Celebal Technologies

Summer Internship – Assignment - 5 Submission
Department: Cloud Infrastructure & Security
Internship Duration: 19th May 2025 – 20th July 2025

Assignment Title

Networking

Submitted by: Sanchit Mathur
Course: 5-Year Integrated M.Tech (CSE – Cyber Security)
Current Week: 5/12
Assignment: Week 8 Final Project

Submitted to:
Celebal Technologies – CSI Team
Submission Date: 19th June 2025
Portal: [CSI Dashboard – Cloud Infra & Security]

Table of Contents

Table of Figures

Introduction

This assignment presents a comprehensive R&D-based exploration into the workings of Azure networking components, particularly focusing on NSG, ASG, IP access controls, public IP management, service tags, and CLI implementations. This document is aligned with the objectives defined by Celebal Technologies and provides real-world implementation insights.

Network Security Groups (NSG)

Network Security Groups (NSGs) are virtual firewalls in Azure used to filter inbound and outbound network traffic. NSGs contain security rules defined by priority, direction, source/destination, protocol, and access (allow/deny).

Key Concepts:

- Security Rules (Allow/Deny)
- Direction: Inbound/Outbound
- Protocols: TCP, UDP, Any
- Prioritization (lower number = higher priority)
- Scope: Subnet-level or NIC-level application

Default Rules:

- AllowVnetInBound
- AllowAzureLoadBalancerInBound
- DenyAllInBound
- AllowVnetOutBound
- AllowInternetOutBound
- DenyAllOutBound

Application Security Groups (ASG)

Application Security Groups (ASGs) allow you to define and group virtual machines by workload roles, making it easier to manage network security policies.

Benefits:

- Logical VM grouping
- Policy definitions independent of IP
- Easier management for micro-segmentation

Use Cases:

- Multi-tier application isolation (Web, App, DB)
- Auto-scaling environments

IP Access Control (Allowing Specific IPs and Denying Internet Access)

Allowing Specific IPs to Access VMs

- Use NSG rules with source as specific IP addresses.
- Destination should be the VM subnet or ASG.
- Common Ports: 22 (SSH), 3389 (RDP)
- Ensure rule priority is higher than default deny rules.

Denying Internet Access Using NSG

- Create outbound rule in NSG:
    - Destination: Internet
    - Action: Deny
    - Priority: Higher than default AllowInternetOutBound
- Use service endpoints or private endpoints for Azure services if internet is denied.

Public IP Addresses and Types

Public IPs allow Azure resources to be accessed over the internet. Azure supports two types:

Static Public IP:

- IP remains the same until deleted.
- Used in production, DNS, SSL-based workloads.

Dynamic Public IP:

- IP changes when VM is deallocated.
- Used in non-critical/dev environments.

Static vs Dynamic IP

Static IP:

- Predictable addressing
- Required for consistent DNS mapping, firewall rules

Dynamic IP:

- Automatically assigned by Azure
- Reassigned upon VM restart
- Limited use for non-critical access

Service Tags

Service tags simplify security rule creation by representing groups of IPs assigned to Azure services.

Common Service Tags:

- Internet
- VirtualNetwork
- AzureLoadBalancer
- Storage
- Sql

Benefits:

- Reduced rule complexity
- Auto-managed by Microsoft

Static IP Allocation to VMs

To assign a static IP to a VM:

- Reserve a private IP within the subnet range
- Use Azure CLI or Portal to configure it
- For public IP, create and associate a Standard SKU static IP

CLI Example:

```
az network nic create
--resource-group myResourceGroup
--name myNIC
--vnet-name myVNet
--subnet mySubnet
--private-ip-address 10.0.0.10
--public-ip-address myPublicIP
--network-security-group myNSG
```

Creating Network Security Group (NSG)

CLI Command:
```
az network nsg create
--resource-group myResourceGroup
--name myNSG
--location eastus
```

Creating Public IP

CLI Command:
```
az network public-ip create
--resource-group myResourceGroup
--name myPublicIP
--sku Standard
--allocation-method Static
```

Associating/De-associating Public IP with VM

Associate:

```
az network nic ip-config update
--resource-group myResourceGroup
--nic-name myNIC
--name ipconfig1
--public-ip-address myPublicIP
```

De-associate:

```
az network nic ip-config update
--resource-group myResourceGroup
--nic-name myNIC
--name ipconfig1
--remove PublicIpAddress
```

Creating Network Interface

CLI Command:
```
az network nic create
--resource-group myResourceGroup
```

```
--name myNIC
--vnet-name myVNet
--subnet mySubnet
--network-security-group myNSG
```

To include static private IP: --private-ip-address 10.0.0.10

To attach public IP: --public-ip-address myPublicIP

Security Best Practices

NSG:

- Follow least privilege model
- Use descriptive names/comments
- Enable NSG flow logs

ASG:

- Logical grouping
- Clean naming conventions

IP Management:

- Document strategy
- Monitor allocations
- Automate using scripts

Troubleshooting

Connectivity Issues:

- Check NSG rule priorities
- Validate ASG memberships
- Use Azure Network Watcher for diagnostics

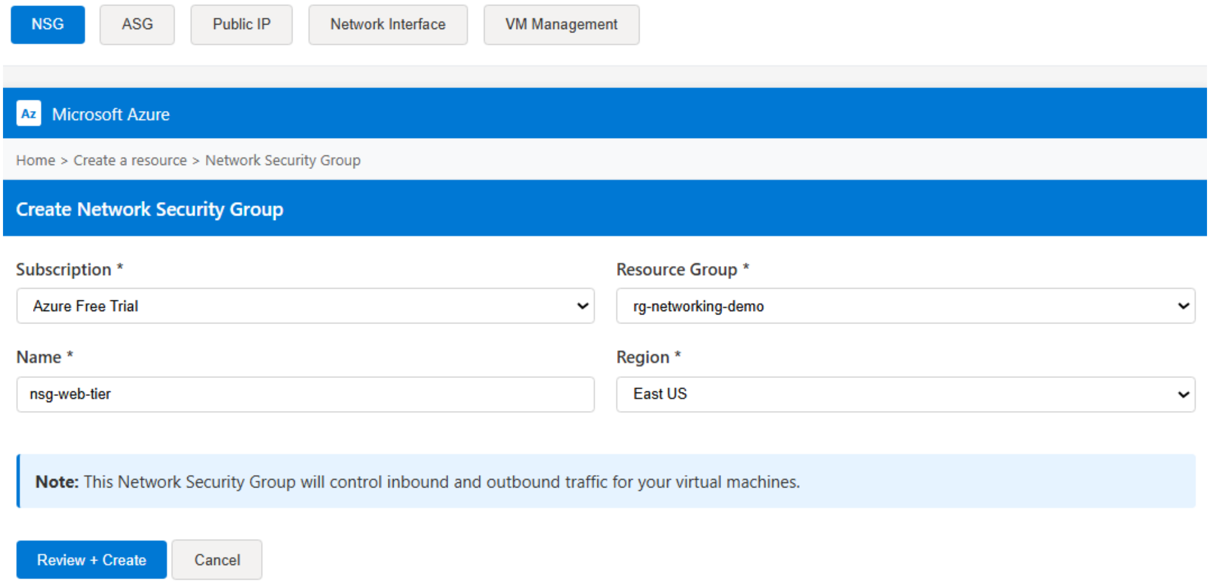
IP Conflicts:

- Verify subnet range and static IP
- Confirm NIC configurations

Conclusion

This R&D assignment provided hands-on understanding of critical Azure networking features. Implementing NSG, ASG, static/dynamic IP configuration, and securing VMs using IP controls and service tags enables organizations to maintain a secure and scalable cloud environment. Regular audits and automation enhance security posture and efficiency.

Screenshots



Home > Create a resource > Network Security Group

Create Network Security Group

Subscription *: Azure Free Trial

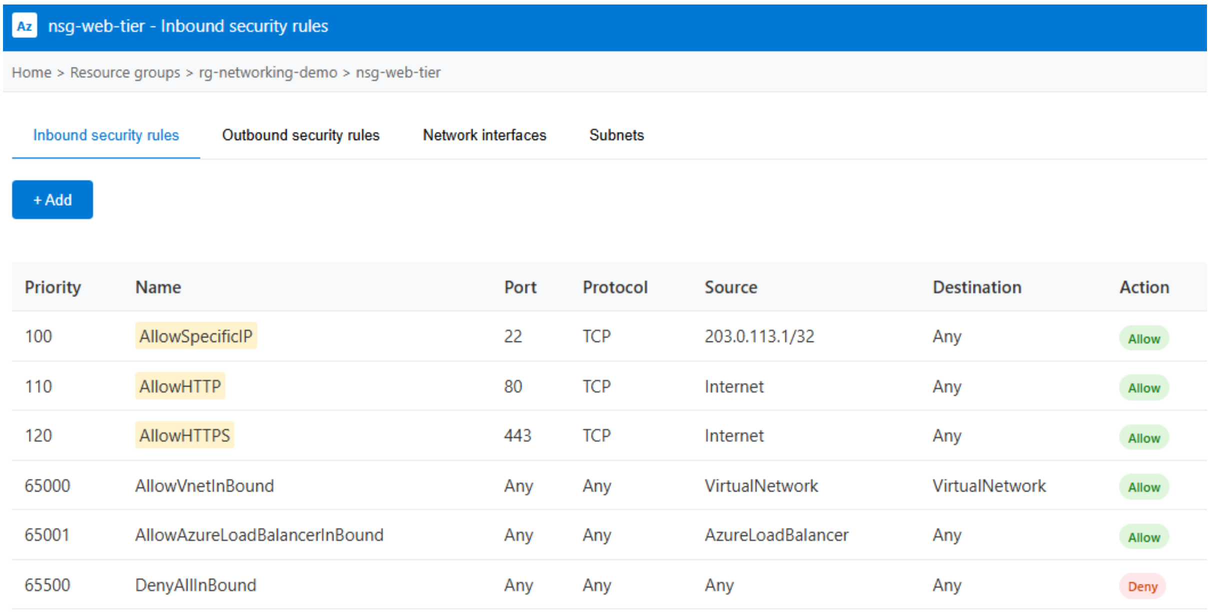
Resource Group *: rg-networking-demo

Name *: nsg-web-tier

Region *: East US

Note: This Network Security Group will control inbound and outbound traffic for your virtual machines.

Figure 1 - Create Network Security Group

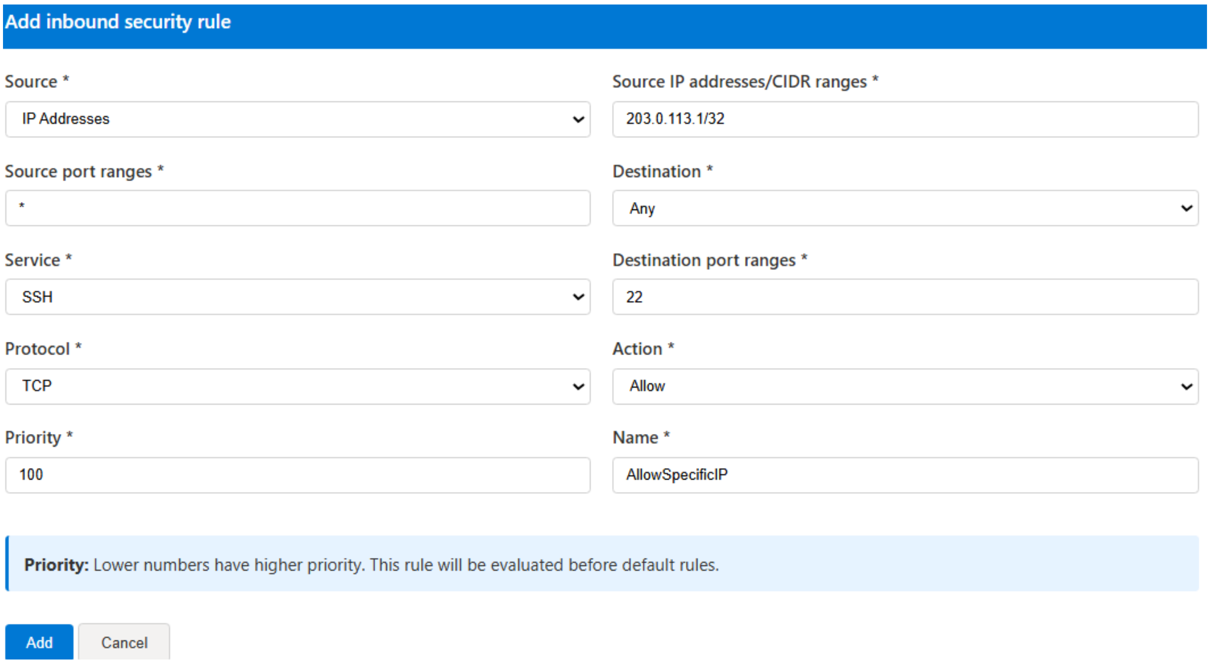


nsg-web-tier - Inbound security rules

Home > Resource groups > rg-networking-demo > nsg-web-tier

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowSpecificIP	22	TCP	203.0.113.1/32	Any	Allow
110	AllowHTTP	80	TCP	Internet	Any	Allow
120	AllowHTTPS	443	TCP	Internet	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Figure 2 - nsg-web-tier - Inbound security rules



Add inbound security rule

Source *: IP Addresses

Source IP addresses/CIDR ranges *: 203.0.113.1/32

Source port ranges *: *

Destination *: Any

Service *: SSH

Destination port ranges *: 22

Protocol *: TCP

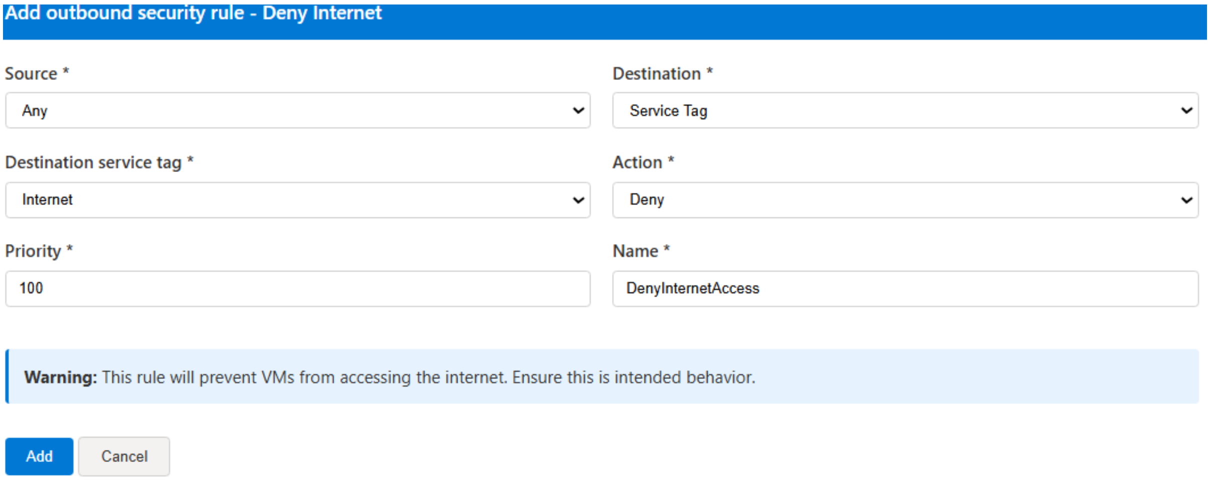
Action *: Allow

Priority *: 100

Name *: AllowSpecificIP

Priority: Lower numbers have higher priority. This rule will be evaluated before default rules.

Figure 3 - Add inbound security rule



Add outbound security rule - Deny Internet

Source *: Any

Destination *: Service Tag

Destination service tag *: Internet

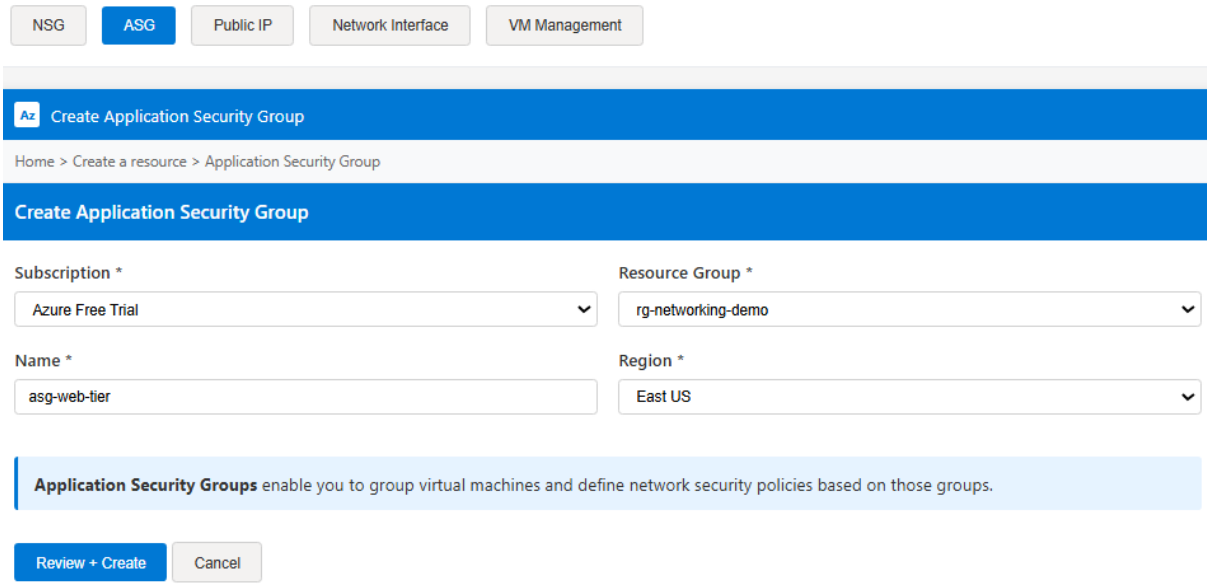
Action *: Deny

Priority *: 100

Name *: DenyInternetAccess

Warning: This rule will prevent VMs from accessing the internet. Ensure this is intended behavior.

Figure 4 - Add outbound security rule - Deny Internet



Create Application Security Group

Home > Create a resource > Application Security Group

Create Application Security Group

Subscription *: Azure Free Trial

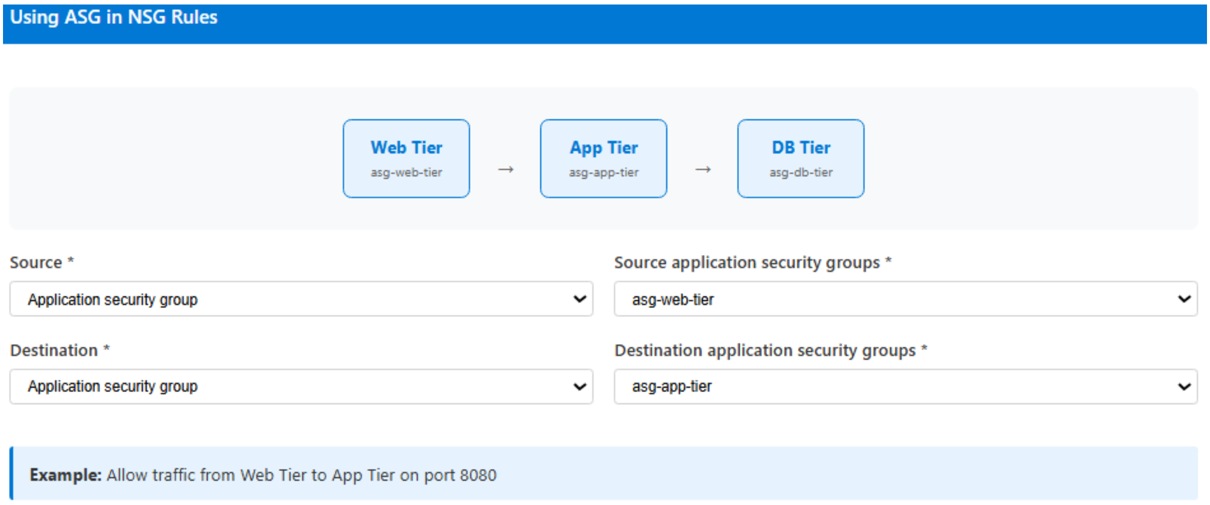
Resource Group *: rg-networking-demo

Name *: asg-web-tier

Region *: East US

Application Security Groups enable you to group virtual machines and define network security policies based on those groups.

Figure 5 - Create Application Security Group



Using ASG in NSG Rules

Source *: Application security group

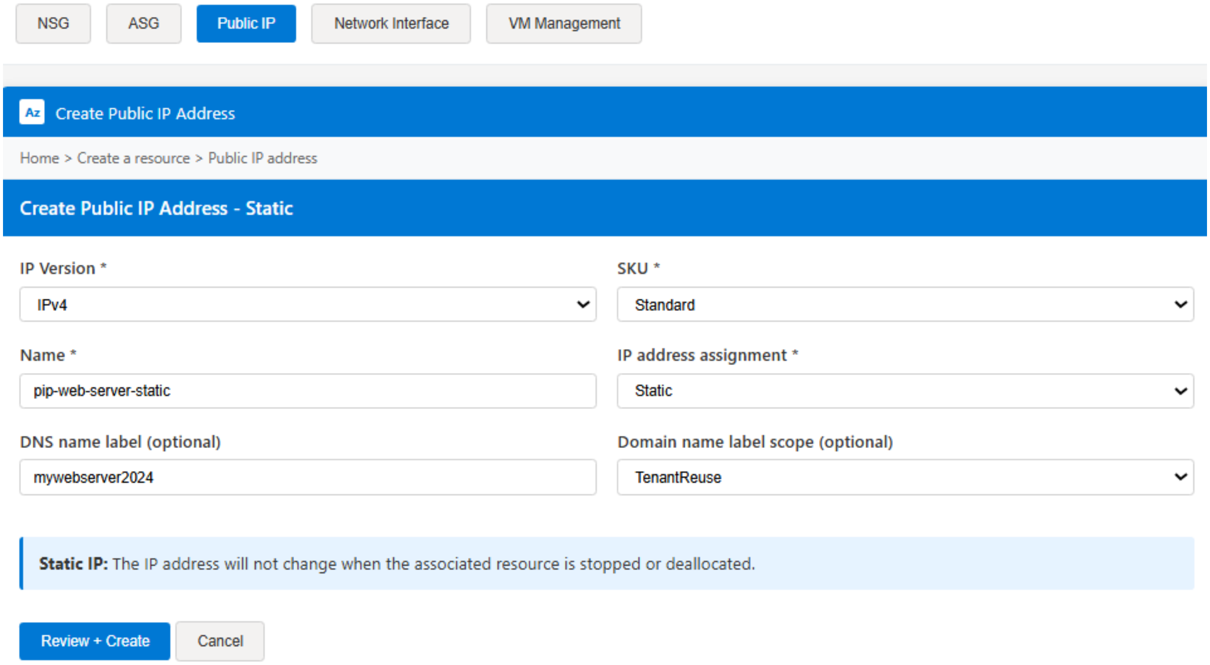
Source application security groups *: asg-web-tier

Destination *: Application security group

Destination application security groups *: asg-app-tier

Example: Allow traffic from Web Tier to App Tier on port 8080

Figure 6 - Using ASG in NSG Rules



Create Public IP Address

Home > Create a resource > Public IP address

Create Public IP Address - Static

IP Version *: IPv4

SKU *: Standard

Name *: pip-web-server-static

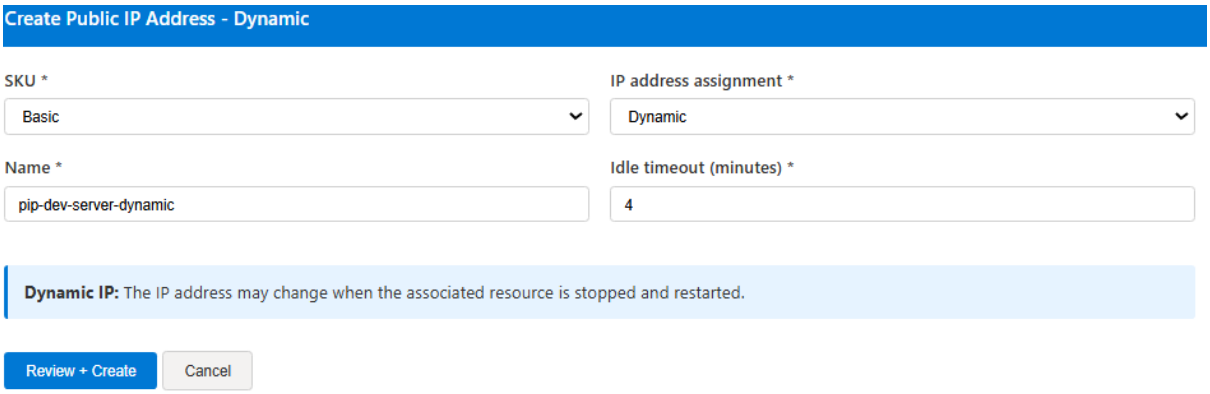
IP address assignment *: Static

DNS name label (optional): mywebserver2024

Domain name label scope (optional): TenantReuse

Static IP: The IP address will not change when the associated resource is stopped or deallocated.

Figure 7 - Create Public IP Address – Static



Create Public IP Address - Dynamic

SKU *: Basic

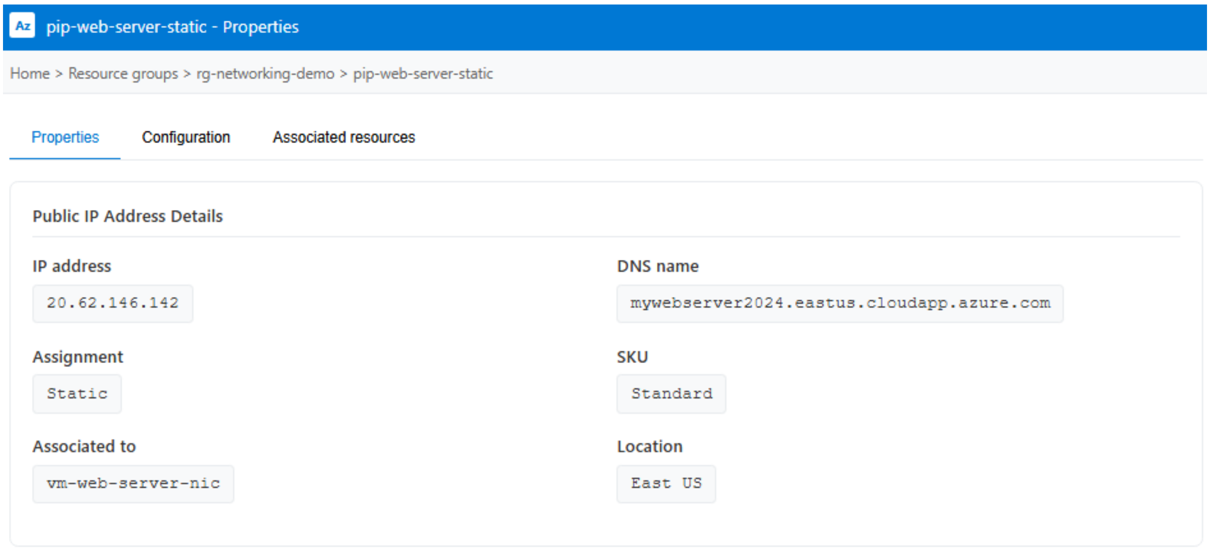
IP address assignment *: Dynamic

Name *: pip-dev-server-dynamic

Idle timeout (minutes) *: 4

Dynamic IP: The IP address may change when the associated resource is stopped and restarted.

Figure 8 - Create Public IP Address – Dynamic



pip-web-server-static - Properties

Home > Resource groups > rg-networking-demo > pip-web-server-static

Public IP Address Details

IP address: 20.62.146.142

DNS name: mywebserver2024.eastus.cloudapp.azure.com

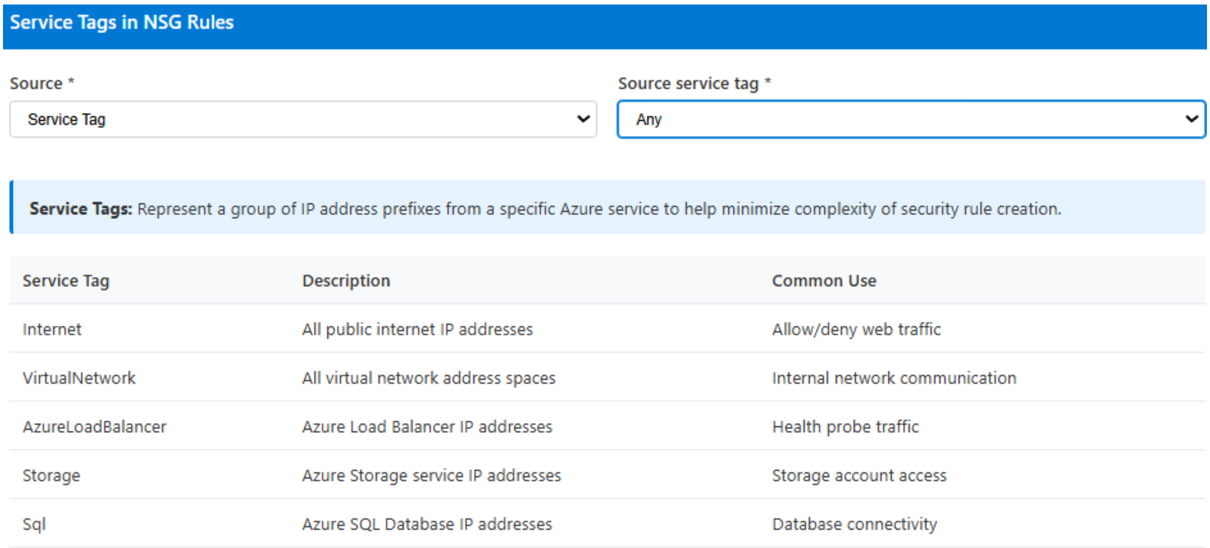
Assignment: Static

SKU: Standard

Associated to: vm-web-server-nic

Location: East US

Figure 9 - pip-web-server-static – Properties



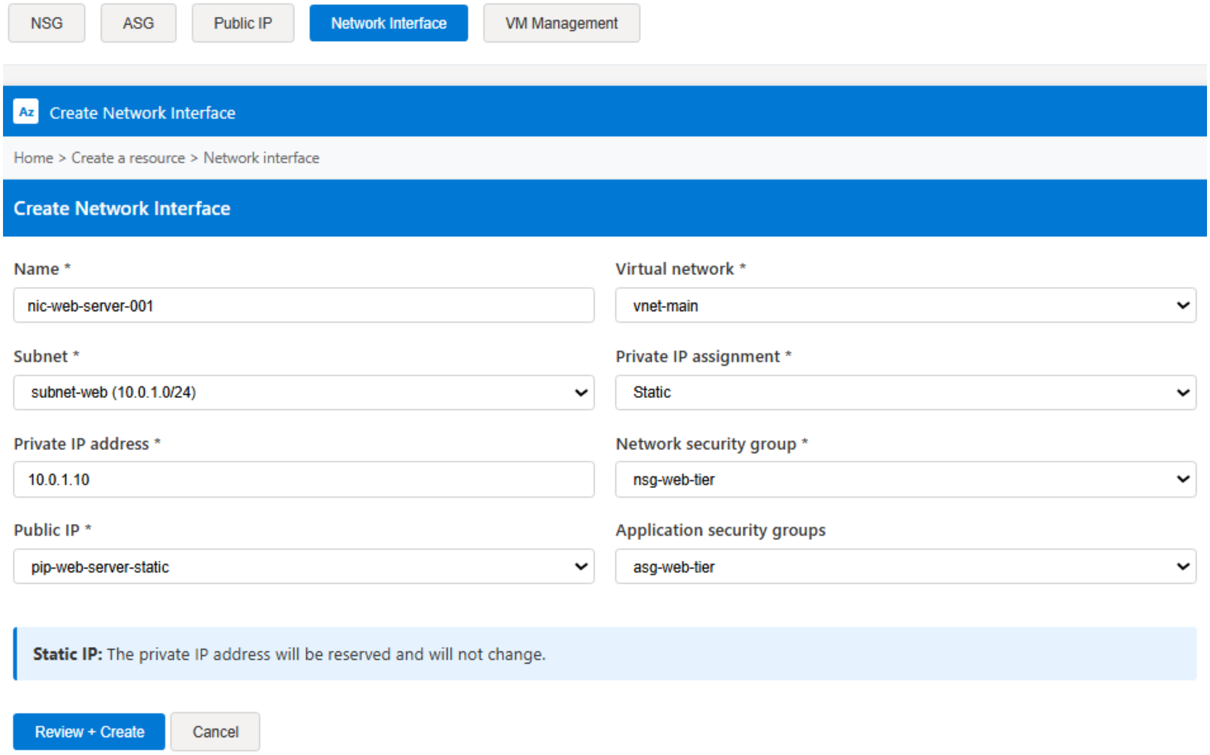
Service Tags in NSG Rules

Source *	Service Tag
Source service tag *	Any

Service Tags: Represent a group of IP address prefixes from a specific Azure service to help minimize complexity of security rule creation.

Service Tag	Description	Common Use
Internet	All public internet IP addresses	Allow/deny web traffic
VirtualNetwork	All virtual network address spaces	Internal network communication
AzureLoadBalancer	Azure Load Balancer IP addresses	Health probe traffic
Storage	Azure Storage service IP addresses	Storage account access
Sql	Azure SQL Database IP addresses	Database connectivity

Figure 10 - Service Tags in NSG Rules

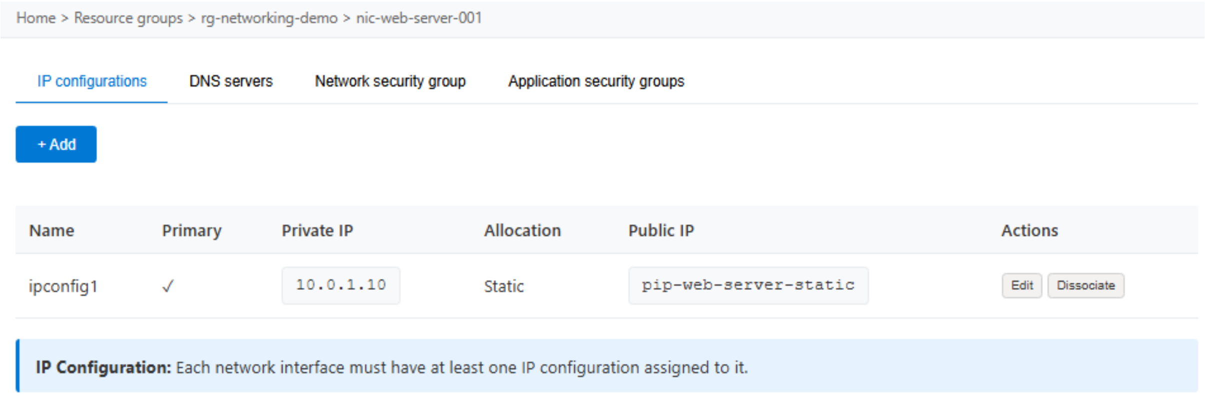


Create Network Interface

Name *	nic-web-server-001
Virtual network *	vnet-main
Subnet *	subnet-web (10.0.1.0/24)
Private IP assignment *	Static
Private IP address *	10.0.1.10
Network security group *	nsg-web-tier
Public IP *	pip-web-server-static
Application security groups	asg-web-tier

Static IP: The private IP address will be reserved and will not change.

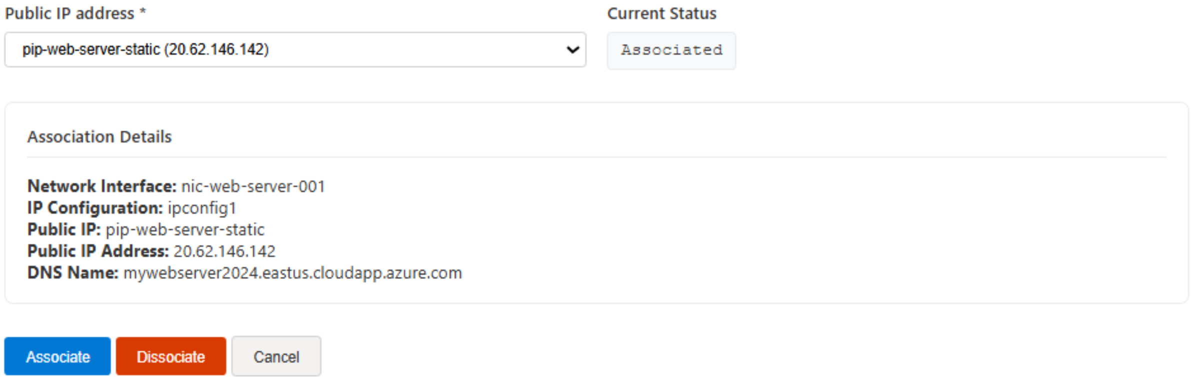
Figure 11 - Create Network Interface


Home > Resource groups > rg-networking-demo > nic-web-server-001
IP configurations
DNS servers
Network security group
Application security groups
+ Add

Name	Primary	Private IP	Allocation	Public IP	Actions
ipconfig1	✓	10.0.1.10	Static	pip-web-server-static	Edit Dissociate

IP Configuration: Each network interface must have at least one IP configuration assigned to it.

Figure 12 - nic-web-server-001 - IP configurations

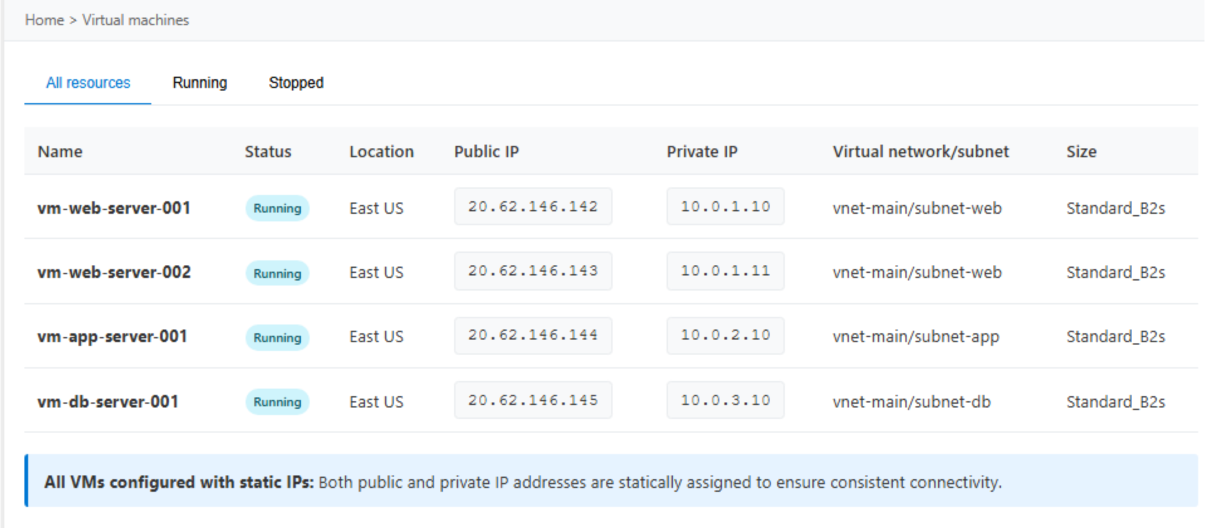


Public IP address *	pip-web-server-static (20.62.146.142)
Current Status	Associated

Association Details

Network Interface: nic-web-server-001
IP Configuration: ipconfig1
Public IP: pip-web-server-static
Public IP Address: 20.62.146.142
DNS Name: mywebserver2024.eastus.cloudapp.azure.com

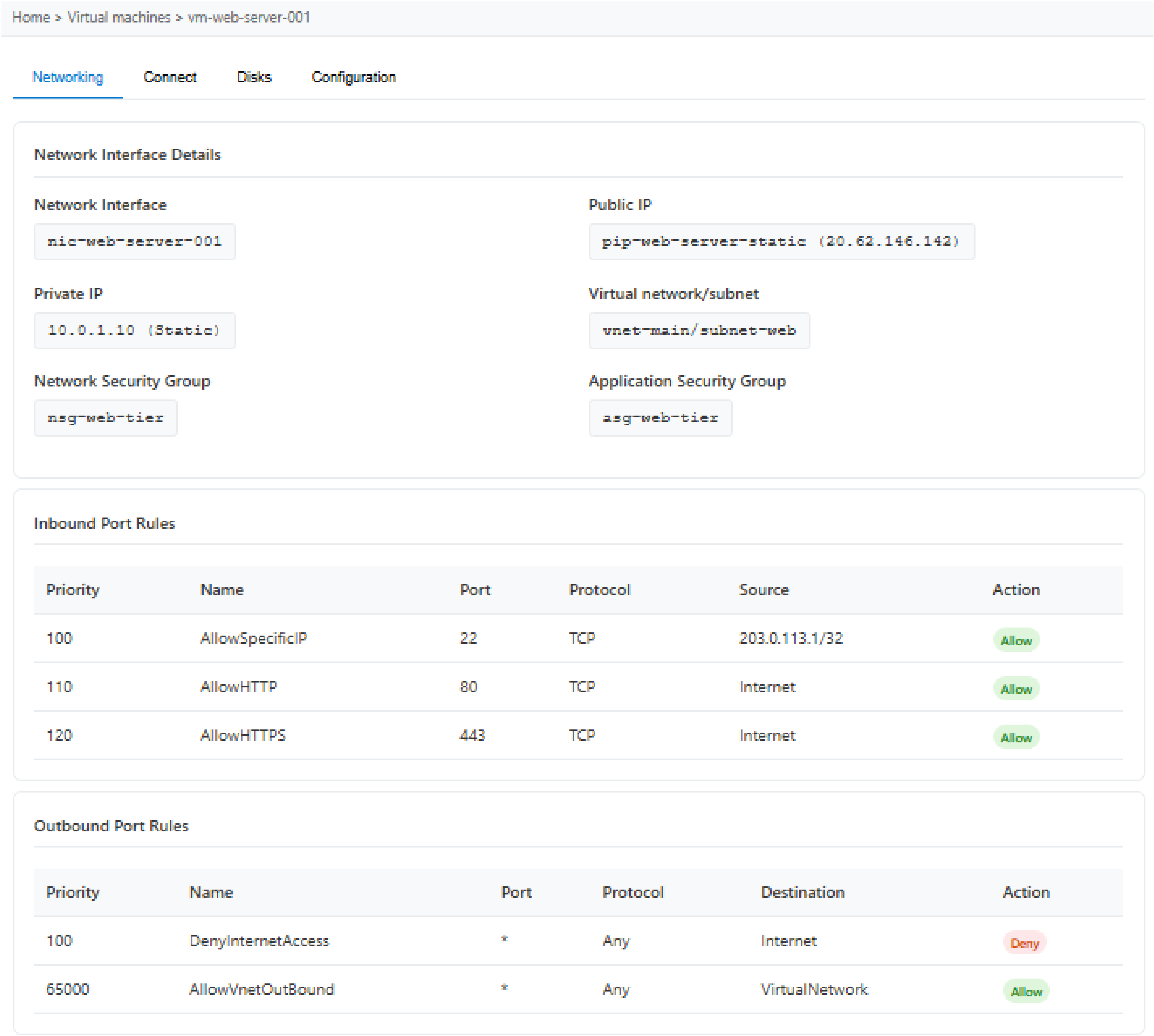
Figure 13 - Public IP Address



Name	Status	Location	Public IP	Private IP	Virtual network/subnet	Size
vm-web-server-001	Running	East US	20.62.146.142	10.0.1.10	vnet-main/subnet-web	Standard_B2s
vm-web-server-002	Running	East US	20.62.146.143	10.0.1.11	vnet-main/subnet-web	Standard_B2s
vm-app-server-001	Running	East US	20.62.146.144	10.0.2.10	vnet-main/subnet-app	Standard_B2s
vm-db-server-001	Running	East US	20.62.146.145	10.0.3.10	vnet-main/subnet-db	Standard_B2s

All VMs configured with static IPs: Both public and private IP addresses are statically assigned to ensure consistent connectivity.

Figure 14 - Virtual machines



Network Interface Details

Network Interface: `nic-web-server-001`

Public IP: `pip-web-server-static (20.62.146.142)`

Private IP: `10.0.1.10 (Static)`

Virtual network/subnet: `vnet-main/subnet-web`

Network Security Group: `nsg-web-tier`

Application Security Group: `asg-web-tier`

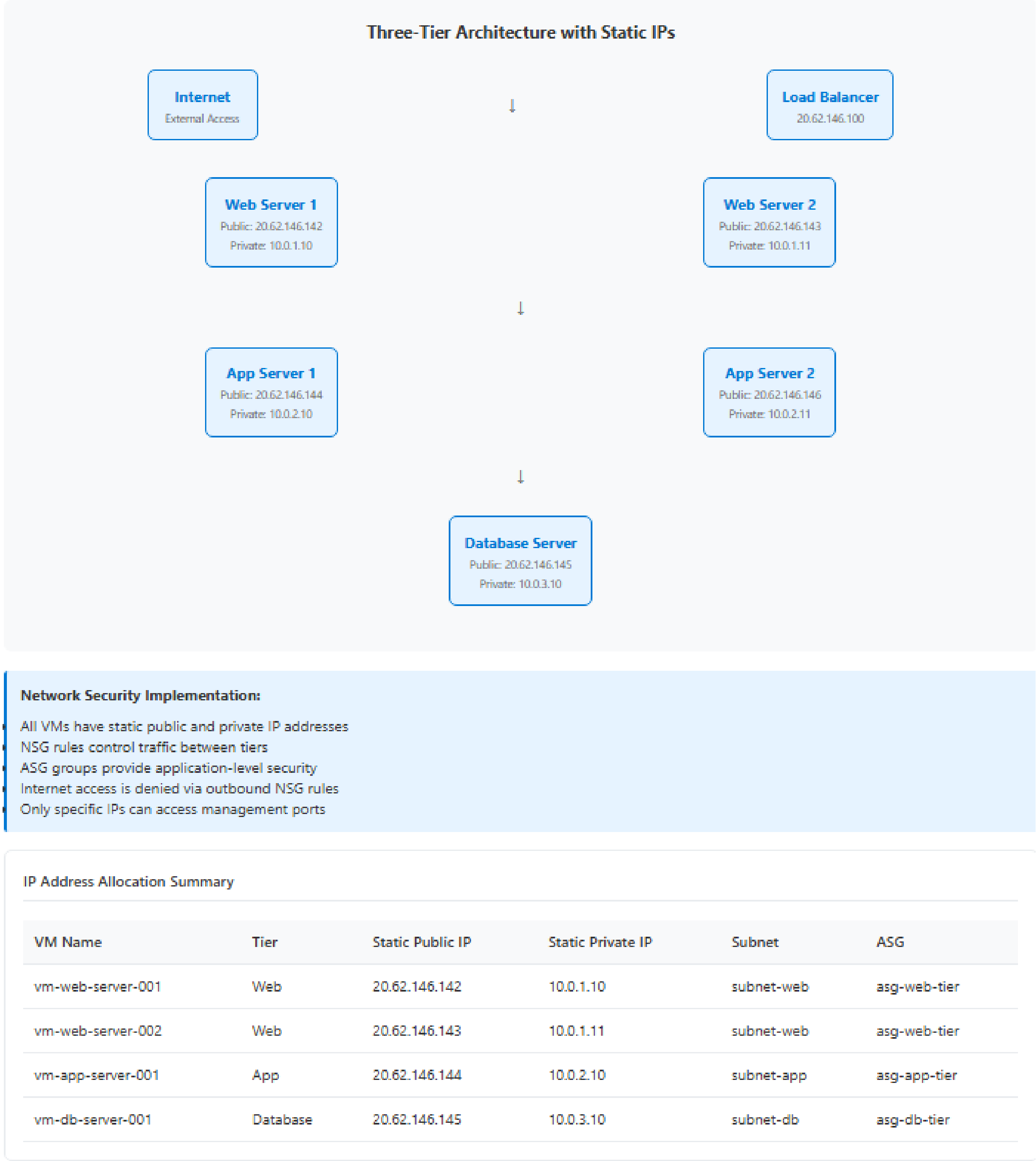
Inbound Port Rules

Priority	Name	Port	Protocol	Source	Action
100	AllowSpecificIP	22	TCP	203.0.113.1/32	Allow
110	AllowHTTP	80	TCP	Internet	Allow
120	AllowHTTPS	443	TCP	Internet	Allow

Outbound Port Rules

Priority	Name	Port	Protocol	Destination	Action
100	DenyInternetAccess	*	Any	Internet	Deny
65000	AllowVnetOutBound	*	Any	VirtualNetwork	Allow

Figure 15 - vm-web-server-001 – Networking



Network Security Implementation:

- All VMs have static public and private IP addresses
- NSG rules control traffic between tiers
- ASG groups provide application-level security
- Internet access is denied via outbound NSG rules
- Only specific IPs can access management ports

IP Address Allocation Summary

VM Name	Tier	Static Public IP	Static Private IP	Subnet	ASG
vm-web-server-001	Web	20.62.146.142	10.0.1.10	subnet-web	asg-web-tier
vm-web-server-002	Web	20.62.146.143	10.0.1.11	subnet-web	asg-web-tier
vm-app-server-001	App	20.62.146.144	10.0.2.10	subnet-app	asg-app-tier
vm-db-server-001	Database	20.62.146.145	10.0.3.10	subnet-db	asg-db-tier

*Figure 16 - **Network Architecture Overview***