

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).

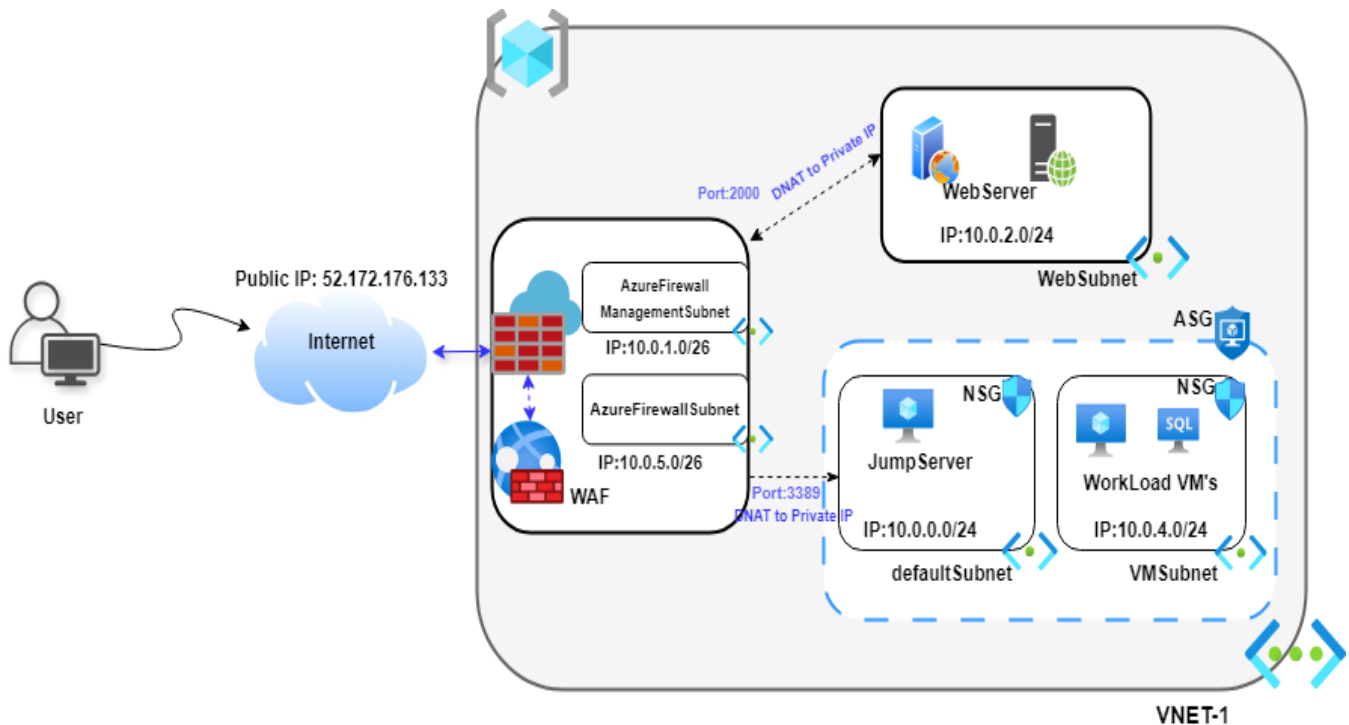
3. Goals and Objectives:

- **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	Associated 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:

Microsoft Azure

Upgrade

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

Copilot

Home > VNET-1

VNET-1 | Subnets

Virtual network

Search

+ Subnet + Gateway subnet Refresh Manage users Delete

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

Bastion

Search subnets

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
default	10.0.0.0/24	-	250	-	-	-
WebSubnet	10.0.2.0/24	-	250	-	-	-
VMSubnet	10.0.4.0/24	-	250	-	-	-
AzureFirewallSubnet	10.0.5.0/26	-	56	-	-	-
AzureFirewallManagementSubnet	10.0.1.0/26	-	56	-	-	-

• 6.1.2 Azure Firewall and WAF Details:

Home > Firewall > Firewall-Policies

Firewall-Policies | Rule collections

Search Add Delete

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Parent policy
 - Rule collections**
 - DNAT rules
 - Network rules
 - Application rules

Rule collections are sets of rules of the same type, DNAT, network, or application rules. Rule collection groups can include rule collections of various types.

Name	Type	Priority	Rules
DefaultDnatRuleCollectionGroup	Rule collection group	100	2
WebAccess	DNAT rule collection	200	1
RDP_Access	DNAT rule collection	201	1
DefaultApplicationRuleCollectionGroup	Rule collection group	300	0

Home > Firewall > Firewall-Policies

Firewall-Policies | DNAT rules

Search Add a rule collection Add rule Edit Delete

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Parent policy
 - Rule collections
 - DNAT rules**
 - Network rules

Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.

Rule Collection P...	Rule collection n...	Rule name	Source	Port	Protocol	Destination	Translated Address ...	Translated Port	Action
Rule Collection Group: DefaultDnatRuleCollectionGroup with priority 100.									
<input type="checkbox"/>	200	WebAccess	Webaccess	* *	2000	TCP	52.172.176.133	10.0.2.4	443 Dnat
<input type="checkbox"/>	201	RDP_Access	RDP	* *	3389	TCP,UDP	52.172.176.133	10.0.0.4	3389 Dnat

Home >

WAF

Search Disable Switch to prevention mode Delete Refresh

- Overview**
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Policy settings
 - Managed rules
 - Custom rules
 - Associations
 - Properties
 - Locks
- Automation

Essentials

Resource group (move)	: Az Project-2	Custom rules	: 1
Status	: Enabled	Associations	: 0
Policy mode	: Detection	Tier	: Azure Front Door Classic
Subscription (move)	: Free Trial		
Subscription ID	: a613202e-03af-49e7-9bf9-290d9742c5f0		
Tags (edit)	: Add tags		

Policy settings
Configure multiple settings that apply to all rules within the policy.

Managed rules
Configure Azure managed rule sets that protect your web application from common threats.

Custom rules
Author custom rules to protect your web application from specifically identified threats.

Associations
Associate a WAF policy with one or more domains hosted on Front Door.

Home > WAF

WAF | Custom rules

Search Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller a higher priority. [Learn more](#)

Add custom rule Refresh Duplicate in this policy Copy to another policy Remove custom rule

Showing all 1 items

Priority	Name	Rule type	Status	Action
<input type="checkbox"/>	100	RegionBlock	Match	Enabled Block

6.1.3 Web Server Details:

The screenshot displays the 'WebServer' virtual machine details in the Azure portal. The left sidebar shows the 'Virtual machines' overview with a list of VMs: JumpServer, WebServer, and Workload-VM-1. The 'WebServer' VM is selected, and its details are shown on the right. The 'Overview' tab is active, displaying the VM's status as 'Running' and its location as 'Central India'. The 'Essentials' section shows the resource group 'Az-Project-2', the subscription 'Free Trial', and the subscription ID 'a613202e-03af-49e7-9bf9-290d9742c5f0'. The 'Properties' section shows the VM's name 'WebServer', operating system 'Windows (Windows Server 2019 Datacenter)', VM generation 'V2', VM architecture 'x64', agent status 'Ready', agent version '2.7.41491.1131', and hibernation 'Disabled'. The 'Networking' section shows the public IP address '10.0.2.4', private IP address '10.0.2.4', virtual network/subnet 'VNET-1/WebSubnet', and DNS name 'VNET-1/WebSubnet'.

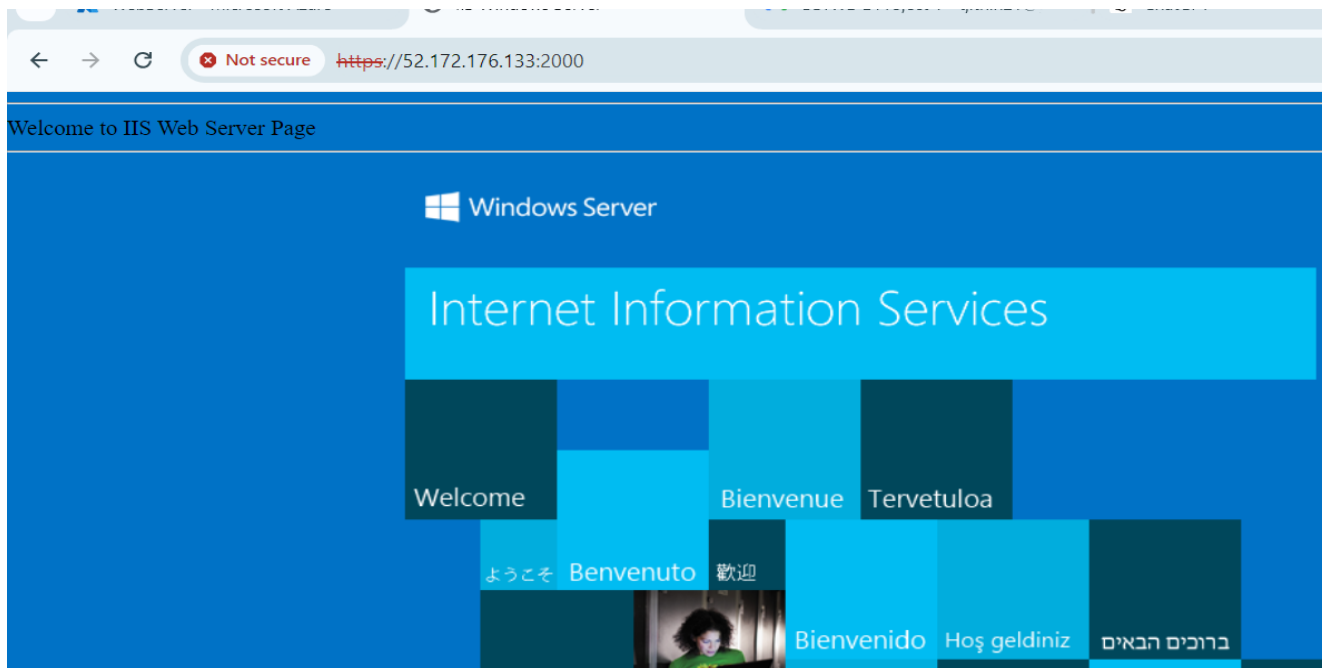
NSG: Allowed Firewall and Jump Server to reach the server.

The screenshot displays the 'WebServer | Network settings' page in the Azure portal. The left sidebar shows the 'Virtual machines' overview with a list of VMs: JumpServer, WebServer, and Workload-VM-1. The 'WebServer' VM is selected, and its network settings are shown on the right. The 'Network settings' section shows the network interface 'webserver630', virtual network/subnet 'VNET-1 / WebSubnet', public IP address '10.0.2.4', private IP address '10.0.2.4', and admin security rules '0 (Configure)'. The 'Rules' section shows the network security group 'WebServer-nsg' (attached to networkInterface: webserver630) and its rules. The rules table is as follows:

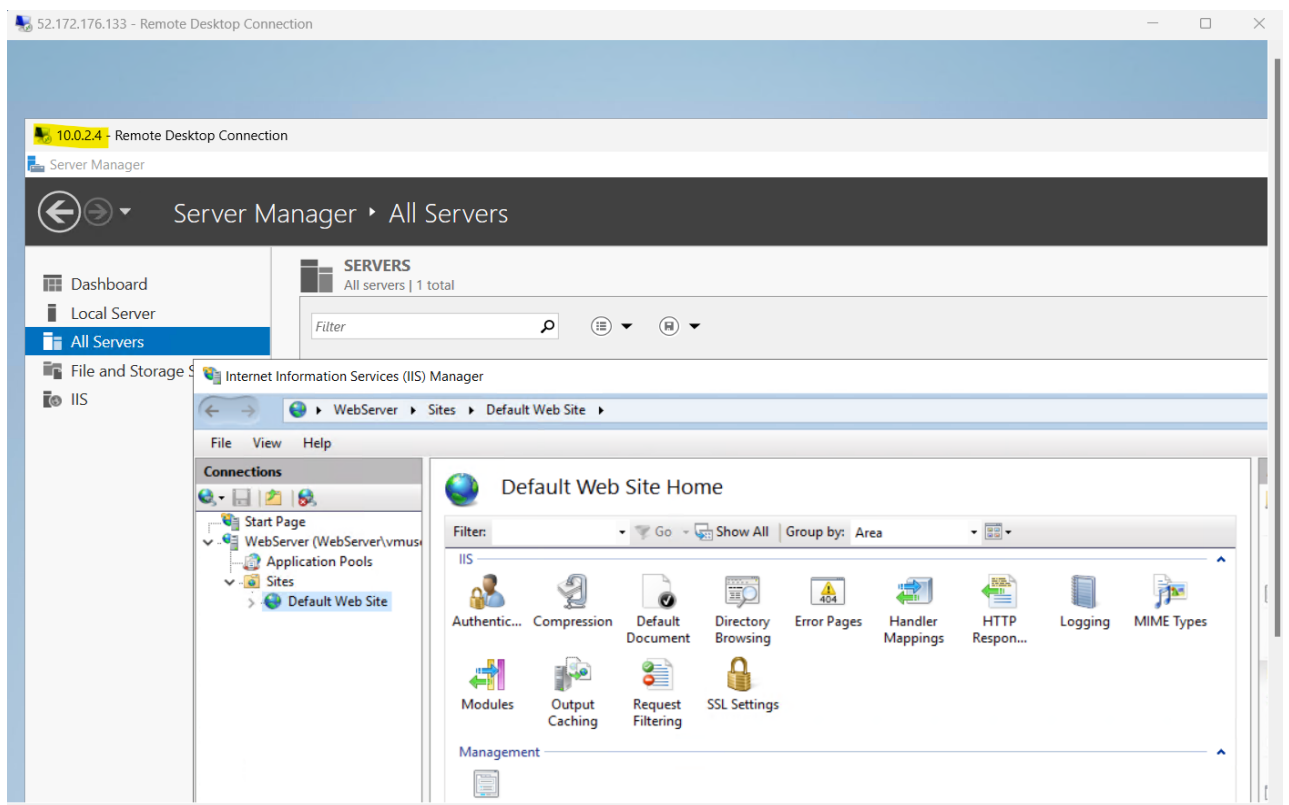
Priority	Name	Port	Protocol	Source	Destination	Action
360	AllowRDPInbound	3389	TCP	10.0.0.4	10.0.2.4	Allow
365	AllowCidrHTTPSInbound	443	TCP	52.172.176.133	Any	Allow
370	DenyAnyRDPInbound	3389	TCP	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Web Access from Firewall:

<https://52.172.176.133:2000>



RDP from Jump Server:



- 6.1.4 Workload-VM-1 Server Details:

WorkLoad-VM-1

Virtual machine

Search

ConnectStartRestartStopHibernateCaptureDeleteRefreshOpen in mobileFeedbackCLI / PS

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Windows Admin Center

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

Operating system

Configuration

Advisor

Resource group (move) : [Az Project-2](#)

Status : Running

Location : Central India

Subscription (move) : [Free Trial](#)

Subscription ID : a613202e-03af-49e7-9bf9-290d9742c5f0

Operating system : Windows (Windows Server 2019 Datacenter)

Size : Standard DS1 v2 (1 vcpu, 3.5 GiB memory)

Public IP address : -

Virtual network/subnet : [VNET-1/VMSubnet](#)

DNS name : -

Health state : -

Time created : 8/18/2024, 12:35 PM UTC

Tags (edit) : [Add tags](#)

PropertiesMonitoringCapabilities (8)RecommendationsTutorials

Virtual machine

Computer name : WorkLoad-VM-1

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 : -

Colocation status : N/A

Capacity reservation group : -

Networking

Public IP address : -

Public IP address (IPv6) : -

Private IP address : 10.0.4.4

Private IP address (IPv6) : -

Virtual network/subnet : [VNET-1/VMSubnet](#)

DNS name : -

Size

Size : Standard DS1 v2

vCPUs : 1

RAM : 3.5 GiB

Source image details

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

WorkLoad-VM-1 | Network settings

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Windows Admin Center

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

Operating system

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

Virtual network / subnet : [VNET-1 / VMSubnet](#)

Public IP address : - ([Configure](#))

Private IP address : 10.0.4.4

Admin security rules : 0 ([Configure](#))

Application security group : 1

Network security group : [WorkLoad-VM-1-nsg](#)

Accelerated networking : Disabled

Effective security rules : 0

Rules Collapse all

Network security group WorkLoad-VM-1-nsg (attached to networkInterface: workload-vm-1754)

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	Action
Inbound port rules (5)						
210	AllowRDP	3389	TCP	10.0.0.4	Any	Allow
220	DenyAnyRDPInbound	3389	TCP	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (4)						

WorkLoad-VM-1 | Application security groups ☆ ...

Virtual machine

Search

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Connect
Bastion
Windows Admin Center
Networking
Network settings
Load balancing
Application security groups
Network manager

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

+ Add application security groups ✕ Remove ↻ Refresh 🗨 Give feedback

Network interface / IP configuration
workload-vm-1754 (primary) / ipconfig1 (primary) ▼

Name	Resource group
HttpBlock	Az_Project-2

Internet Service is blocked.

52.172.176.133 - Remote Desktop Connection

10.0.4.4 - Remote Desktop Connection

Recycle Bin
Microsoft Edge

Administrator: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.17763.6189]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Users\vmuser>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
    Connection-specific DNS Suffix  . : 1hiah  
    Link-local IPv6 Address . . . . . : fe80:  
    IPv4 Address. . . . . : 10.0.2  
    Subnet Mask . . . . . : 255.2  
    Default Gateway . . . . . : 10.0.2  
  
C:\Users\vmuser>ping www.google.com  
  
Pinging www.google.com [172.217.160.164] with:  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 172.217.160.164:  
    Packets: Sent = 3, Received = 0, Lost = 3 (100%  
Control-C  
C:\Users\vmuser>
```

www.google.com

https://www.google.com/search?q=news&sca_esv=e1fec5d00f268d5e&sc

Hmmm... can't reach this page

www.google.com took too long to respond

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_TIMED_OUT

Troubleshoot Refresh

• 6.1.5 Jump Server Details:

JumpServer

Virtual machine

Search

ConnectStartRestartStopHibernateCaptureDeleteRefreshOpen in mobileFeedbackCLI / PS

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Windows Admin Center

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

Operating system

Configuration

Essentials

Resource group : [Az Project-2](#)

Status : Running

Location : Central India

Subscription : [Free Trial](#)

Subscription ID : a613202e-03af-49e7-9bf9-290d9742c5f0

Operating system : Windows (Windows 11 Pro)

Size : Standard B1s (1 vcpu, 1 GiB memory)

Public IP address : -

Virtual network/subnet : [VNET-1/default](#)

DNS name : -

Health state : -

Time created : 8/18/2024, 11:55 AM UTC

Tags : [Add tags](#)

Properties

Monitoring

Capabilities (8)

Recommendations

Tutorials

Virtual machine

Computer name : JumpServer

Operating system : Windows (Windows 11 Pro)

VM generation : V2

VM architecture : x64

Agent status : Ready

Agent version : 2.7.41491.1131

Hibernation : Disabled

Host group : -

Host : -

Proximity placement group : -

Colocation status : N/A

Networking

Public IP address : -

Public IP address (IPv6) : -

Private IP address : 10.0.0.4

Private IP address (IPv6) : -

Virtual network/subnet : [VNET-1/default](#)

DNS name : -

Size

Size : Standard B1s

vCPUs : 1

RAM : 1 GiB

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.

JumpServer | Network settings

Virtual machine

Search

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

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Windows Admin Center

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

Operating system

Essentials

Network interface : [jumpserver717](#)

Virtual network / subnet : [VNET-1 / default](#)

Public IP address : - [\(Configure\)](#)

Private IP address : 10.0.0.4

Admin security rules : 0 [\(Configure\)](#)

Load balancers : 0 [\(Configure\)](#)

Application security gro... : 1

Network security group : [JumpServer-nsg](#)

Accelerated networking : Disabled

Effective security rules : 0

Rules

Collapse all

Network security group [JumpServer-nsg](#) (attached to networkInterface: [jumpserver717](#))

Impacts 0 subnets, 1 network interfaces

Create port rule

Search rules

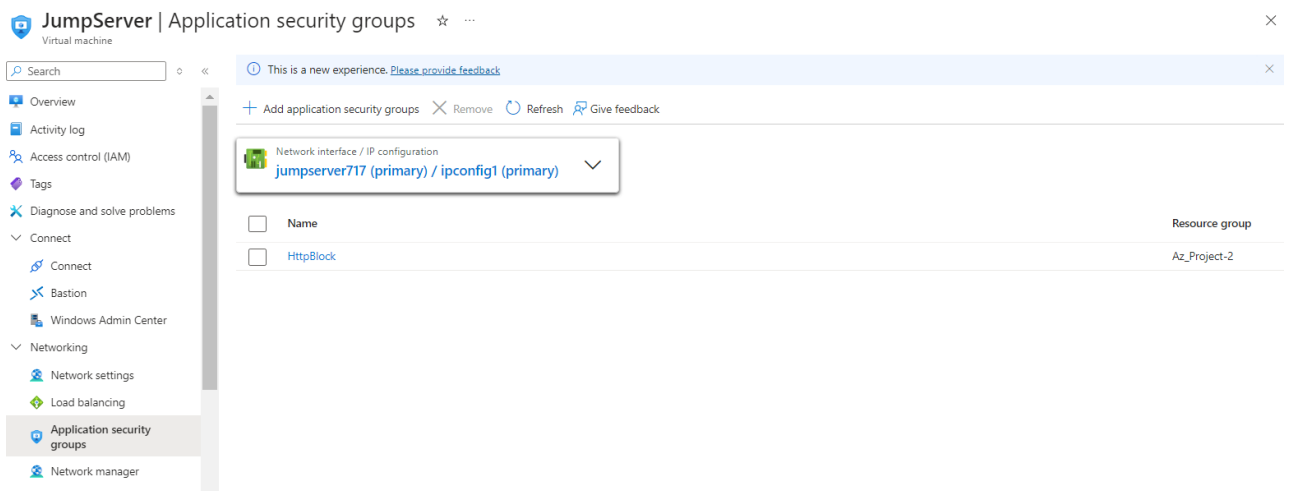
Source == all

Destination == all

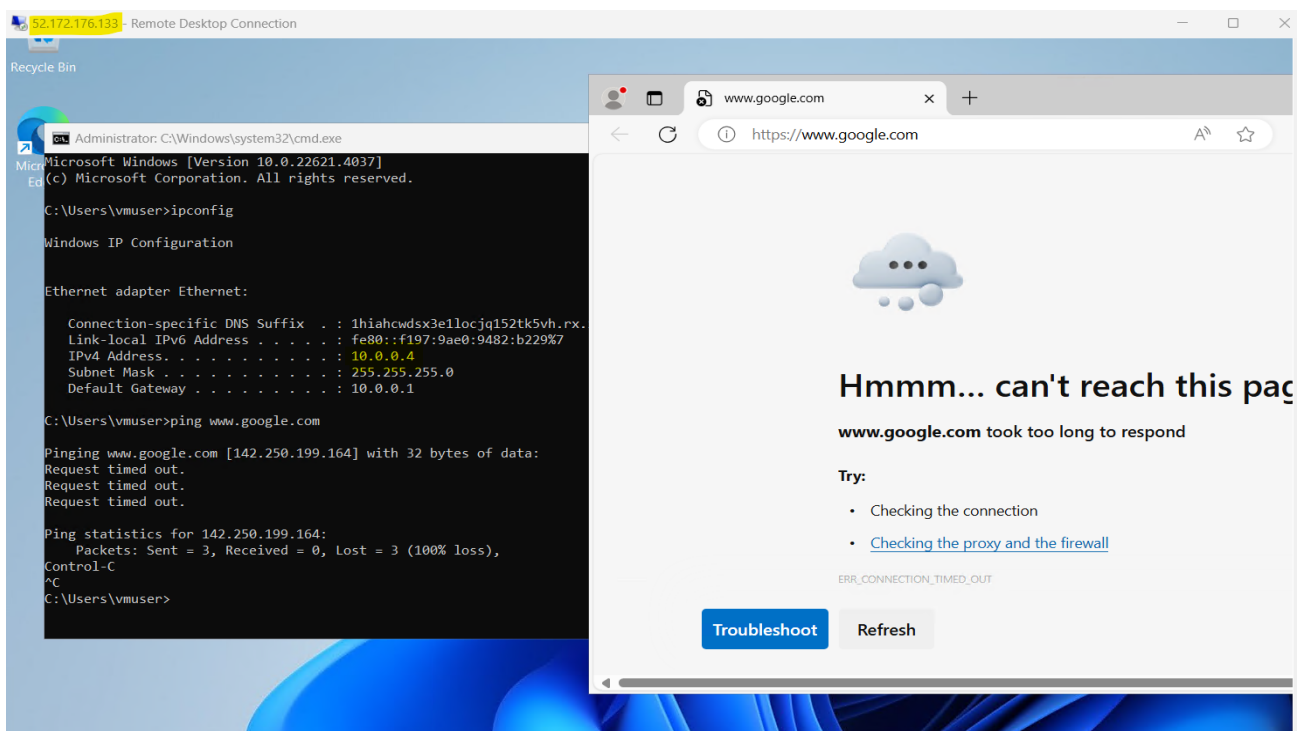
Protocol == all

Action == all

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (3)						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (4)						



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-----