Project Summary: Azure Micro-Segmentation Architecture Design with security-focused

1. Project-2 Title:

Azure Micro-Segmentation Architecture Design

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: ***20-08-2024***

2. Project Description:

Design and implement a micro-segmentation architecture within an Azure Virtual Network (VNet) to enhance security through network segmentation, strict access controls using Network Security Groups (NSGs), centralized traffic management with Azure Firewall, and optional use of Application Security Groups (ASGs).

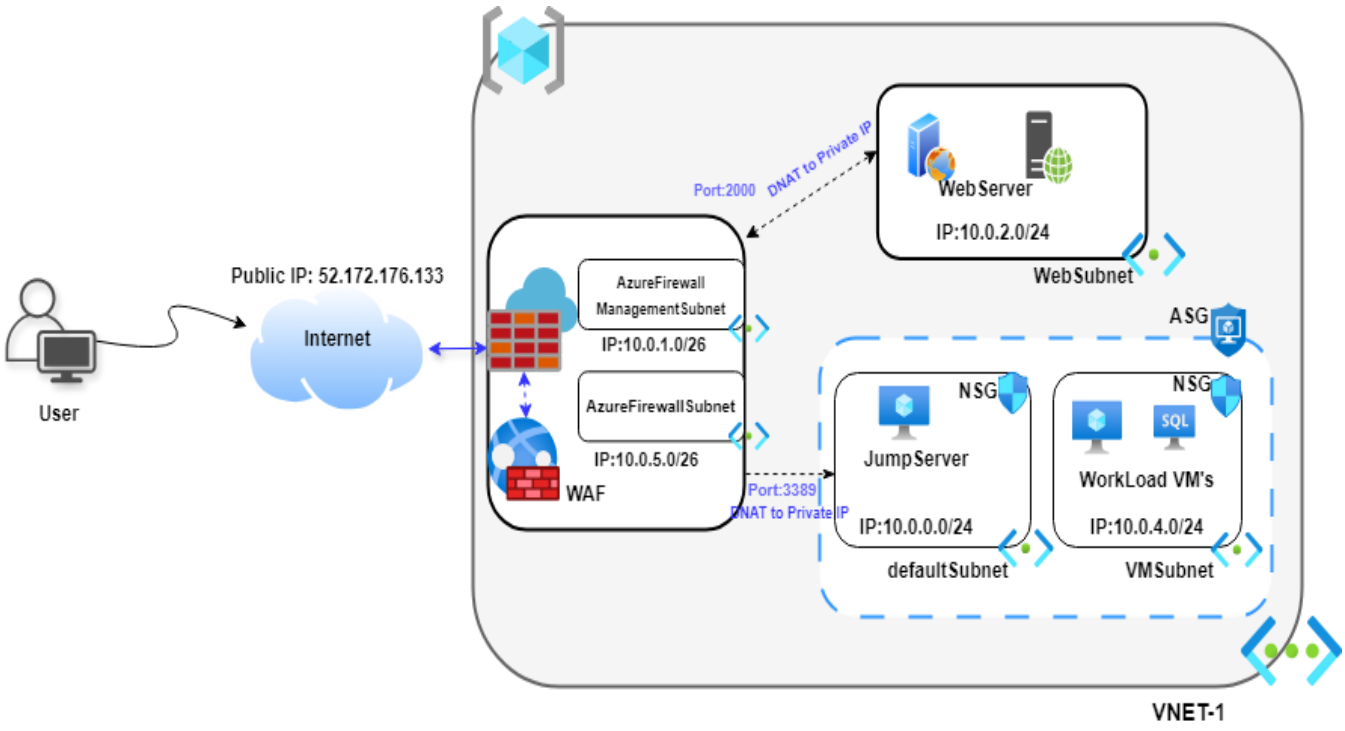
3. Goals and Objectives:

- **Secure Segmentation:** Create Sub network to segregate as per usage and enable required NSG
- **Traffic Management:** Implement Azure Firewall to effective traffic handling by enabling inbound and outbound port.
- **Enhanced Security:** Configure NSGs, ASG and WAF to protect against threats and ensure safe traffic flows.

4. Architecture Components:

- **Virtual Networks (VNets):**
  - **VNET-1:** Single virtual network and Divided into smaller sub VNet's for Firewall, Web Application and VM's
- **Network Security Groups (NSGs):**
  - **Jump Server NSG:** Allows traffic from Firewall
  - **Web Server NSG:** Permits traffic from Firewall
  - **Workload VM's NSG:** Restricts access only to the Jump server for Mgmt. (Internal Access Only)
- **Azure Firewall:**
  - **Firewall Rules & Policy:** Define allow and deny policy to handle traffic to internal subnets in secure manner.
  - **Web Application Firewall (WAF):** Protects against common web threats.
- **Application Security Group (ASGs):**
  - ASGs were utilized in NSG rules to streamline security management and control communication between application groups.

5. Architecture Design and Resource Details:



5.1 Azure Firewall:

Azure Firewall is a cloud-based network security service provided by Microsoft Azure. It acts as a protective barrier that monitors and controls the traffic flowing into and out of your Azure Virtual Network (VNet).

Firewall Policies Configured:

- ✓ Allowed or Deny outbound traffic to the internet for updates and external API access.
- ✓ Restricted inbound traffic based on source IP, destination IP, ports, and protocols.

Security Features Integrated:

- ✓ **Web Application Firewall (WAF):** Enabled to protect against common web threats

In This Project, I have configured DNAT Rules for both Jum Server and Web server to access via particular port. Backend IP and port is not exposed to frontend. And WAF is configured as Gobal level and Resist/Block traffic hit from any specific regions as per config.

5.2 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 Firewall opened Port. To reach any other server we need to access via jump server only.

5.3 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 different subnet in VNET-1 and NSG is Configured to allow and Deny Ports to secure the network. And also blocked Internet via ASG.

5.4 Workload Server (Backend Server):

A backend server is like the behind-the-scenes worker of a website or app. It does all the important tasks that users don't see directly but that keep everything running smoothly.

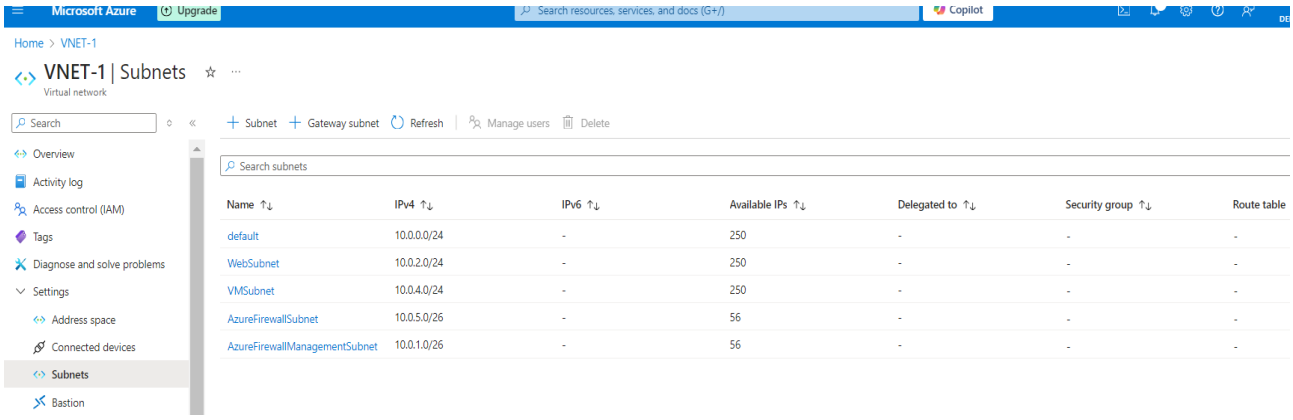
In This Project, I created Windows Server in different subnet and which can be accessible via jump server and Blocked Internet service via ASG.

6. Implementation and Testing of Design:

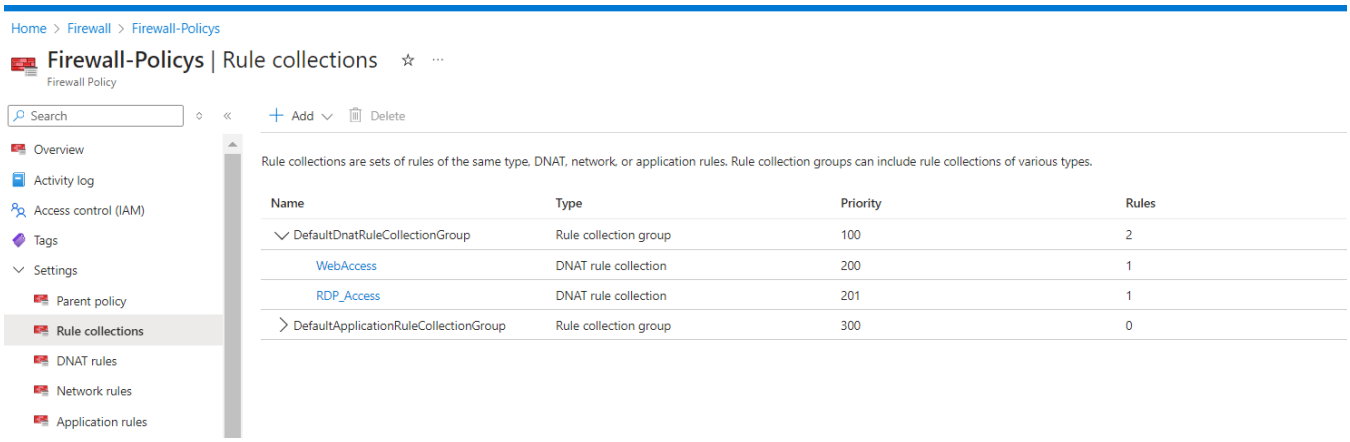
Configuration Details									
S.No	**Resource Name**	**Type**	**Associanted Network**	**Network IP Segment**	**Subnet Name**	**Subnet IP Details**	**Public IP / Private IP**	**Port Opened / Description**	**Remarks**
1	VNET-1	Virtual Network	N/A	10.0.0.0/16	default	10.0.0.0/24			
		Virtual Network			WebSubnet	10.0.2.0/24			
		Virtual Network			VMSubnet	10.0.4.0/24			
		Virtual Network			AzureFirewallSubnet	10.0.5.0/26			
		Virtual Network			AzureFirewallManagementSubnet	10.0.1.0/26			
2	Azure Firewall	Firewall	VNET-1		AzureFirewallSubnet	10.0.5.4	52.172.176.133 (Public)		Rules has been Created to define the Traffic route.
	WAF Policy	Azure Front Door Classic							Geo Location Base Block Traffic
6	JumpServer	VM	VNET-1		default	10.0.0.0/24	10.0.0.4 (Private)	RDP-3389 Allowed via Firewall	Used for Managing all VM
7	IIS-Webserver	VM	VNET-1		WebSubnet	10.0.2.0/24	10.0.2.4 (Private)	RDP-3389 Allowed via JumpServer only, HTTPS:443 allowed via firewall	IIS Web Site Loaded
8	Workload VM-1	VM	VNET-1		VMSubnet	10.0.4.0/24	10.0.4.4 (Private)	RDP-3389 Allowed via JumpServer only	Used for any Backend Server Work load.

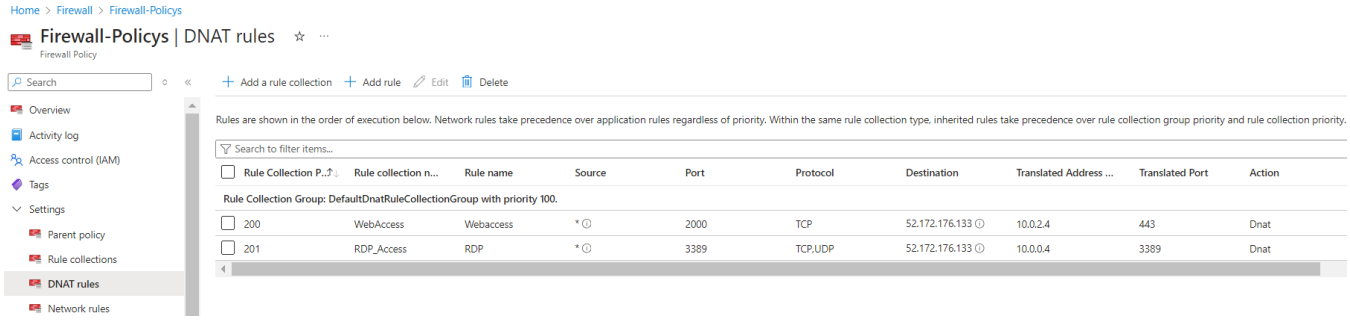
6.1 Snapshots & Testing:

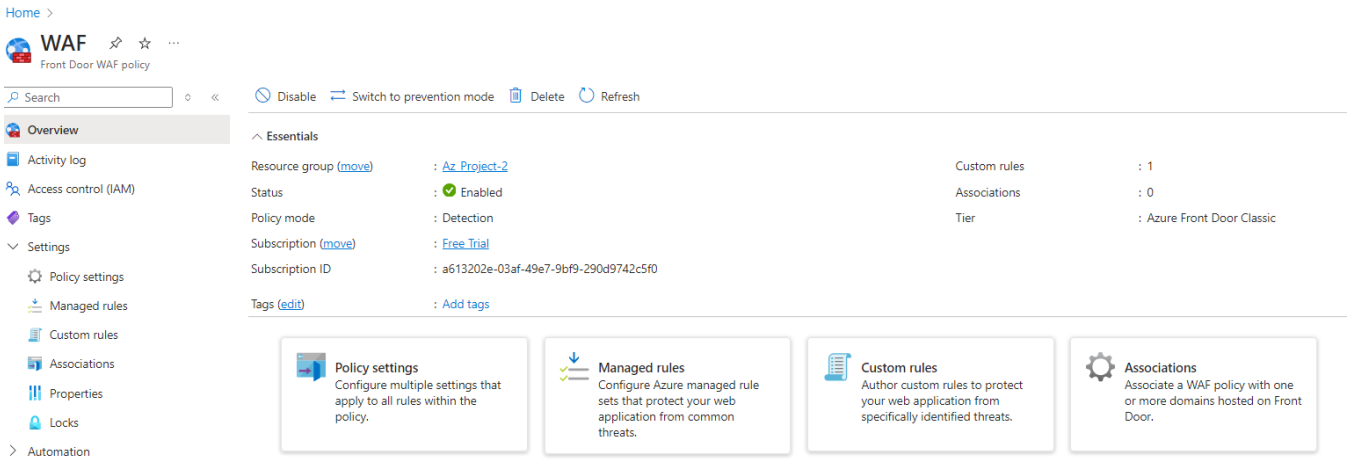
- ***6.1.1 Virtual Network and Subnetwork Details:***

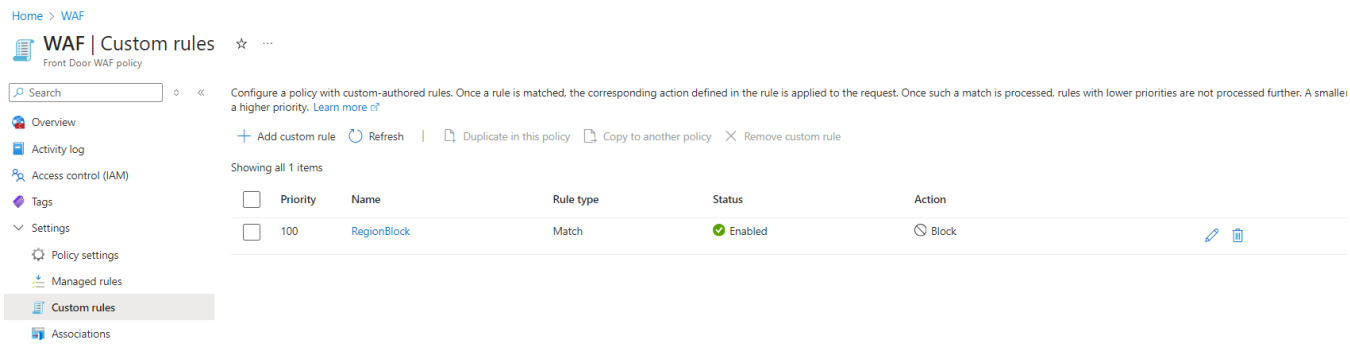


- ***6.1.2 Azure Firewall and WAF Details:***

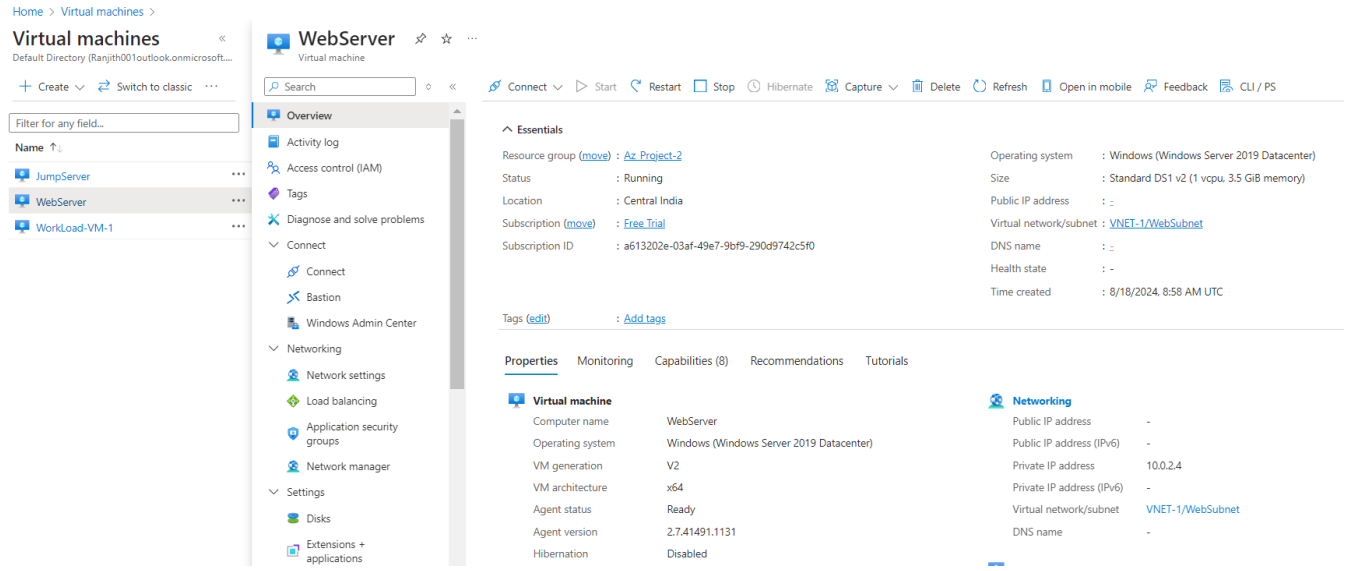




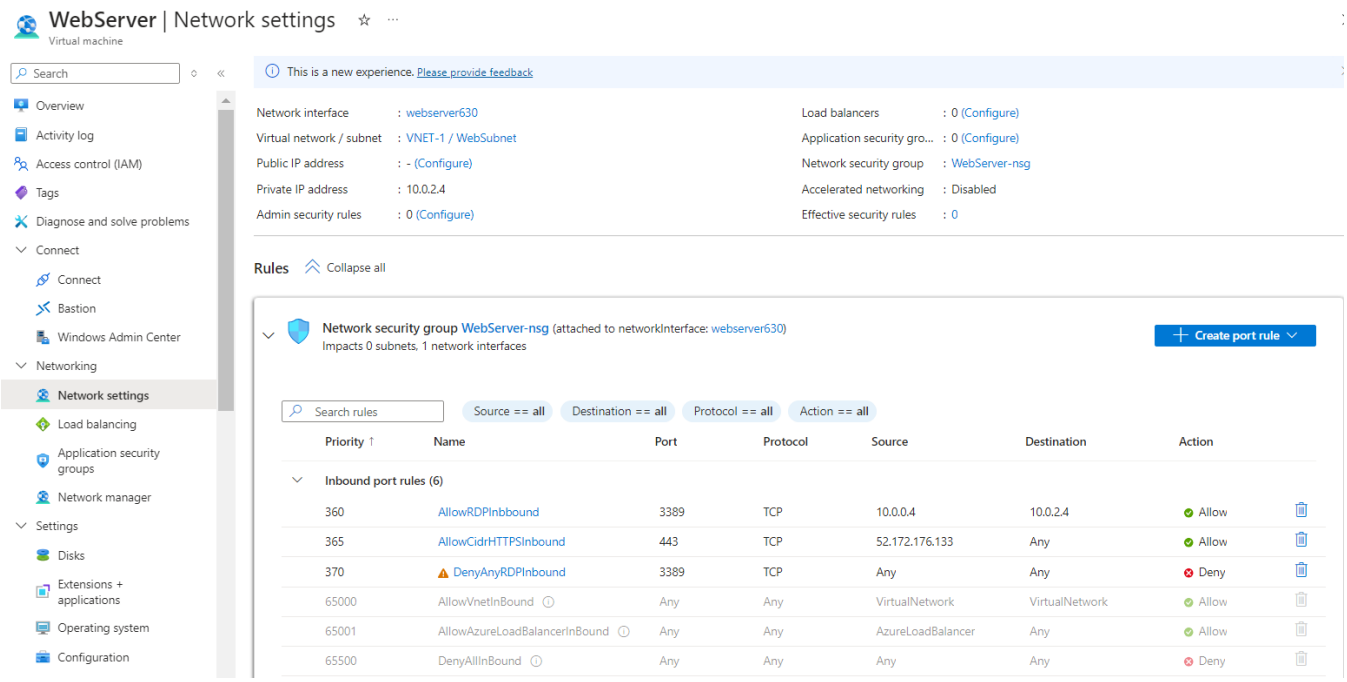




- ***6.1.3 Web Server Details:***

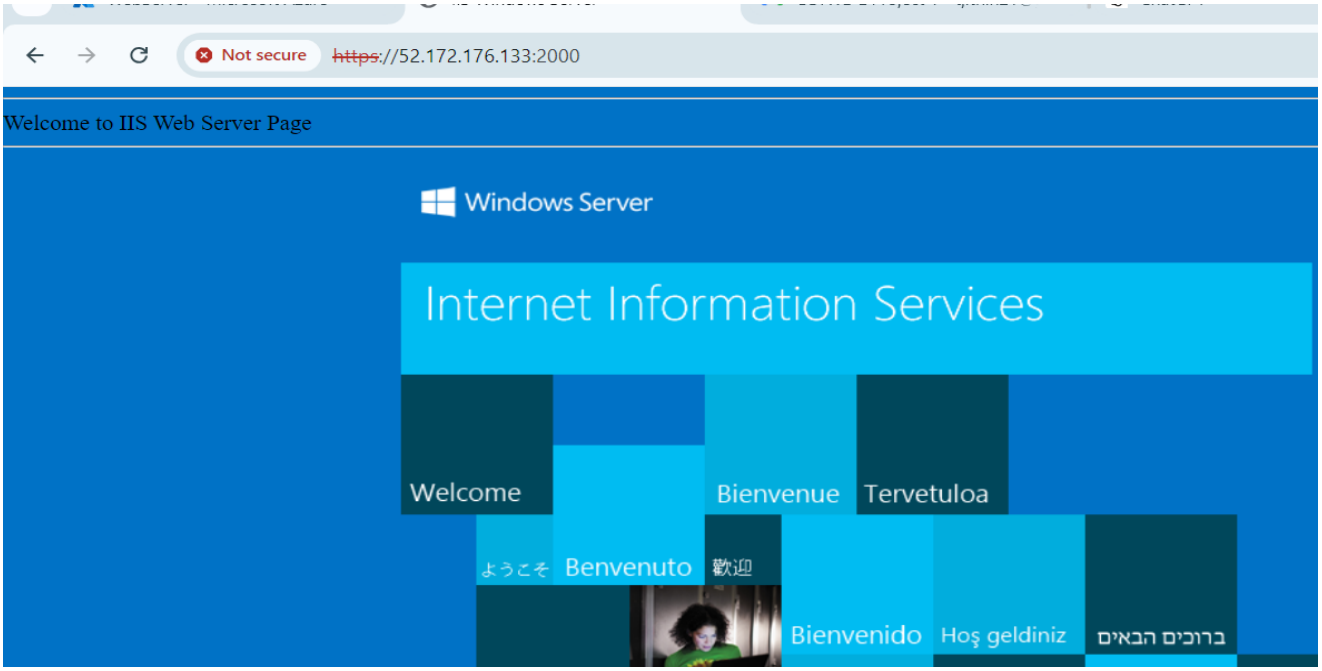


NSG: Allowed Firewall and Jump Server to reach the server.

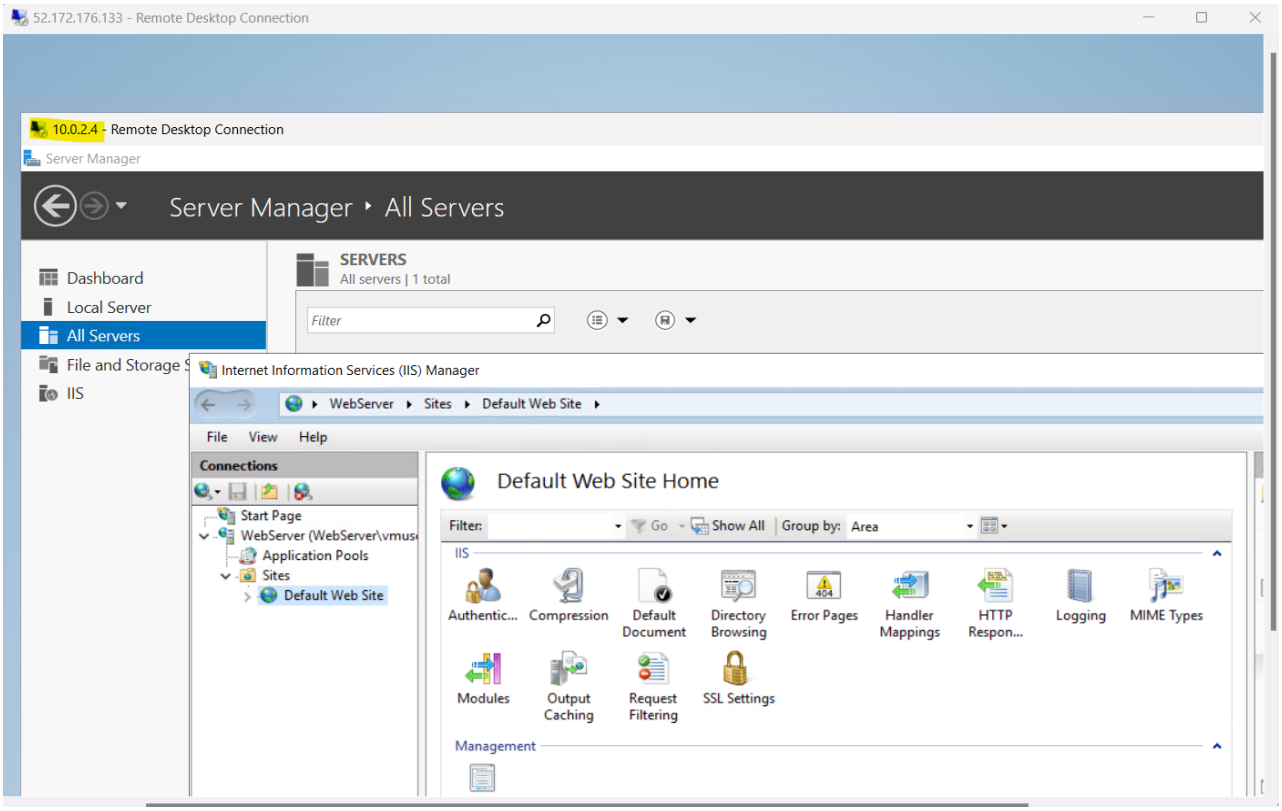


Web Access from Firewall:

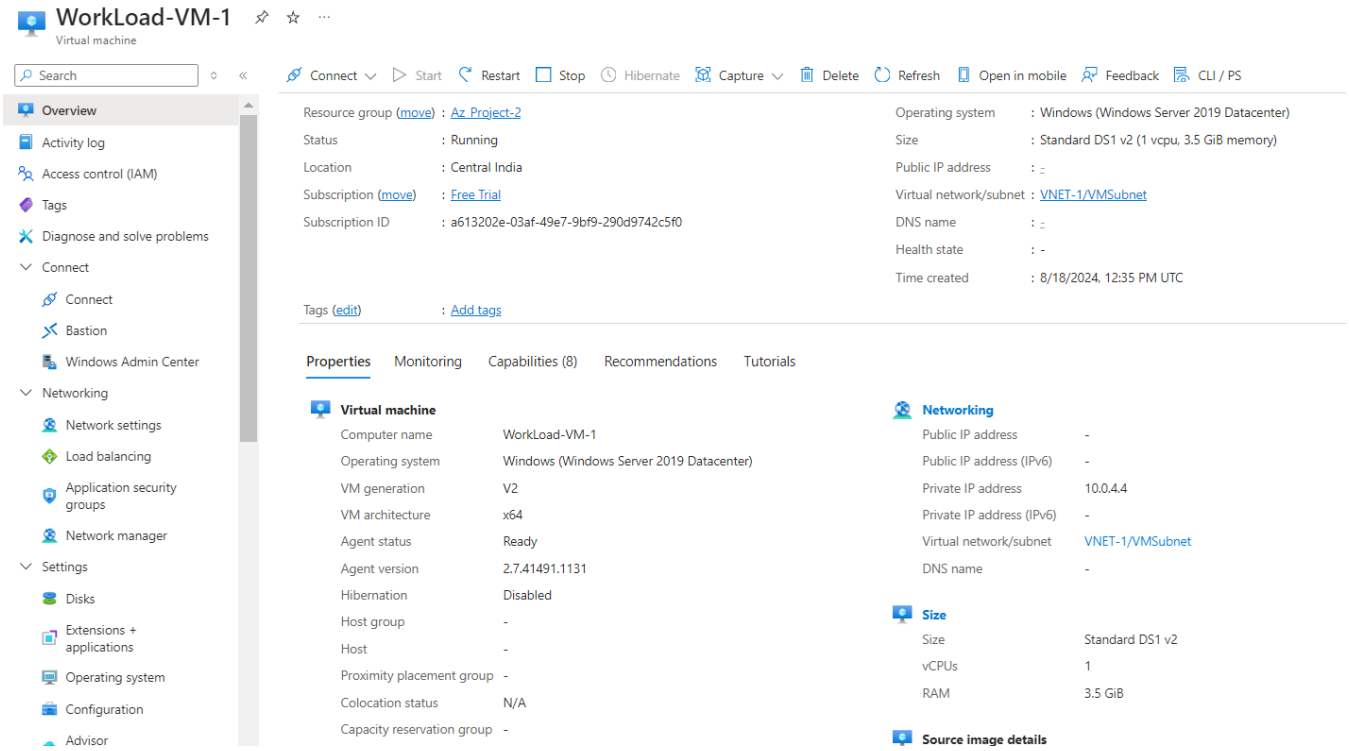
https://52.172.176.133:2000



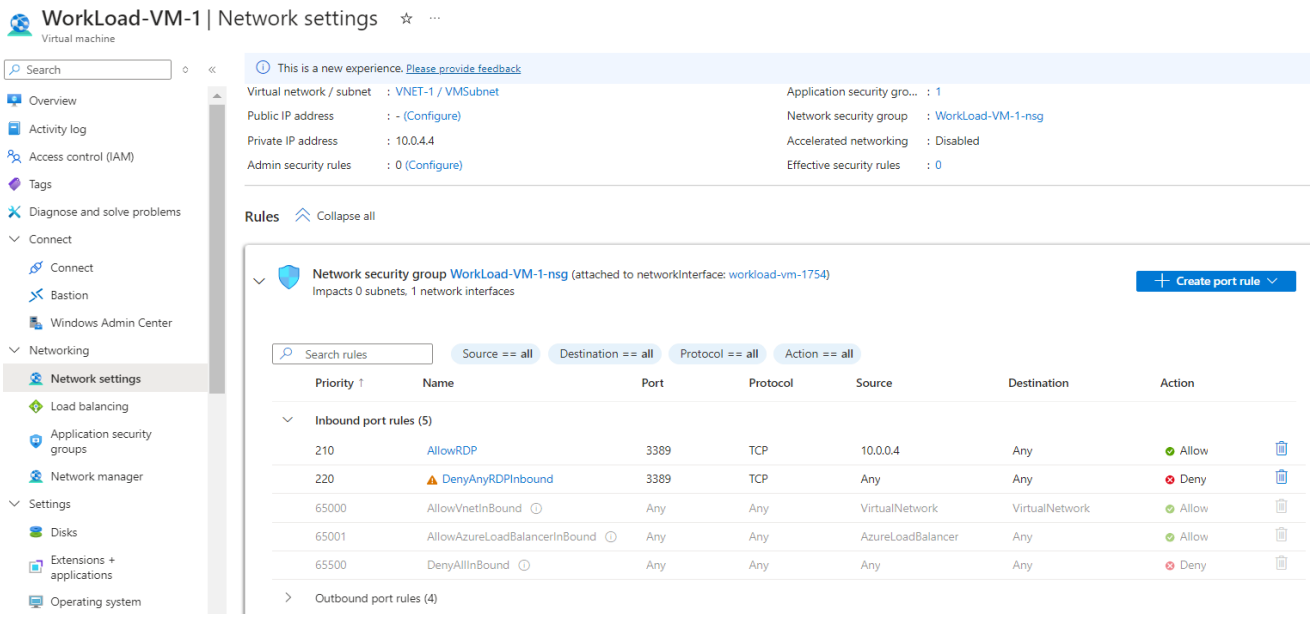
RDP from Jump Server:

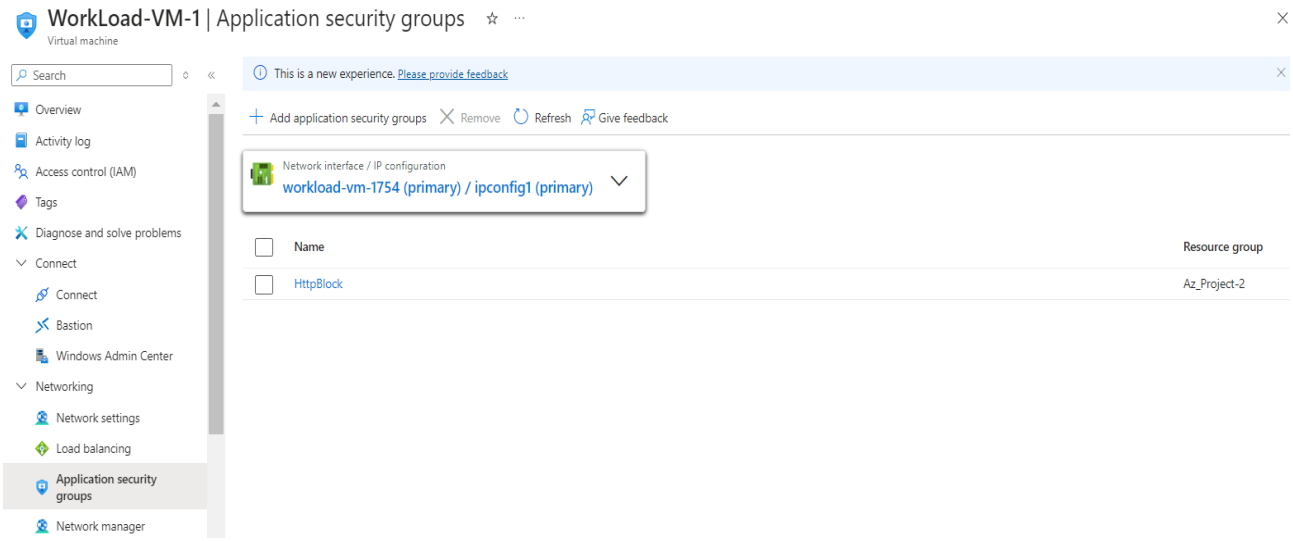


- ***6.1.4 Workload-VM-1 Server Details:***

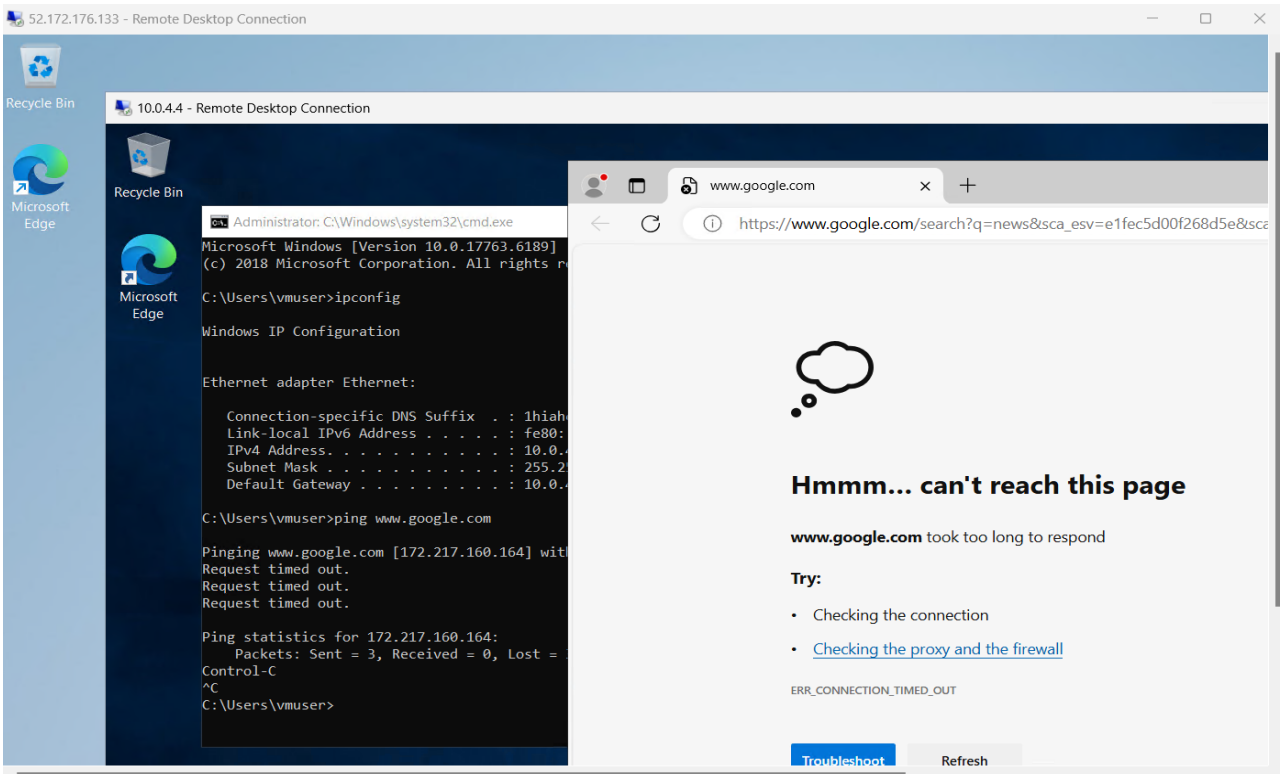


NSG: Allowed RDP from Jump Server and Blocked Internet Server via ASG.

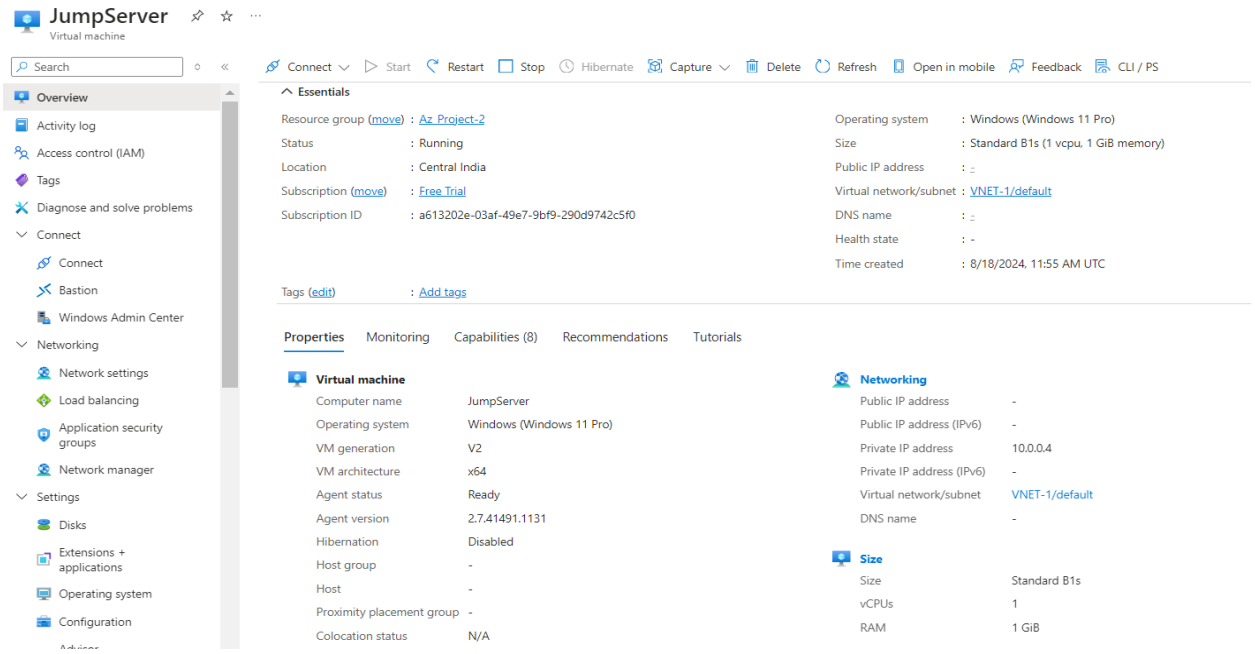




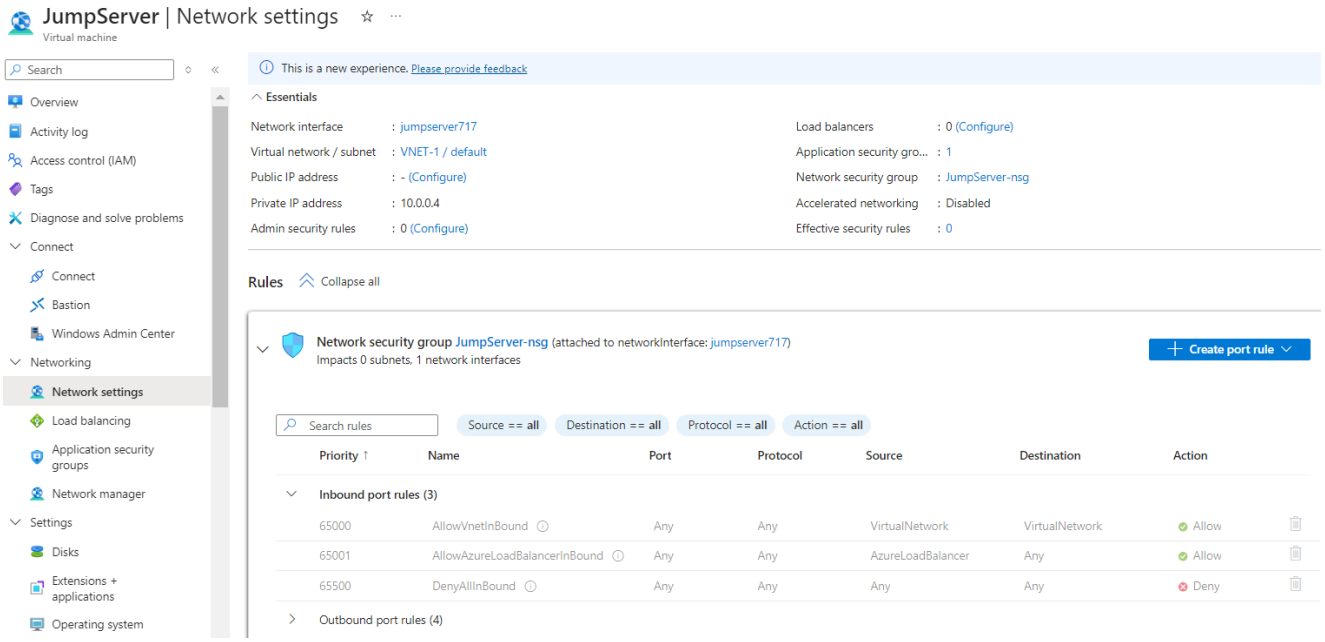
Internet Service is blocked.

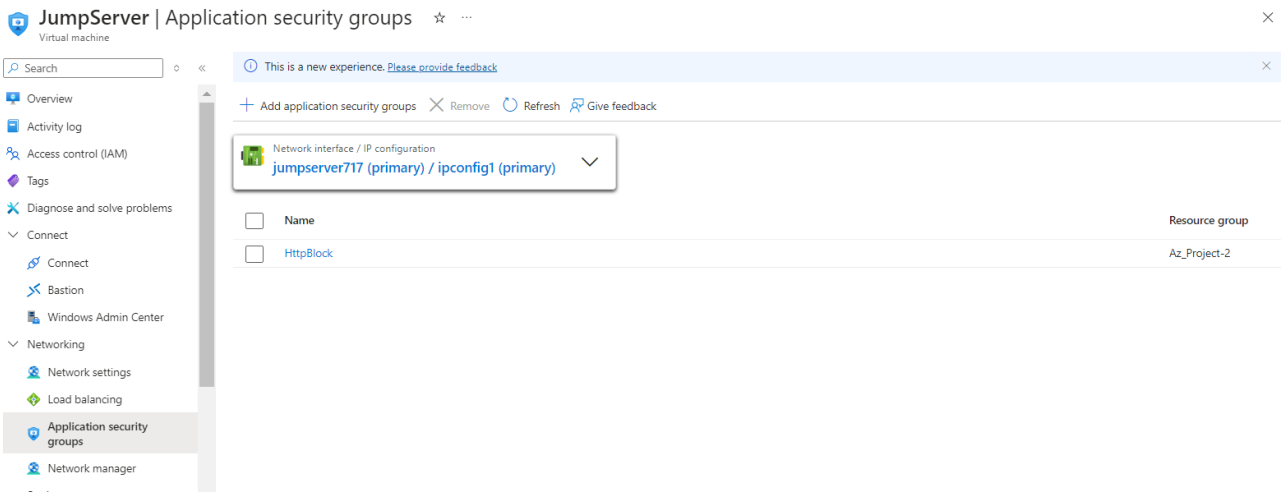


- ***6.1.5 Jump Server Details:***

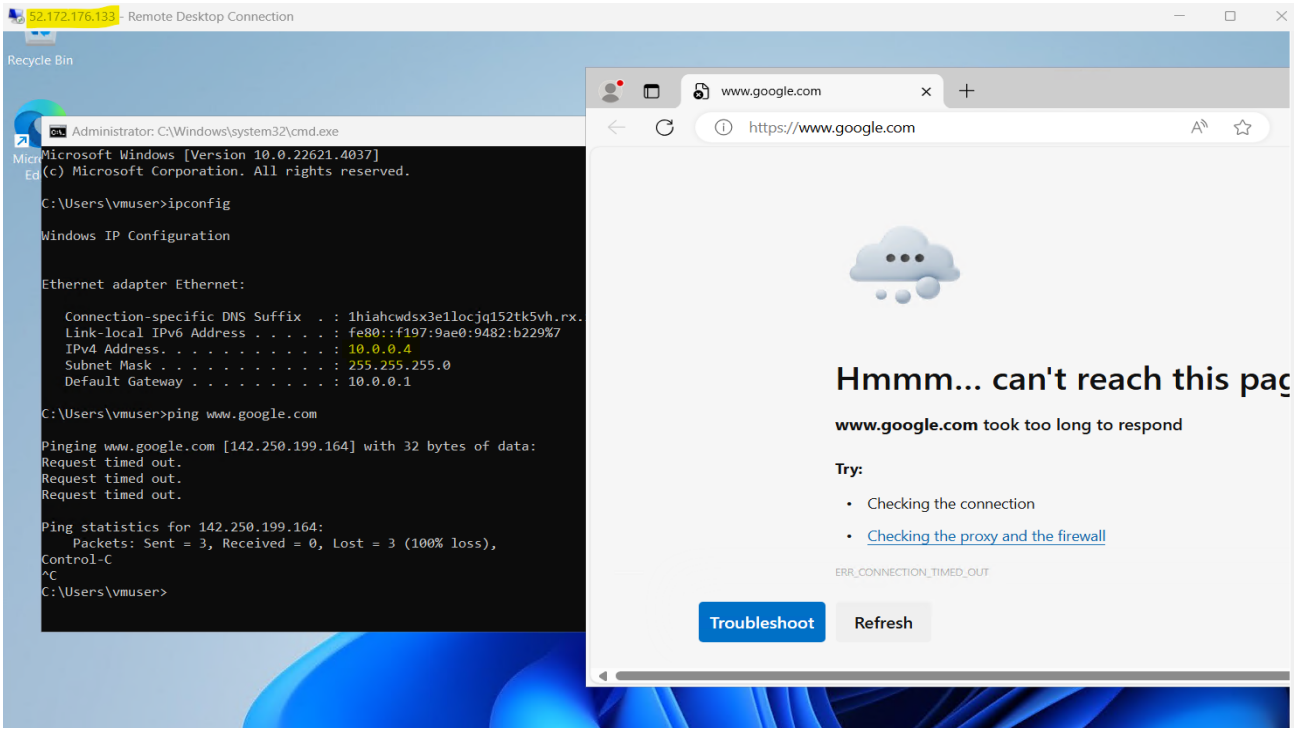


NSG: RDP is not configured in inbound rule but can take RDP access due to Port opening in Firewall pointing to Jump server. Internet is blocked by ASG.





RDP Access via Firewall and Internet Service Block.



Conclusion Summary:

1. Configured Centralized Azure Firewall to access web server and Jump server
2. Configured DNAT rule to route the traffic from firewall to server Private IP with particular port.
3. WAF is configured as global level to block specific region traffic hits.
4. In Jump server and Workload server VM Internet service is blocked by applying ASG.
5. NSG is configured for all server to resist inbound and outbound access.
6. All Server can be manageable via Jump server only. All Public access is blocked.

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