

# Cloud Computing Lab 04

## Vivek Kumar 2280166

Microsoft Azure portal interface showing the configuration of Outbound security rules for the myNSGSecure network security group. The left sidebar displays the navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings, Inbound security rules, Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring, Automation, and Help.

The main content area displays the Outbound security rules table. The rules are evaluated by priority, source, destination, destination port, and protocol. The table shows three rules:

Priority	Name	Port	Protocol	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Deny

The 'Add outbound security rule' dialog is open on the right, showing the configuration for a new rule. The rule is named 'myNSGSecure'. The source is set to 'Any'. The destination is set to 'Service Tag'. The destination service tag is set to 'Internet'. The service is set to 'Custom'. The destination port ranges are set to '8080'. The protocol is set to 'Any'. The action is set to 'Deny'. The priority is set to '4096'.

Microsoft Azure portal interface showing the configuration of Inbound security rules for the myNSGSecure network security group. The left sidebar displays the navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings, Inbound security rules, Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring, Automation, and Help.

The main content area displays the Inbound security rules table. The rules are evaluated by priority, source, destination, destination port, and protocol. The table shows three rules:

Priority	Name	Port	Protocol	Destination	Action
65000	AllowVnetInbound	Any	Any	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	Allow
65500	DenyAllInbound	Any	Any	Any	Deny

The 'Add inbound security rule' dialog is open on the right, showing the configuration for a new rule. The rule is named 'myNSGSecure'. The source is set to 'Any'. The destination is set to 'Any'. The service is set to 'Custom'. The destination port ranges are set to '80,443'. The protocol is set to 'Any'. The action is set to 'Allow'. The priority is set to '100'. The name is set to 'AllowA30'. The description is set to 'AllowA30'.

Microsoft Azure

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

Copilot

kumaravivek22@gmail.c...  
DEFAULT DIRECTORY: SUMANAV...

Home > myNSGSecure

myNSGSecure | Subnets

Network security group

Search

Associate

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets**
- Properties
- Locks

Monitoring

Automation

Help

Search subnets

Name	Address range	Virtual network
SharedServicesSubnet	10.20.10.0/24	CoreServiceVnet

Give feedback

Microsoft Azure

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

Copilot

kumaravivek22@gmail.c...  
DEFAULT DIRECTORY: SUMANAV...

Home >

CreateApplicationSecurityGroupBladeViewModel | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

✓ Your deployment is complete

Deployment name : CreateApplicationSecurityGroupBladeViewModel  
Subscription : Azure subscription 1  
Resource group : az104-rg4

Start time : 12/9/2025, 6:24:09 PM  
Correlation ID : f9fa6dcb-bd6d-4528-8067-821a3be528f

Deployment details

Next steps

Go to resource

Give feedback

Tell us about your experience with deployment

Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill.  
Set up cost alerts >

Microsoft Defender for Cloud

Secure your apps and infrastructure  
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

Start learning today >

Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.  
Find an Azure expert >

Add or remove filters by pressing Ctrl+V (1/1 of 1)

Microsoft Azure

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

Copilot

kumaravivek22@gmail.c...  
DEFAULT DIRECTORY kumaraviv...

Home > Network foundation > Virtual networks >

Create virtual network

Validation passed

BasicsSecurityIP addressesTagsReview + create

View automation template

Basics

Subscription

Azure subscription 1

Resource Group

az104-rg4

Name

CoreServicesVnet

Region

West US 2

Security

Azure Bastion

Disabled

Azure Firewall

Disabled

Azure DDoS Network Protection

Disabled

IP addresses

Address space

10.20.0.0/16 (65,536 addresses)

Subnet

default (10.20.0.0/24) (256 addresses)

Subnet

SharedServicesSubnet (10.20.10.0/24) (256 addresses)

Subnet

DatabaseSubnet (10.20.20.0/24) (256 addresses)

Tags

PreviousNextCreateDownload a template for automationGive feedback

Microsoft Azure

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

Copilot

kumaravivek22@gmail.c...  
DEFAULT DIRECTORY kumaraviv...

Home > az104-rg4 > CoreServicesVnet

CoreServicesVnet | Export template

Virtual network

DownloadCopy contentDeployFeedback

ARM TemplateBicepTerraform

Include parameters

TemplateParameters

To export all resources in this resource group, navigate to the "Export template" experience under "Automation" on the left menu of the resource group.

1 Generating template.....

Parameters (0)  
Variables (0)  
Resources (0)

Cloud  
Network manager  
DNS  
Peerings  
Service endpoints  
Private endpoints  
Properties  
Locks  
Monitoring  
Alerts  
Metrics  
Diagnostic settings  
Logs  
Virtual network flow logs  
Topology  
Automation  
CU / PS  
Tasks  
Export template  
Help  
Connection troubleshooting  
Support