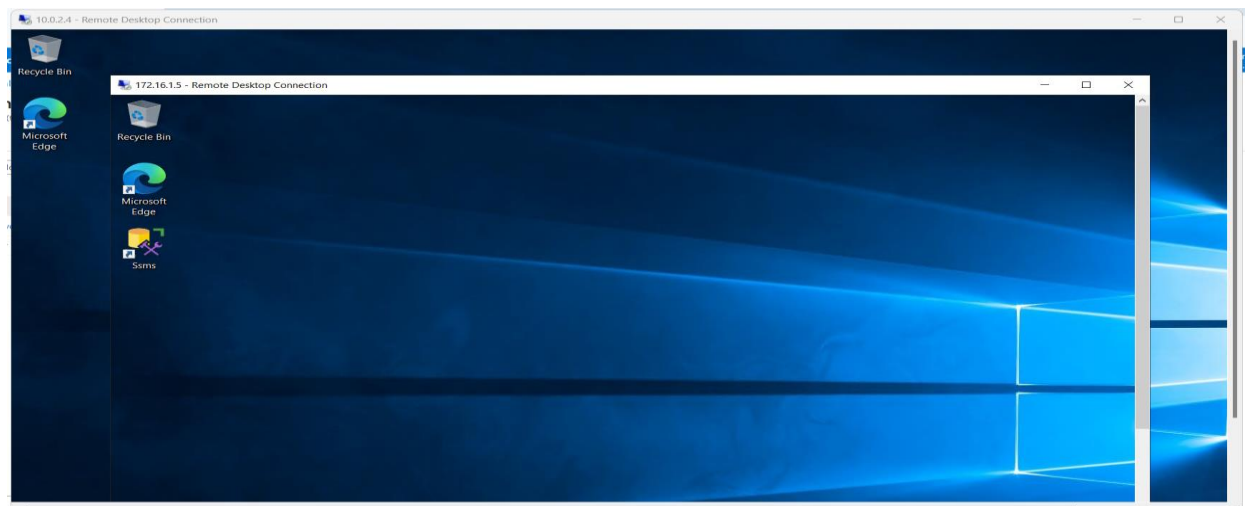


RDP Testing From Jump Server:

- RDP to IIS Web Server



- RDP to DB-VM



6.1.5 IIS Web Server Configuration:

The screenshot shows the Microsoft Azure portal interface. The left sidebar displays the "Virtual machines" section with a list of VMs: "DB-VM", "IIS-Webserver", and "JumpServer". The main area shows the configuration for the "IIS-Webserver" VM. The "Properties" tab is selected, displaying the following details:

Section	Property	Value
Virtual machine	Computer name	IIS-Webserver
	Operating system	Windows (Windows Server 2019 Datacenter)
	VM generation	V2
	VM architecture	x64
	Agent status	Ready
	Agent version	2.7.41491.1131
	Hibernation	Disabled
	Host group	-
	Host	-
	Proximity placement group	-
Networking	Public IP address	-
	Public IP address (IPv6)	-
	Private IP address	192.168.1.4
	Private IP address (IPv6)	-
Size	Size	Standard B2s
	vCPUs	2
	RAM	4 GiB
Source image details		

NSG: Allowed only RDP Access from Jump Server IP Remaining all IP will get blocked.

Search resources, services, and docs (G+)

githin21@outlook.co...
DEFAULT DIRECTORY (TJITHIN21...)

IIS-Webserver | Network settings

Virtual machine

Search

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Security

This is a new experience. [Please provide feedback](#)

Network security group IIS-Webserver-nsg (attached to networkInterface: iis-webserver224_z1)
Impacts 0 subnets, 1 network interfaces

+ Create port rule

Search rules

Source == all Destination == all Protocol == all Action == all

Priority	Name	Port	Protocol	Source	Destination
Inbound port rules (7)					
300	RDP	3389	TCP	10.0.2.4	Any
320	HTTP	80	TCP	Any	Any
340	HTTPS	443	TCP	Any	Any
350	DenyAnyRDPInbound	3389	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any
Outbound port rules (3)					

RDP Failed after connecting VPN also. Since it is secured with IP based access.

Microsoft Azure

Search resources, services, and docs (G+)

tjithin21@outlook.co...
DEFAULT DIRECTORY (TJITHIN21...)

Home > Virtual machines > IIS-Webserver

Virtual machines

Default Directory

+ Create

Filter for all

Name

DB-VM
IIS-Webserver
JumpServer

Remote Desktop Connection

Computer: 192.168.1.4

Remote Desktop Connection

Remote Desktop can't connect to the remote computer for one of these reasons:

- 1) Remote access to the server is not enabled
- 2) The remote computer is turned off
- 3) The remote computer is not available on the network

Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.

See details

OK

Control-C
^C
C:\Users\tjith>ping 10.0.2.4

Pinging 10.0.2.4 with 32 bytes of data:
Reply from 10.0.2.4: bytes=32 time=7ms TTL=127
Reply from 10.0.2.4: bytes=32 time=9ms TTL=127

Ping statistics for 10.0.2.4:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
Minimum = 79ms, Maximum = 90ms, Average = 84ms

Control-C
^C
C:\Users\tjith>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=66ms TTL=127
Reply from 192.168.1.4: bytes=32 time=66ms TTL=127

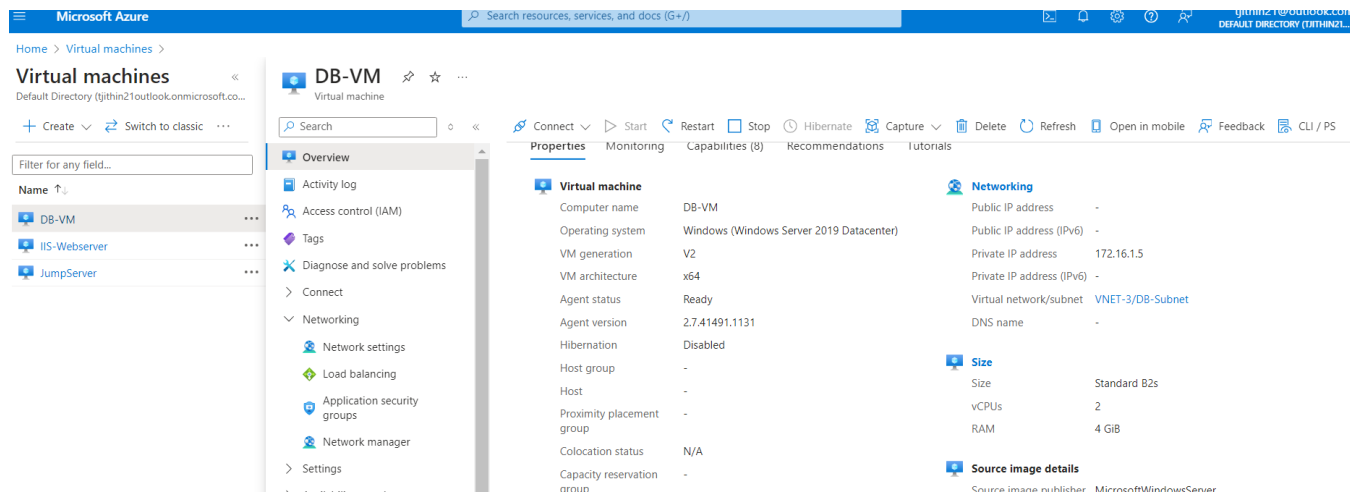
Ping statistics for 192.168.1.4:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
Minimum = 66ms, Maximum = 66ms, Average = 66ms

Control-C
^C
C:\Users\tjith>

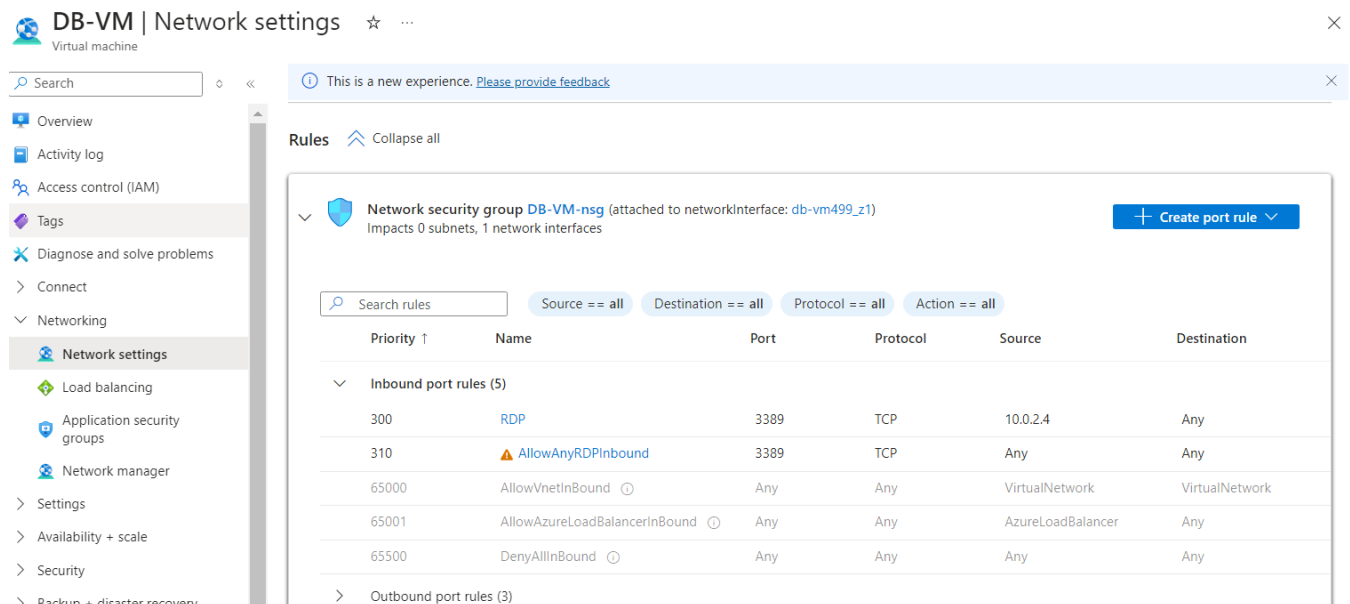
VPN

VNET-1
Connected

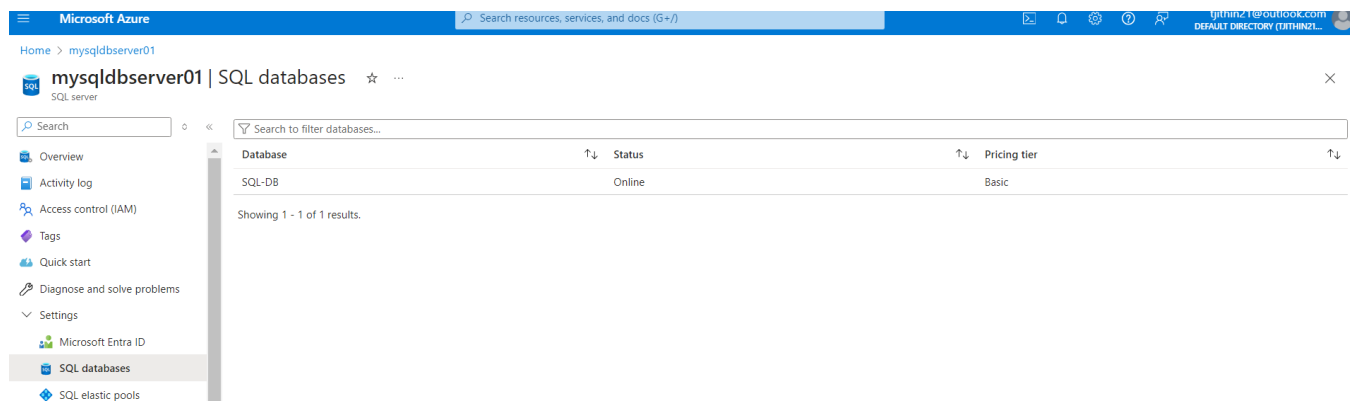
- 6.1.6 DB Server Configuration:

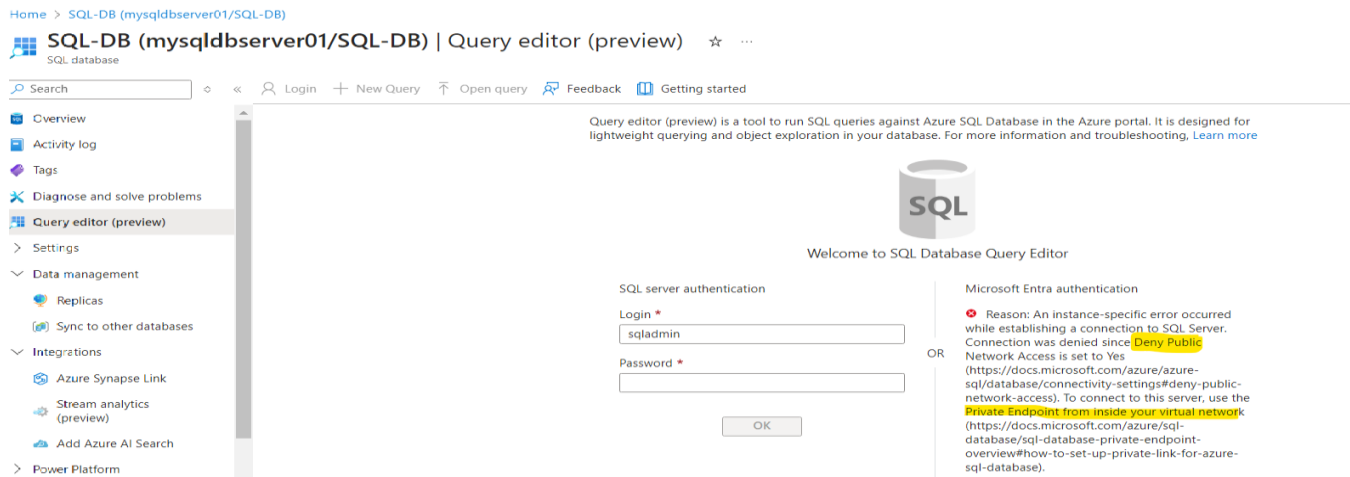


NSG: RDP Allowed from Jump Server IP only remaining all will be blocked.

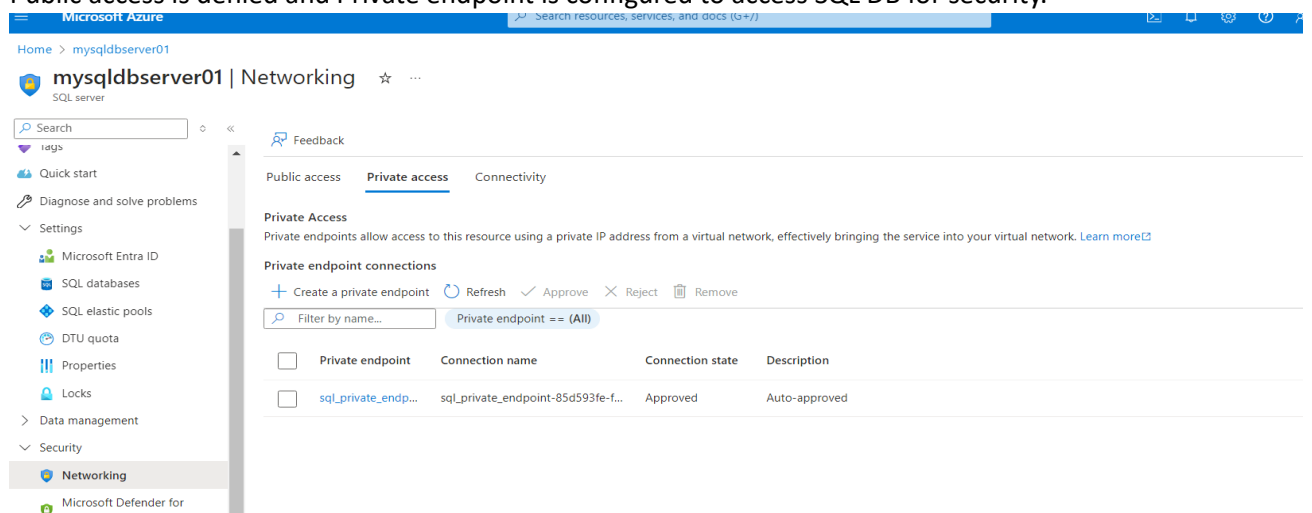


- 6.1.7 SQL DB Configuration:

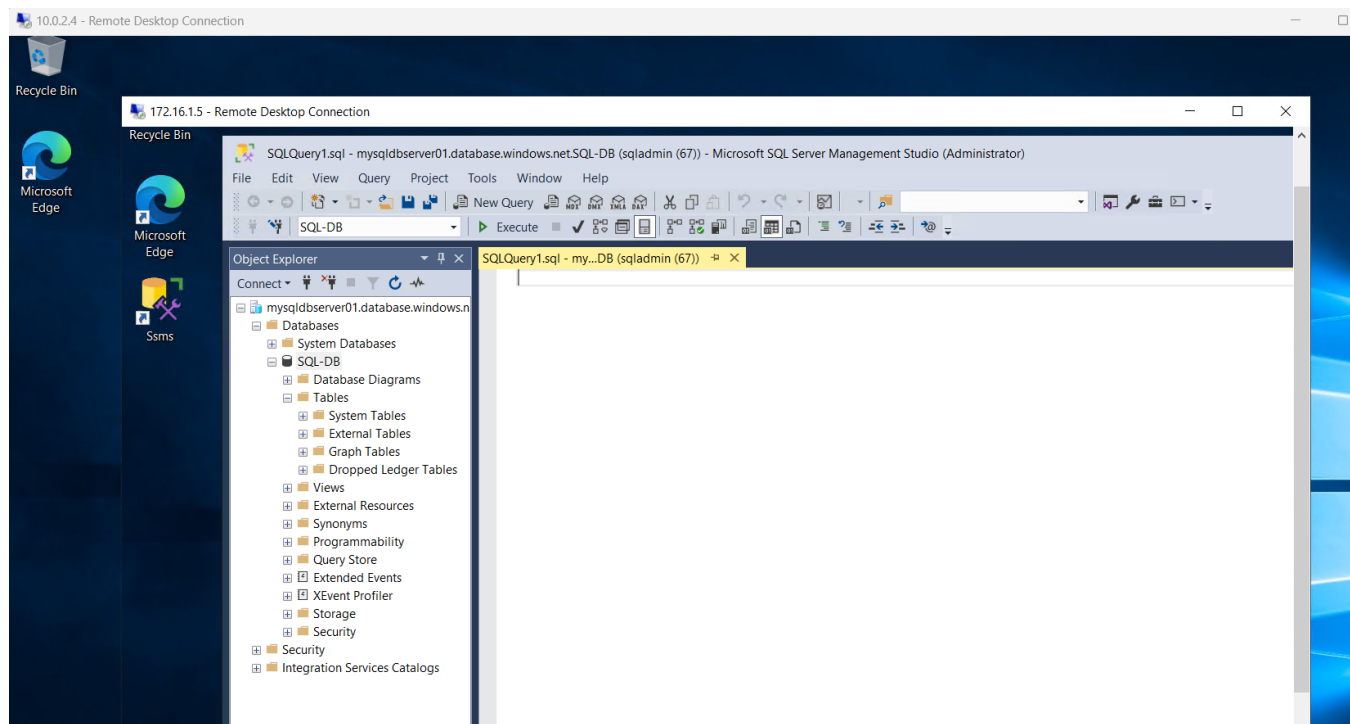




Public access is denied and Private endpoint is configured to access SQL DB for security.



DB Access Test via DB-VM:



Conclusion Summary:

1. Application Gateway Application deployed as frontend and Backend as IIS Webserver and Static Web site for image and Video path route
2. WAF Policy Applied in Application Gateway for Block attacks and unwanted traffic.
3. VPN Gateway (P2S) is configured for remote access.
4. VNET-1 is configured as HUB and VNET-2 and VNET-3 as SPOKE and All Internal SPOKE communication will flow via HUB Gateway.
5. Jump server is Deployed and configured. It act like proxy where all Spoke server can be accessible via jump server, no direct access to spoke server.

-----Thank You-----