

Branden Solomon
5/7/25
Professor Francis
CTEC 475

Capstone Module 6

1. Create two VPCs with one subnet each, either in the same cloud platform or in two different cloud platforms. (Your instructor might require that you use the same cloud platform for this project or two cloud platforms—check with your instructor for specific requirements.) Make sure both subnets have access to the Internet. For example, in AWS, you’ll need to add an Internet gateway to each subnet and add an Internet route to each subnet’s route table.

The screenshot displays the Microsoft Azure portal interface for creating and configuring a virtual network. The top navigation bar includes the Microsoft Azure logo, a search bar, and a Copilot button. The user's profile, SOLOMONB0509@stud..., is visible in the top right corner.

Create virtual network

The 'Create virtual network' page shows the 'IP addresses' tab selected. It provides instructions on configuring the virtual network address space with IPv4 and IPv6 addresses and subnets. A table lists the subnets:

Subnets	IP address range	Size	NAT gateway
default	192.16.0.0 - 192.16.0.255	/24 (256 addresses)	-

Below the table, there is a warning message: "The entered IPv4 address range may not work correctly. It is recommended to use an address range that is not globally routable, such as 172.16.0.0/12, or a range defined in RFC 1918 and RFC 6598." The 'Review + create' button is highlighted.

Edit subnet

The 'Edit subnet' page allows for customizing a default subnet. The 'Subnet purpose' is set to 'Default'. The 'Name' is 'Web-VNet'. The 'IPv4' section is checked, and the 'IPv4 address range' is '192.16.0.0/24'. The 'Starting address' is '192.16.0.0', and the 'Size' is '/24 (256 addresses)'. The 'Subnet address range' is '192.16.0.0 - 192.16.0.255'. The 'IPv6' section is unchecked. The 'Private subnet' section is unchecked. The 'Security' section is unchecked. The 'NAT gateway' is set to 'None'. The 'Save' button is highlighted.

Create virtual network

The 'Create virtual network' page shows the 'Review + create' tab selected. It provides a summary of the virtual network configuration:

- Basics**
 - Subscription: Azure for Students
 - Resource Group: Web-VNet
 - Name: Web-VNet
 - Region: East US
- Security**
 - Azure Bastion: Disabled
 - Azure Firewall: Disabled
 - Azure DDoS Network Protection: Disabled
- IP addresses**
 - Address space: 192.16.0.0/24 (256 addresses)
 - Subnet: Web-VNet (192.16.0.0/24) (256 addresses)
- Tags**

The 'Create' button is highlighted.

Microsoft Azure

Home > Virtual networks >

Create virtual network

Basics Security **IP addresses** Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

+ Add a subnet

192.16.1.0/24
192.16.1.0 - 192.16.1.255
256 addresses

Delete address space

Subnets	IP address range	Size	NAT gateway
default	192.16.1.0 - 192.16.1.255	/24 (256 addresses)	-

Add IPv4 address space

The entered IPv4 address range may not work correctly. It is recommended to use an address range that is not globally routable, such as 172.16.0.0/12, or a range defined in RFC 1918 and RFC 6598. [Learn more](#)

Previous Next **Review + create**

Edit subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose

Name

IPv4

Include an IPv4 address space ☒

IPv4 address range
192.16.1.0 - 192.16.1.255

Starting address

Size

Subnet address range

IPv6

Include an IPv6 address space ☐ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default outbound access) ☐

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more](#)

NAT gateway
[Create new](#)

Save Cancel [Give feedback](#)

Microsoft Azure

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags **Review + create**

[View automation template](#)

Basics

Subscription	Azure for Students
Resource Group	DB-VNet
Name	DB-VNet
Region	East US

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	192.16.1.0/24 (256 addresses)
Subnet	DB-VNet (192.16.1.0/24) (256 addresses)

Tags

Previous Next **Create** [Give feedback](#)

2. Create a VM instance in each subnet. Make sure each VM receives a public IP address. What public IP address is assigned to your VMs?

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

SOLOMON80509@stud...
BOMBE STATE

Home > Web-VNet | Network settings > web-vnet57_z1

web-vnet57_z1 | IP configurations

Network interface

Search

Refresh

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Settings

IP configurations

DNS servers

Network security group

Properties

Locks

Monitoring

Automation

Help

IP Settings

Enable IP forwarding

Virtual network: Web-VNet

Gateway load balancer

Subnet *

Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. [Learn more](#)

+ Add

Make primary

Delete

Name	IP Version	Type	Private IP Address	Public IP Address
<input checked="" type="checkbox"/> ipconfig1	IPv4	Primary	192.16.0.4 (Dynamic)	52.224.242.242 (Web-VNet-ip)

Apply

Discard changes

Give feedback

Add or remove favorites by pressing Ctrl+Shift+F

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

SOLOMON80509@stud...
BOMBE STATE

Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Help me create a low cost VM

Help me create a VM optimized for high availability

Help me choose the right VM size for my workload

Basics

Disks

Networking

Management

Monitoring

Advanced

Tags

Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *

Subnet *

Public IP

NIC network security group

Public inbound ports *

Select inbound ports *

None

Basic

Advanced

None

Allow selected ports

SSH (22)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is deleted

< Previous

Next: Management >

Review + create

Give feedback

Microsoft Azure

Home > DB-VNet

DB-VNet | Network settings

Virtual machine

Search resources, services, and docs (G+)

Copilot

SOLOMON80509@stud... BOWNE STATE

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Connect

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Availability + scale

Security

Backup + disaster recovery

Operations

Monitoring

Automation

Help

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

List all my network interfaces for DB-VNet. What are the requirements for attaching or detaching a network interface? How can I make my virtual machine secure?

Attach network interface Detach network interface View topology Troubleshoot Refresh Give feedback

Network interface / IP configuration

db-vnet583_z1 (primary) / ipconfig1 (primary)

Essentials

Network interface : db-vnet583_z1

Virtual network / subnet : DB-VNet / DB-VNet

Public IP address : 74.235.96.97

Private IP address : 192.16.14

Admin security rules : 0 (Configure)

Load balancers : 0 (Configure)

Application security groups : 0 (Configure)

Network security group : DB-VNet-nsg

Accelerated networking : Enabled

Effective security rules : 0

Rules

Network security group DB-VNet-nsg (attached to networkinterface: db-vnet583_z1)

Impacts 0 subnets, 1 network interfaces

Search rules

Source == all Destination == all Protocol == all Action == all

Priority 1 Name Port Protocol Source Destination Action

Inbound port rules (4)

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
65000	AllowVNetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow

https://portal.azure.com/?Microsoft_Azure_Education_correlationId=c3f699c4-7df8-4b7d-8c42-4e5528cafa47#@studentsbowstate.onmicrosoft.com/resource/subscriptions/0904767-abe7-4415-a691-ac73987dc6a8/resourceGroups/DB-VNet/providers/Microsoft.Compute/virtualMachines/DB-VNet/networkSettings

3. Configure security rules that allow ICMP traffic from any source to your target VM so you can confirm the target VM will respond successfully to pings. Get a working ping from your local computer to your target VM before proceeding.

Microsoft Azure

Home > Network security groups >

Network security group...

Bovine State

+ Create Manage view ...

Filter for any field...

Name ↑

- DB-VNet-nsg
- Web-VNet-nsg

Web-VNet-nsg

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
- Alerts
- Diagnostic settings
- Logs
- NSG flow logs
- Automation
- Help

Essentials

Resource group (move) : Web-VNet

Location : East US

Subscription (move) : Azure for Students

Subscription ID : 09047b7-a8e7-44f5-a691-ac73987dca9

Tags (edit) : Add tags

Custom security rules : 2 inbound, 1 outbound

Associated with : 0 subnets, 1 network interfaces

JSON View

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
Inbound Security Rules						
300	SSH	22	TCP	Any	Any	allow
330	AllowAnyCustomAnyIn...	Any	ICMP	Any	Any	allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
320	AllowAnyCustomAnyOutbo...	Any	ICMP	Any	Any	allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Page 1 of 1

Add or remove priorities by pressing Ctrl+Shift+P

Microsoft Azure

Home > Network security groups >

Network security g...

Bovine State

+ Create Manage view ...

Filter for any field...

Name ↑

- DB-VNet-nsg
- Web-VNet-nsg

DB-VNet-nsg

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
- Alerts
- Diagnostic settings
- Logs
- NSG flow logs
- Automation
- Help

Essentials

Resource group (move) : DB-VNet

Location : East US

Subscription (move) : Azure for Students

Subscription ID : 09047b7-a8e7-44f5-a691-ac73987dca9

Tags (edit) : Add tags

Custom security rules : 2 inbound, 1 outbound

Associated with : 0 subnets, 1 network interfaces

JSON View

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
Inbound Security Rules						
300	SSH	22	TCP	Any	Any	allow
310	AllowAnyCustomAnyIn...	Any	ICMP	Any	Any	allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
320	AllowAnyCustomAnyOutbo...	Any	ICMP	Any	Any	allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Page 1 of 1

Add or remove priorities by pressing Ctrl+Shift+P

4. Configure security rules that allow SSH or RDP connections to your source VM. Remote into the source VM.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Network security groups > DB-VNet-nsg

Network security group | DB-VNet-nsg | Inbound security rules

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 | Alerts | Diagnostic settings | Logs | NSG flow logs | Automation | Help

Filter for any field...

DB-VNet-nsg

Web-VNet-nsg

Created security rule
Successfully created security rule 'Allow-RDP'.

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name | Port == all | Protocol == all | Source == all | Destination == all | Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
310	AllowAnyCustomAnyIn...	Any	ICMP	Any	Any	Allow
330	Allow-SSH	22	TCP	Any	Any	Allow
340	Allow-RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

Page 1 of 1

Add or remove favorites by pressing Ctrl+Shift+F

Microsoft Azure | Search resources, services, and docs (G+)

Home > Network security groups > Web-VNet-nsg

Network security group | Web-VNet-nsg | Inbound security rules

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 | Alerts | Diagnostic settings | Logs | NSG flow logs | Automation | Help

Filter for any field...

DB-VNet-nsg

Web-VNet-nsg

Created security rule
Successfully created security rule 'Allow-RDP'.

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name | Port == all | Protocol == all | Source == all | Destination == all | Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
330	AllowAnyCustomAnyIn...	Any	ICMP	Any	Any	Allow
340	Allow-SSH	22	TCP	Any	Any	Allow
350	Allow-RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

Page 1 of 1

Add or remove favorites by pressing Ctrl+Shift+F

5. Configure security rules that only allow ICMP traffic from your source VM to your target VM. What rules did you add? What effect do you expect each rule to have on traffic to and from each VM?

Microsoft Azure

Home > Network security groups > DB-VNet-nsg

Network security group DB-VNet-nsg

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

Alerts

Diagnostic settings

Logs

NSG flow logs

Automation

Help

Page 1 of 1

Add or remove favorites by pressing Ctrl+Shift+F

DB-VNet-nsg | Inbound security rules

Search

+ Add Hide default rules Refresh Delete Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
330	Allow-SSH	22	TCP	Any	Any	Allow
340	Allow-RDP	3389	TCP	Any	Any	Allow
350	Allow-Web-VM	Any	ICMP	71.127.41.163	192.16.1.0	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Microsoft Azure

Home > Network security groups > Web-VNet-nsg

Network security group Web-VNet-nsg

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

Alerts

Diagnostic settings

Logs

NSG flow logs

Automation

Help

Page 1 of 1

Add or remove favorites by pressing Ctrl+Shift+F

Web-VNet-nsg | Inbound security rules

Search

+ Add Hide default rules Refresh Delete Give feedback

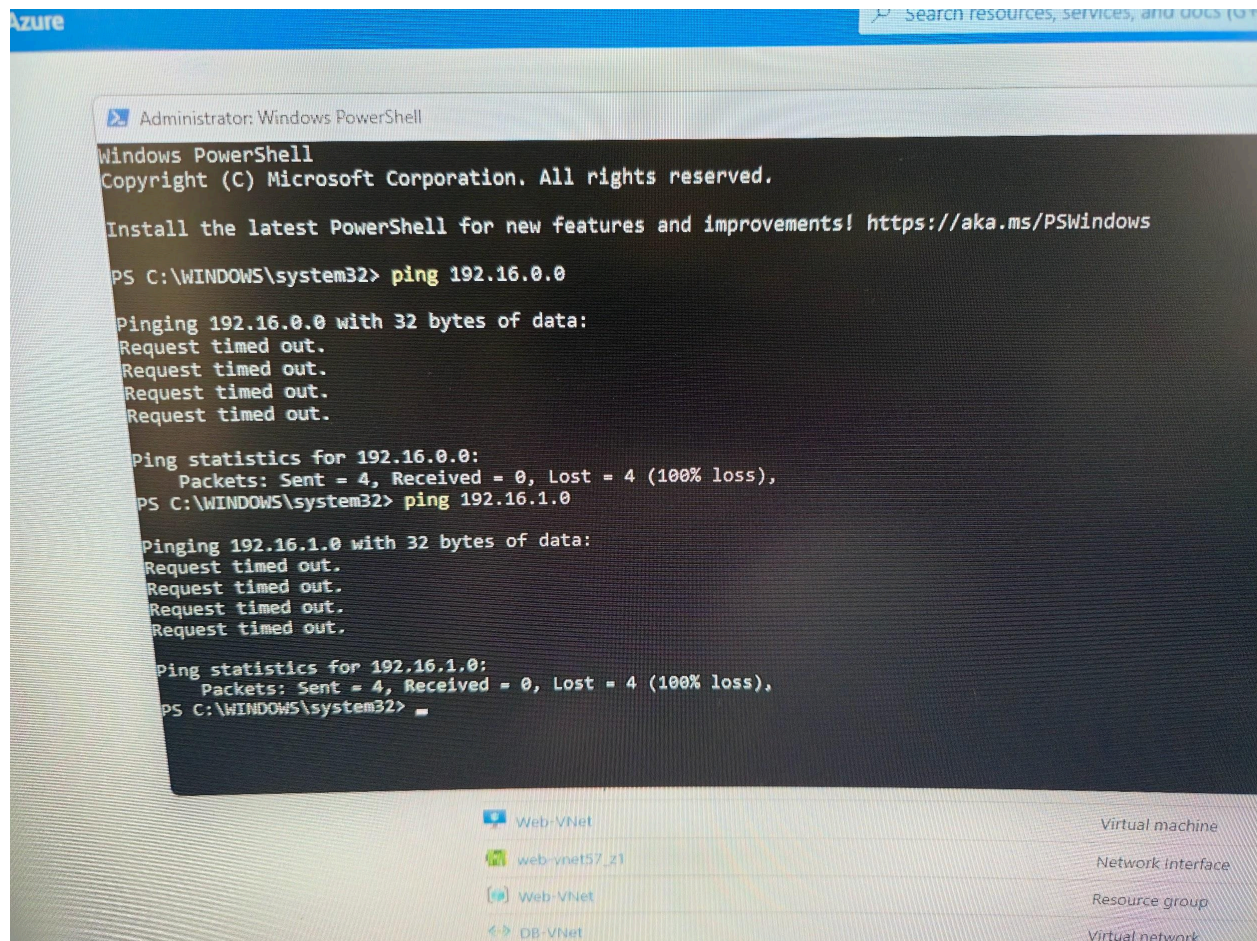
Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

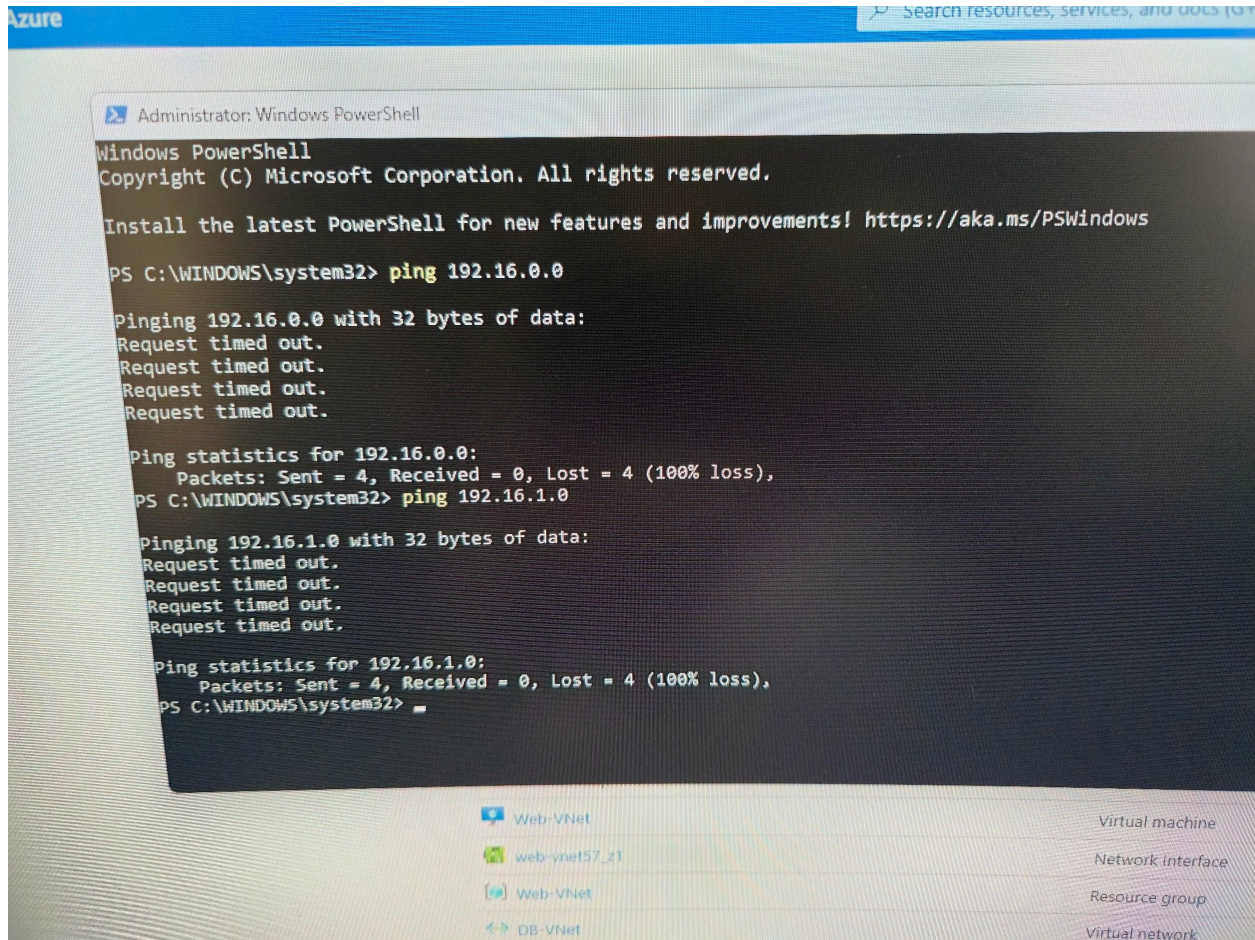
Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
340	Allow-SSH	22	TCP	Any	Any	Allow
350	Allow-RDP	3389	TCP	Any	Any	Allow
360	Allow-DB-VM	Any	ICMP	71.127.41.163	192.16.1.0	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Updated security rule
Successfully saved security rule 'Allow-DB-VM'.

6. Run a ping from the source VM to the target VM that shows ICMP traffic is reaching the target VM. Take a screenshot showing the output; include this visual with your answers to this project's questions.



7. Run a ping from your local computer to your target VM that shows ICMP traffic from other sources cannot reach the target VM. Take a screenshot showing the output; include this visual with your answers to this project's questions.



8. Delete all resources created in this Capstone project. Check through your account to confirm that all related resources have been deleted.

