## *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:*

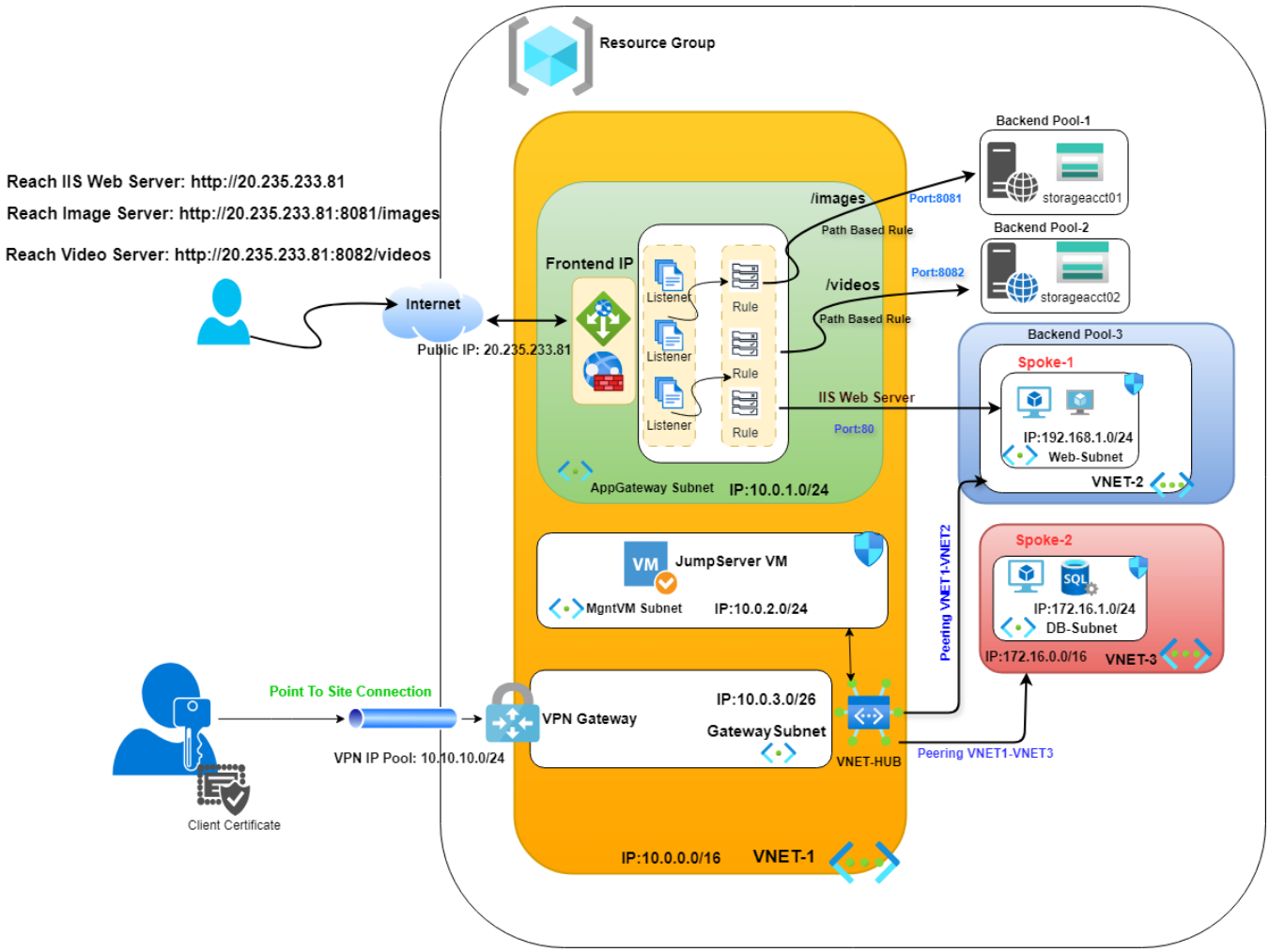
- **Secure Segmentation:** Create separate VNets for each application tier to ensure isolation and security.
- **Traffic Management:** Implement Azure Application Gateway for effective traffic handling, including advanced load balancing features.
- **Enhanced Security:** Configure NSGs and WAF to protect 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:

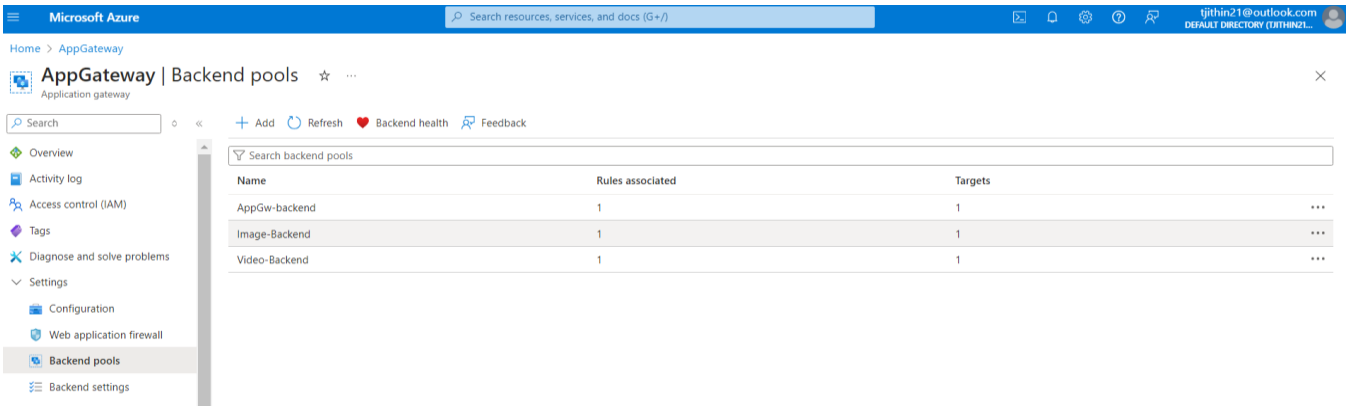
| Configuration Details | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| S.No | Resource Name | Type | Associanted Network | Network IP Segment | Subnet Name | Subnet IP Details | Public IP / Private IP | Port Opened / Description | Remarks |
| 1 | VNET-1 (HUB) | Virtual Network | N/A | 10.0.0.0/16 | default | 10.0.0.0/24 | | | |
| | | Virtual Network | | | AppGw-Subnet | 10.0.1.0/24 | | | |
| | | Virtual Network | | | MgntSubnet | 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 | | MgntSubnet | 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 (mysqldbserver01.database.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:

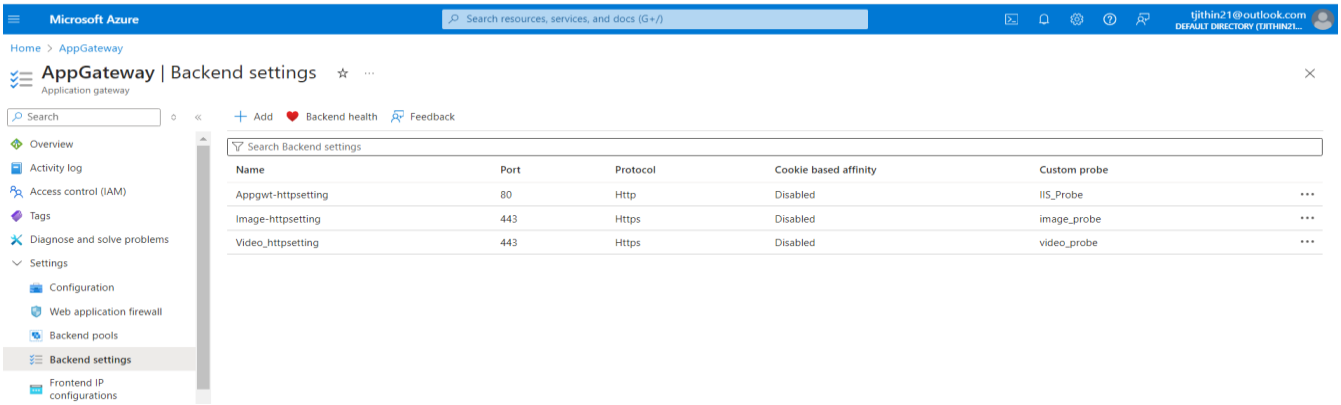
- ### 6.1.2 Application Gateway details and Backend Mapped Details

Configuration: WAF V2 / Auto scale Mode

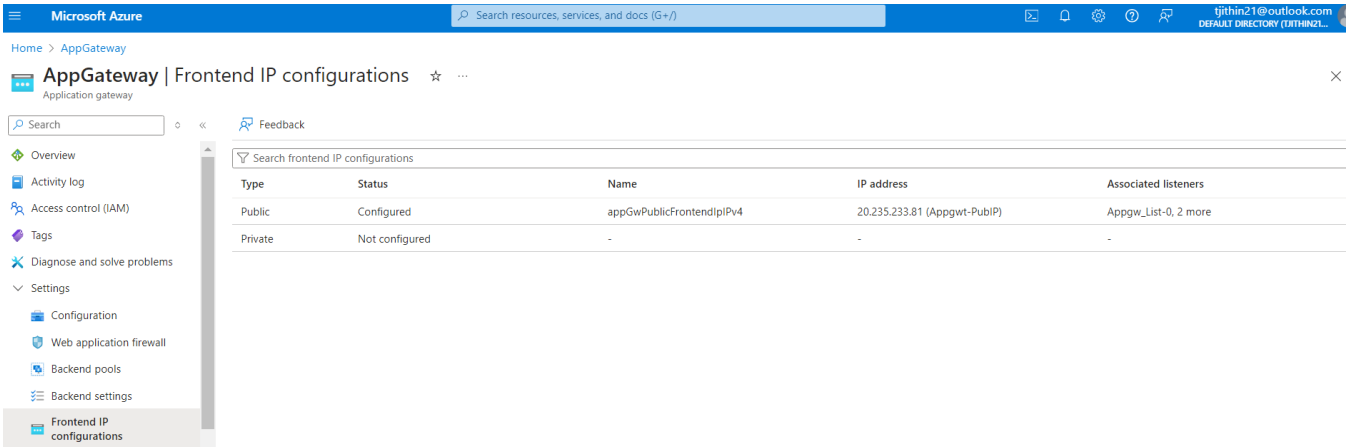
Backend Pool:



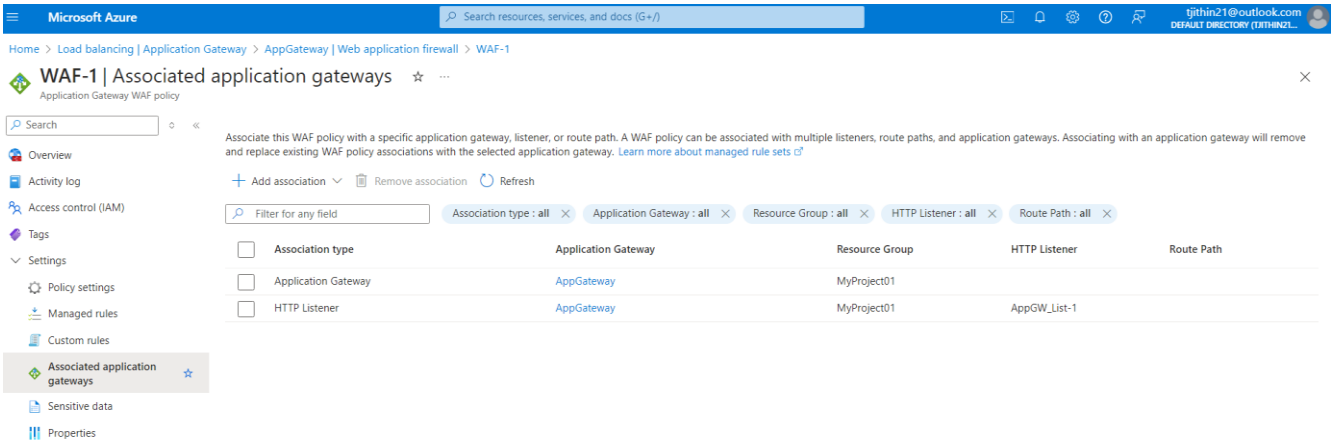
## Backend Setting or Http Setting:



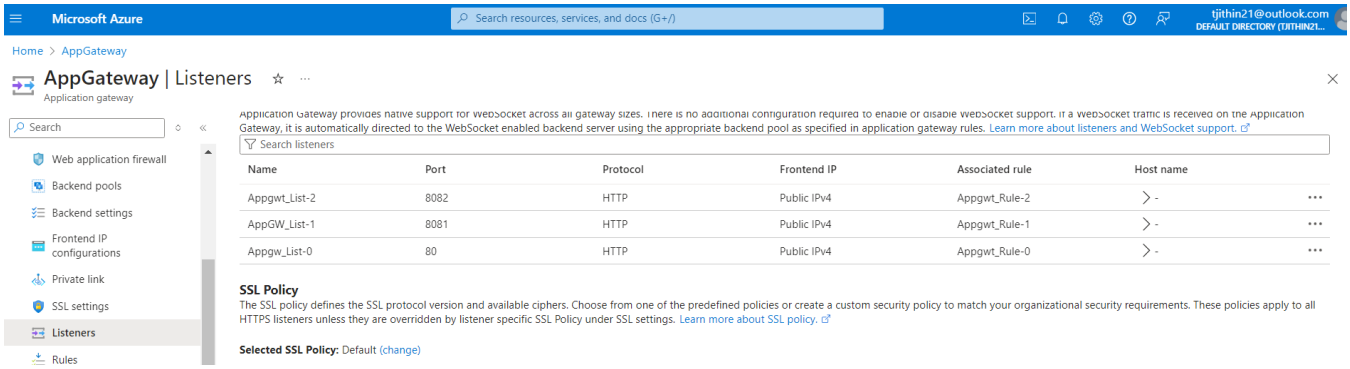

## Frontend IP:



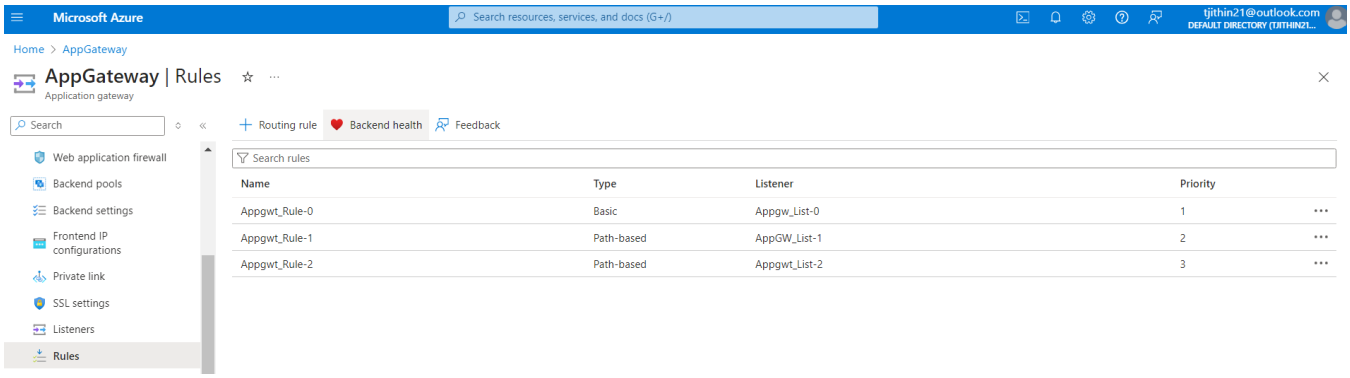

## WAF Policy associated with Application Gateway:



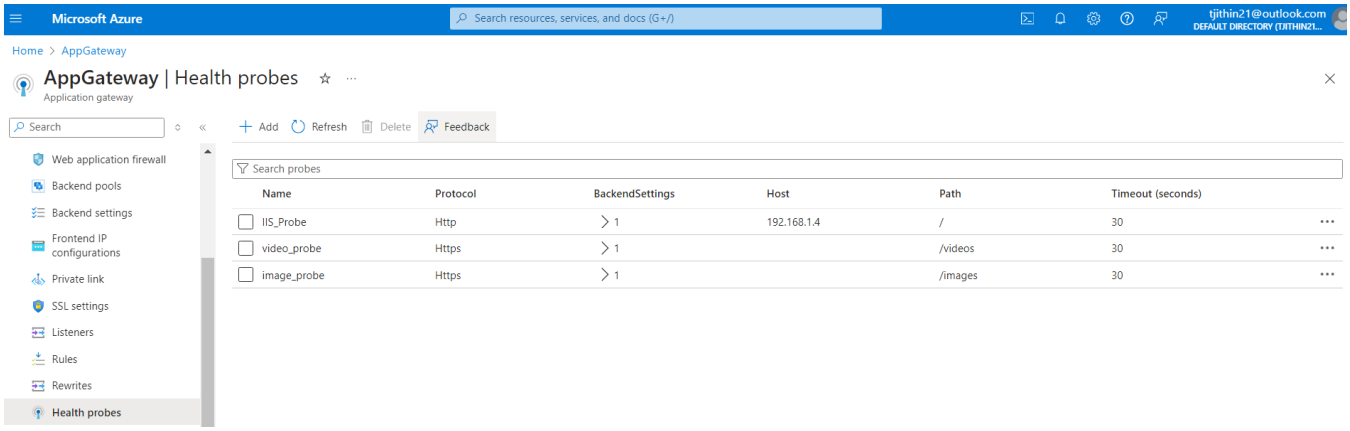
## Listener:




## Rules:



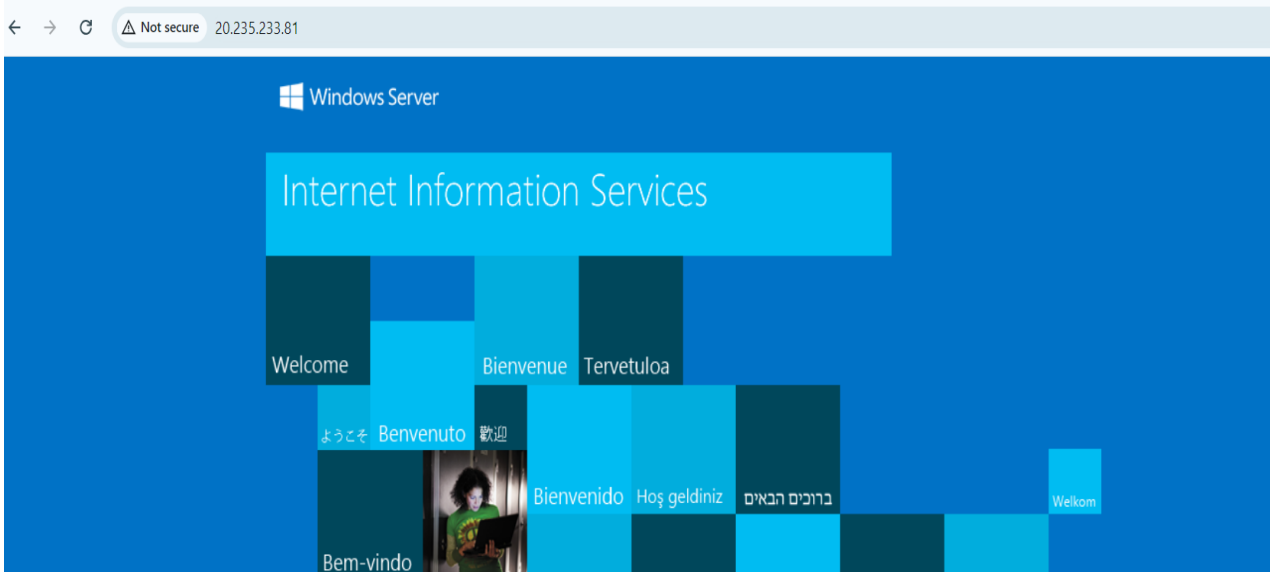

## Health Probes:



## *Results:*

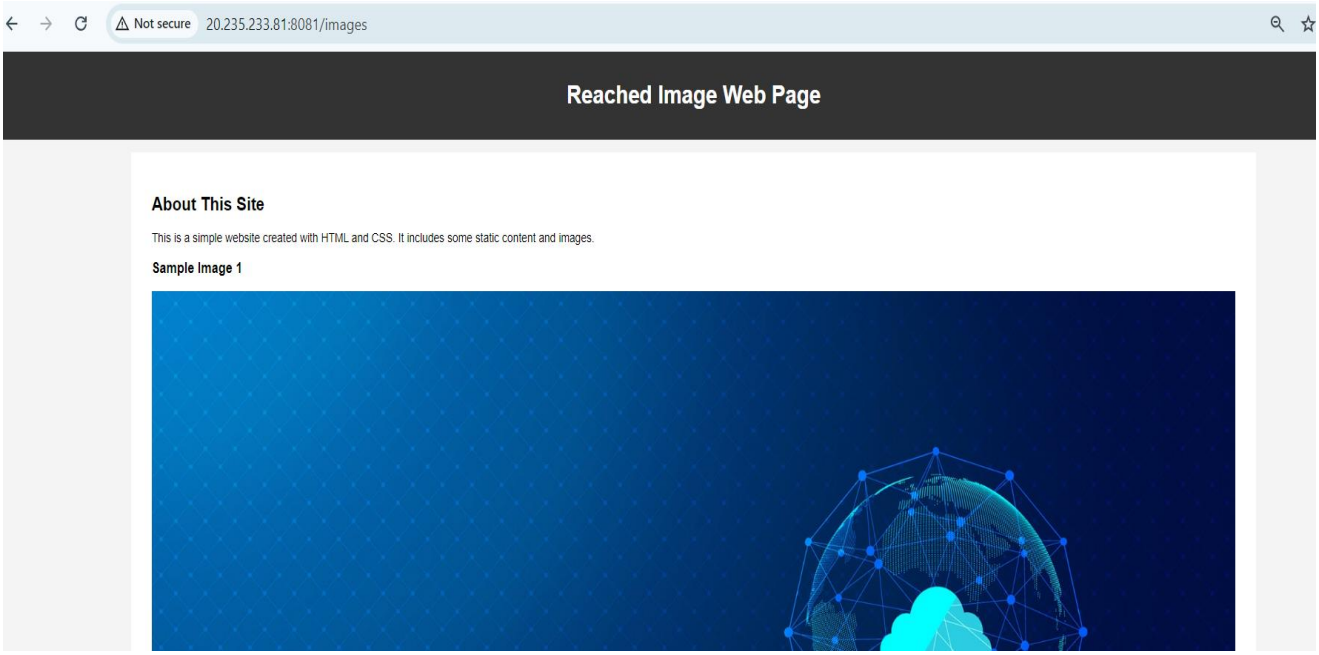
Application Gateway IP: 20.235.233.81

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

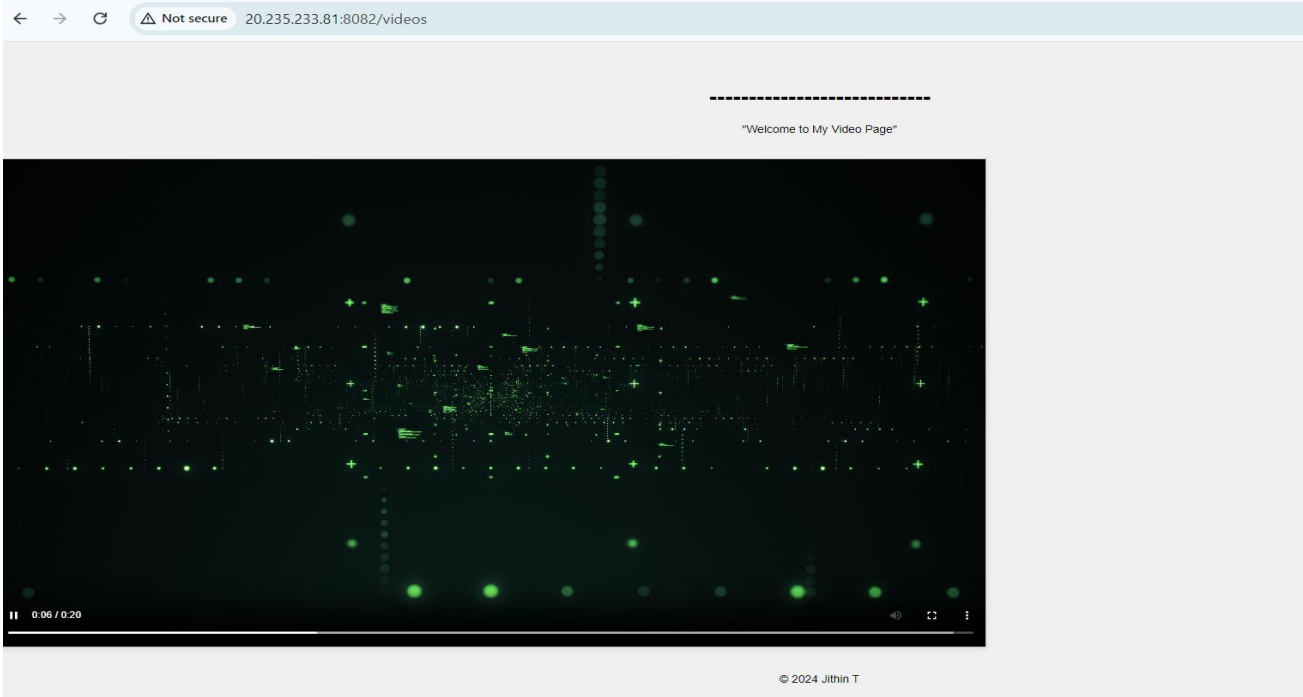



**Path based Route:**

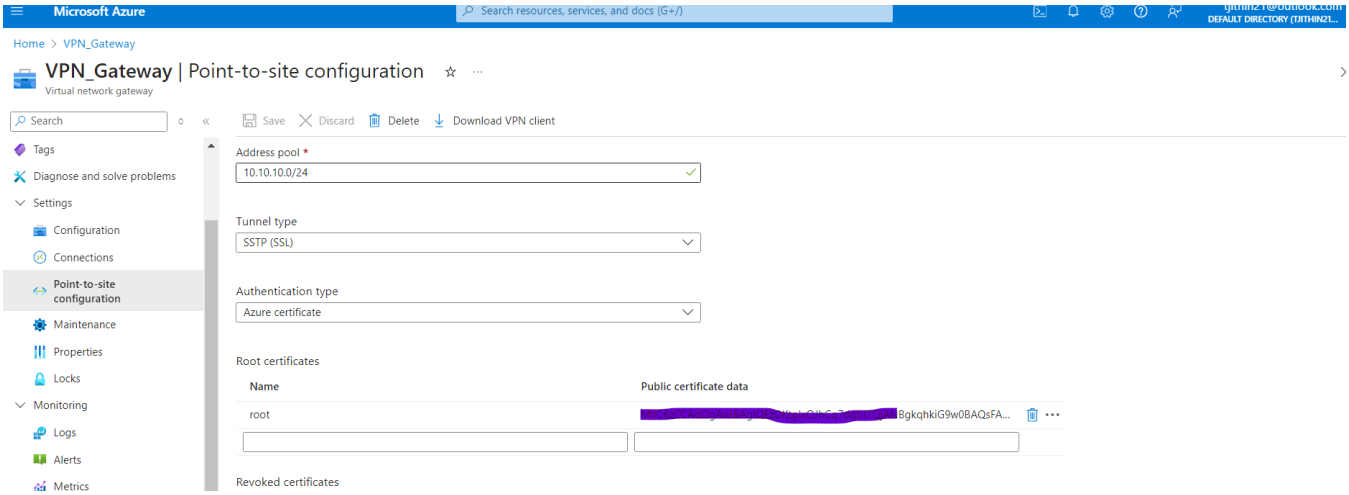
Path: /images → http://20.235.233.81:8081/images



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




### *6.1.3 VPN Gateway: Point to Site Configuration:*

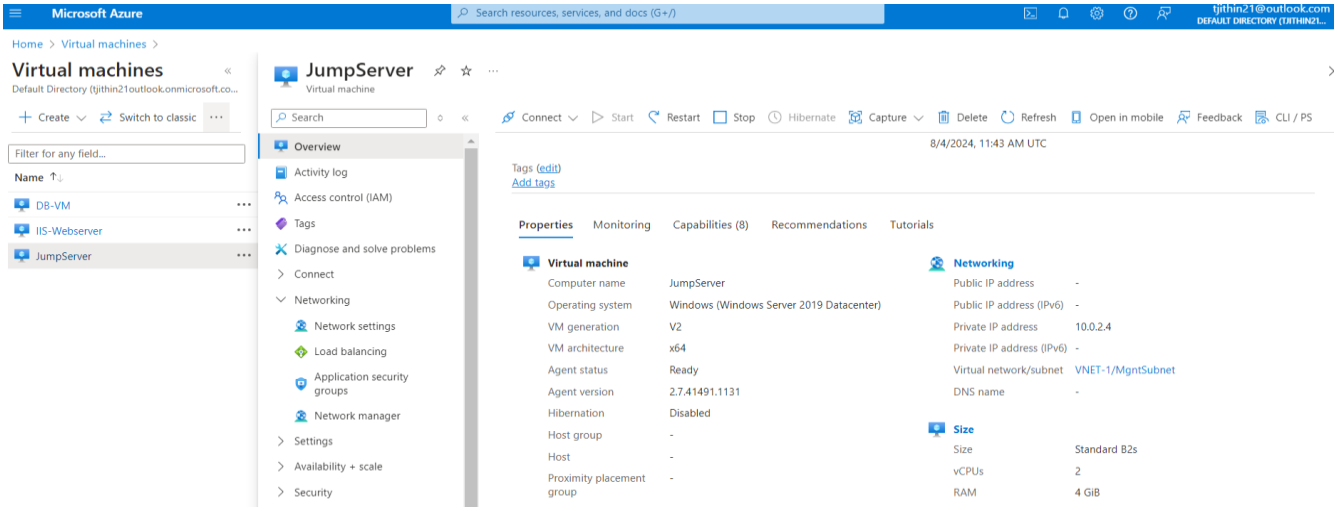



Note: For accessing Azure network, need to install Client Certificate and VPN Client in PC or LAP to get the secured connection. Client certificate and VPN client is uploaded in G Drive.

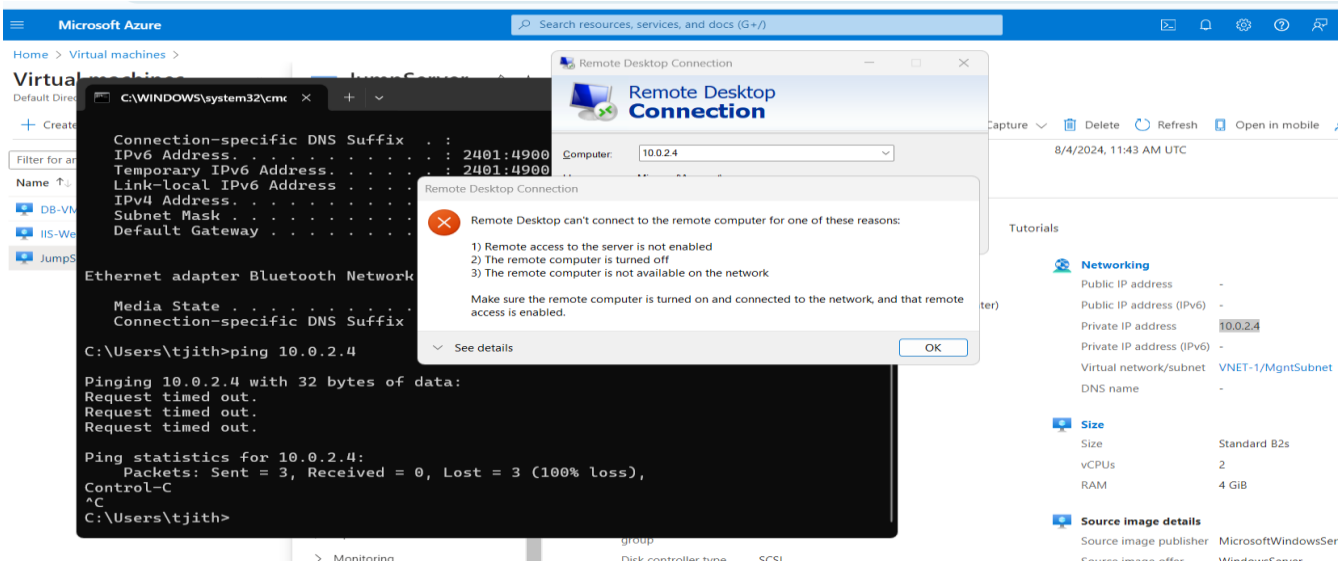
Note: For Installing Client Certificate follow the below mentioned link for ref.

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

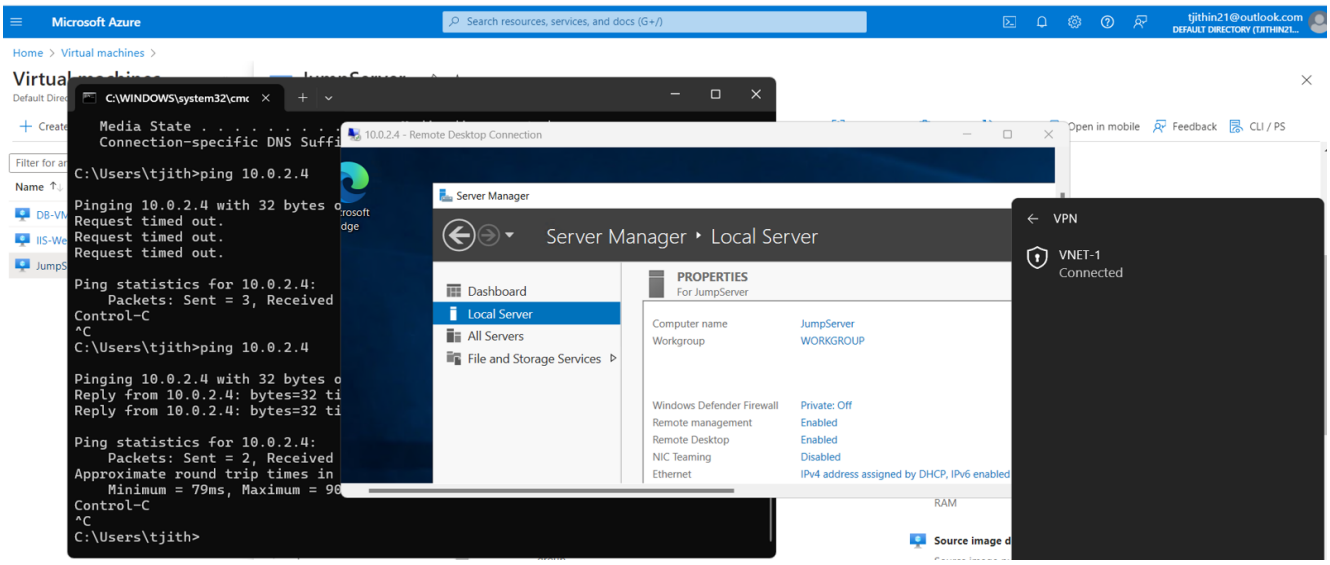
- ### *6.1.4 Jump Server Configuration:*




Ping Test and RDP Fail without VPN Connection:

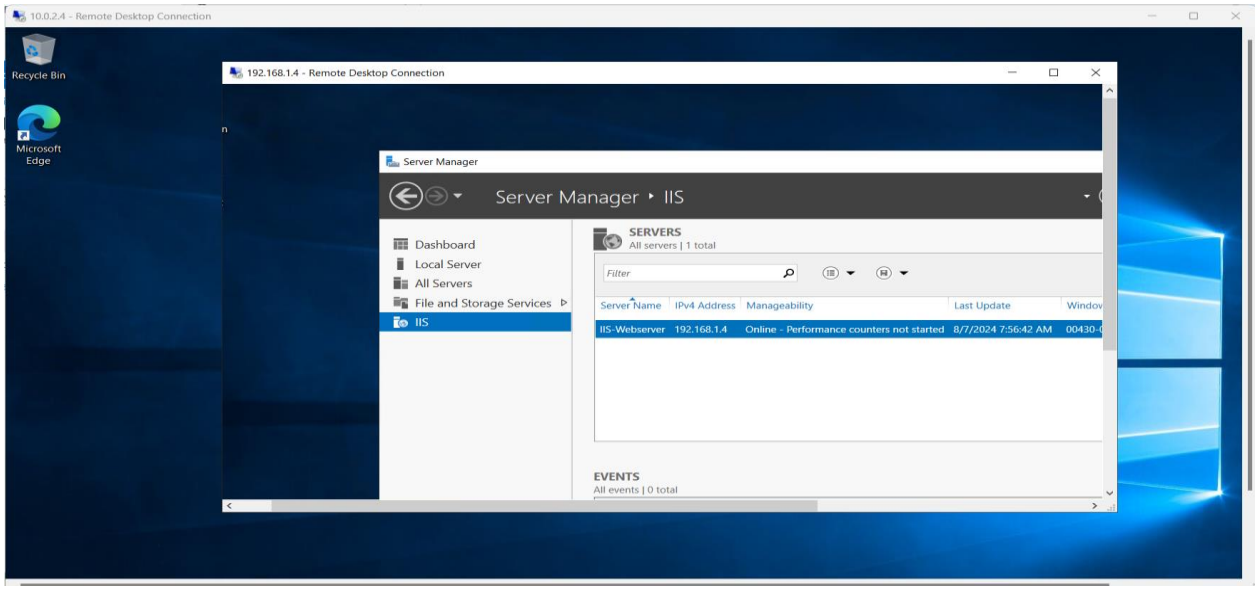



Jump Server can be accessible after connecting VPN: VNET-1

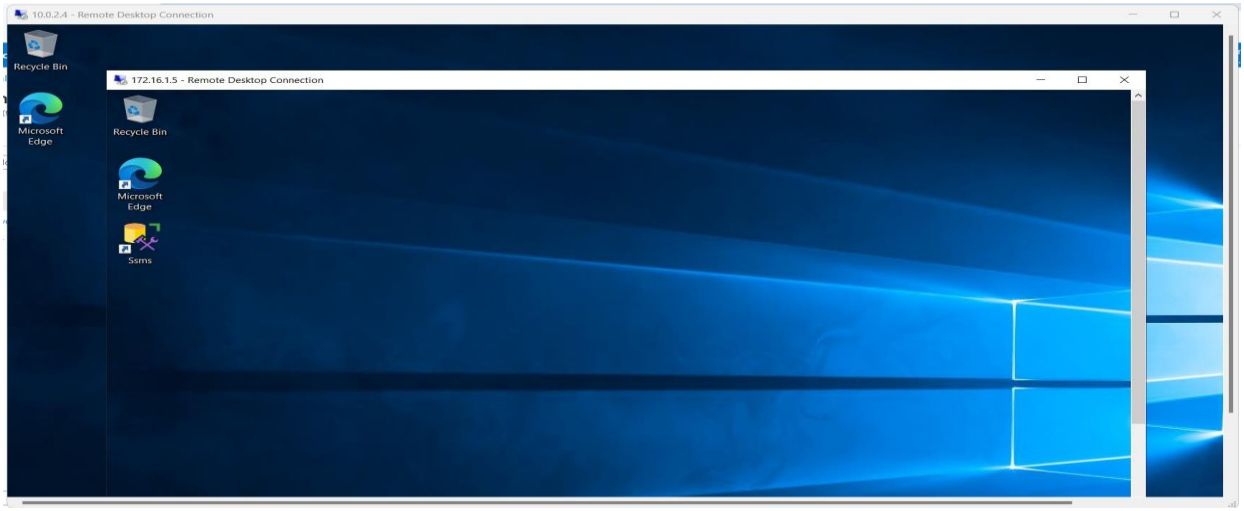


**RDP Testing From Jump Server:**

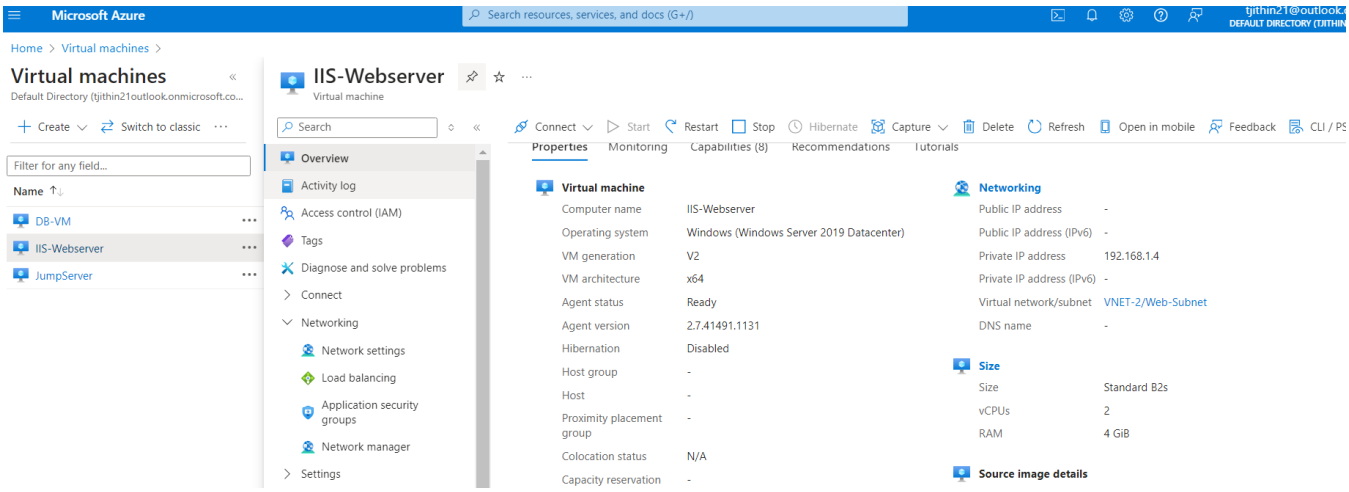
- RDP to IIS Web Server



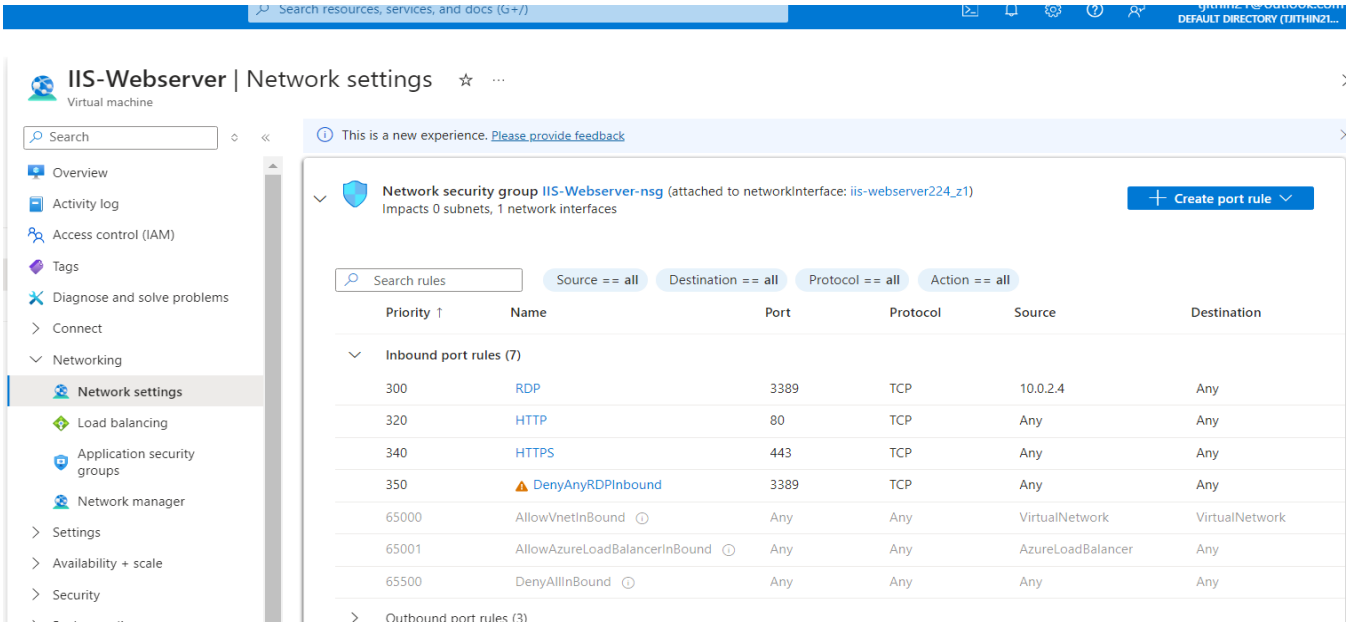

- RDP to DB-VM



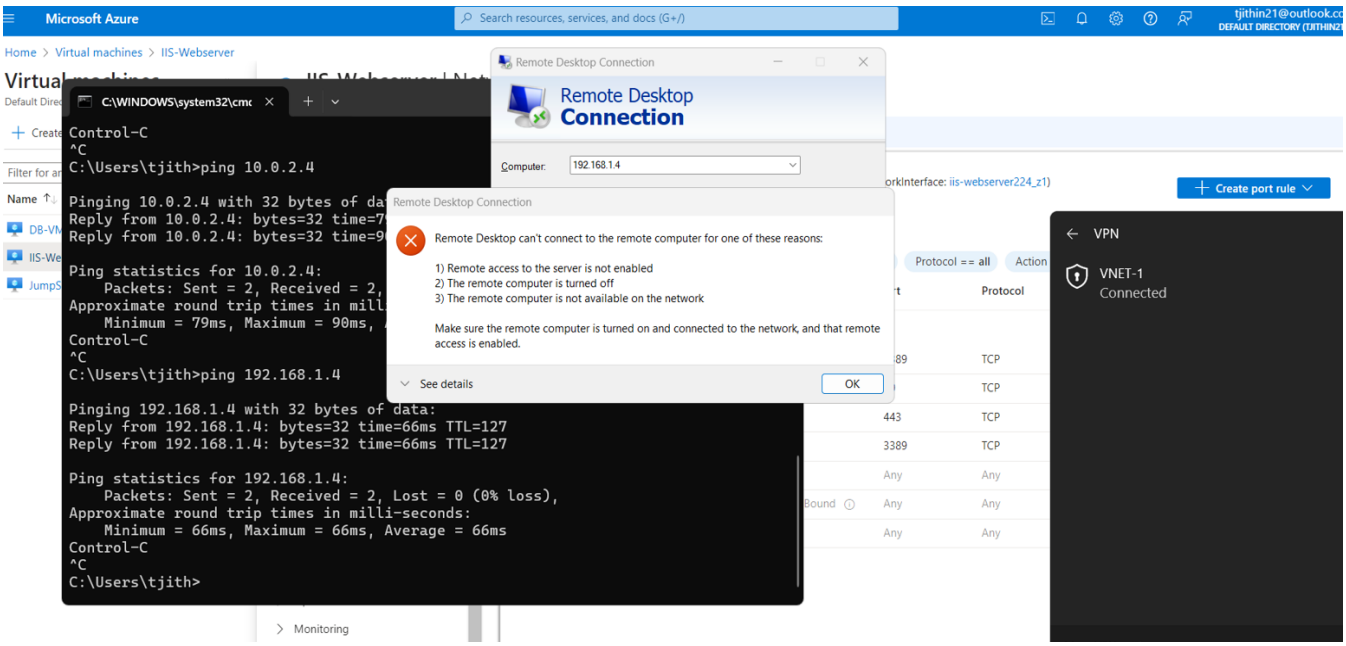

- ***6.1.5 IIS Web Server Configuration:***



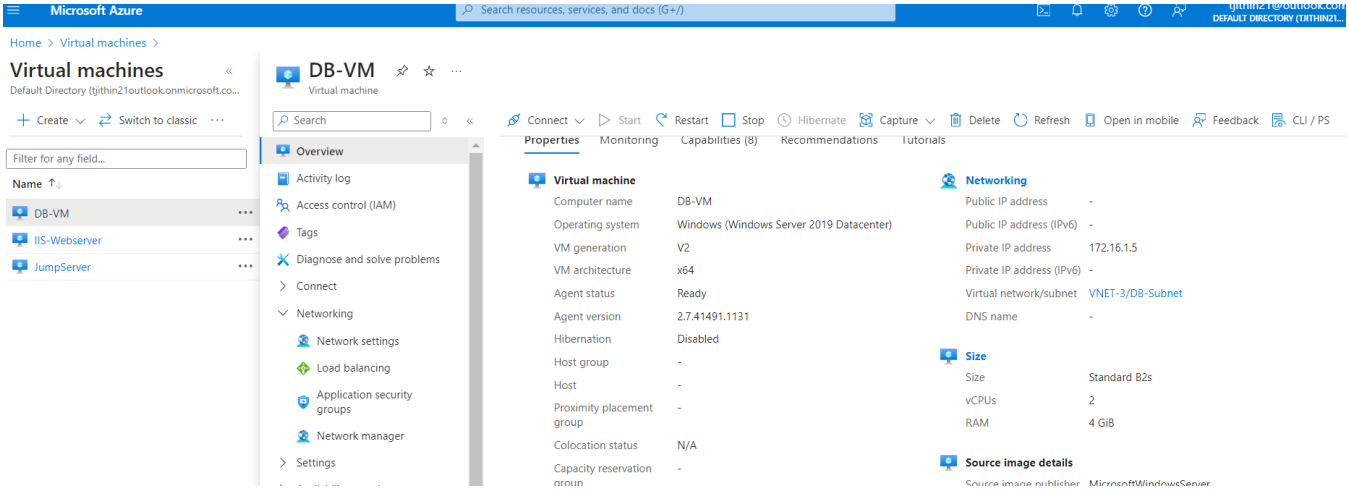
NSG: Allowed only RDP Access from Jump Server IP Remaining all IP will get blocked.



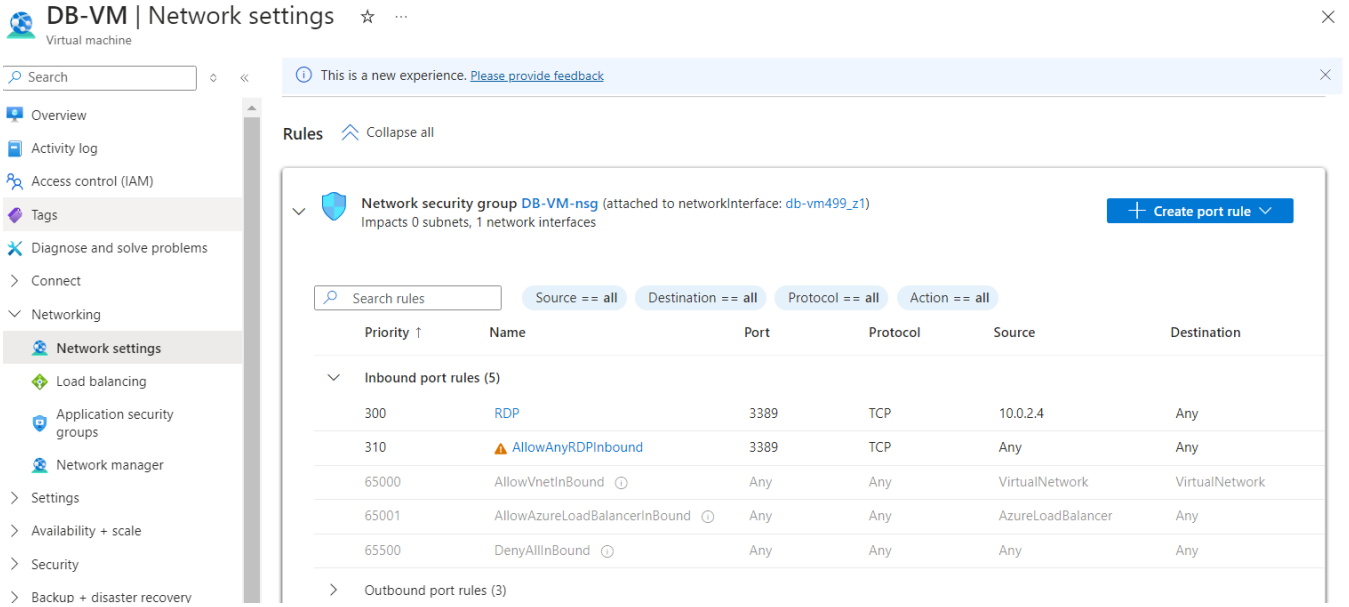

RDP Failed after connecting VPN also. Since it is secured with IP based access.



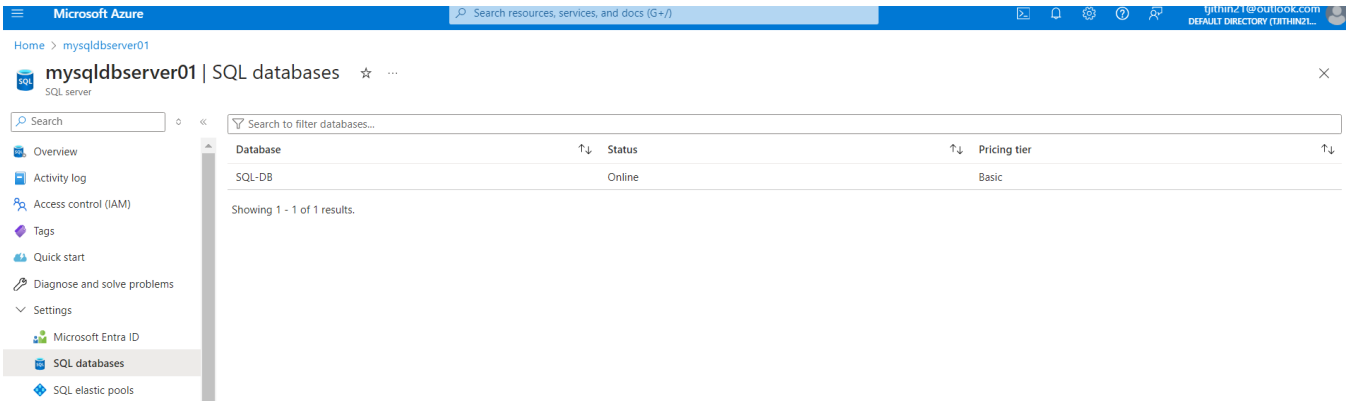
- ### *6.1.6 DB Server Configuration:*

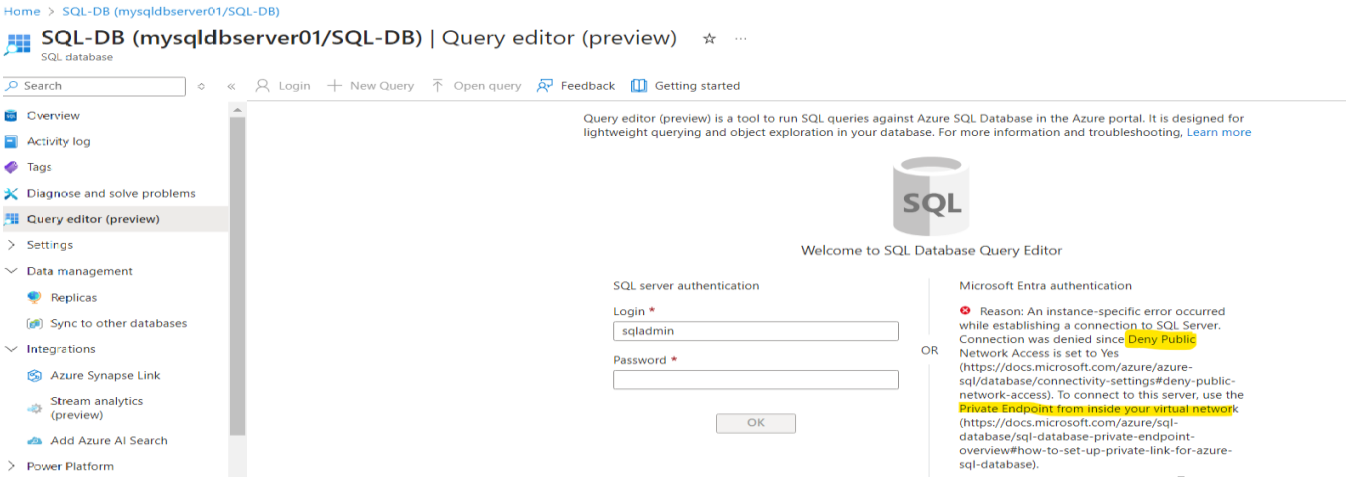



NSG: RDP Allowed from Jump Server IP only remaining all will be blocked.

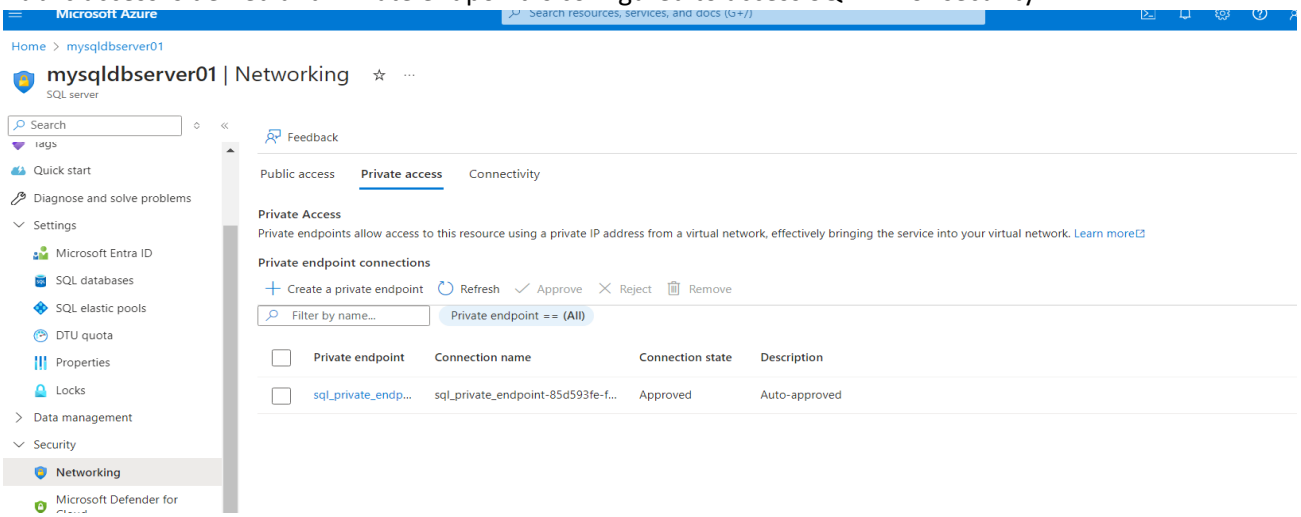



- ### *6.1.7 SQL DB Configuration:*

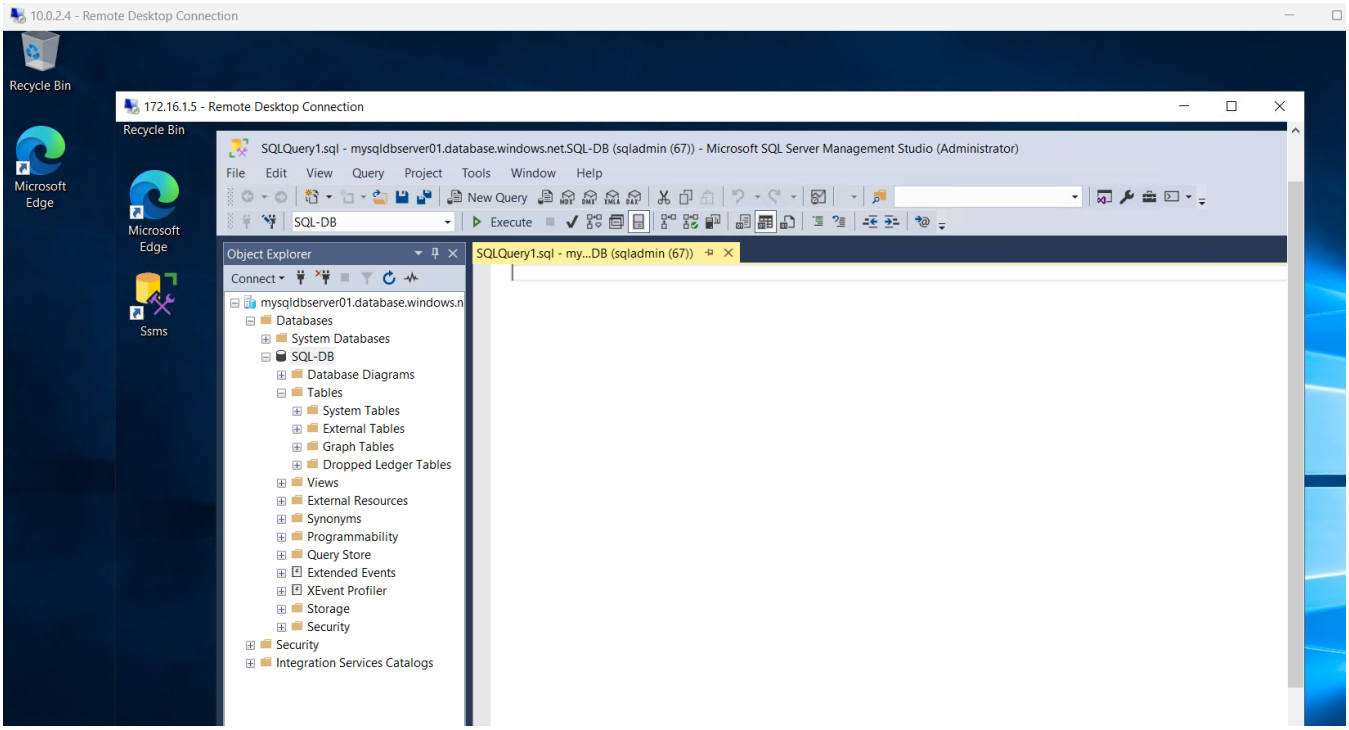





Public access is denied and Private endpoint is configured to access SQL DB for security.




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----------