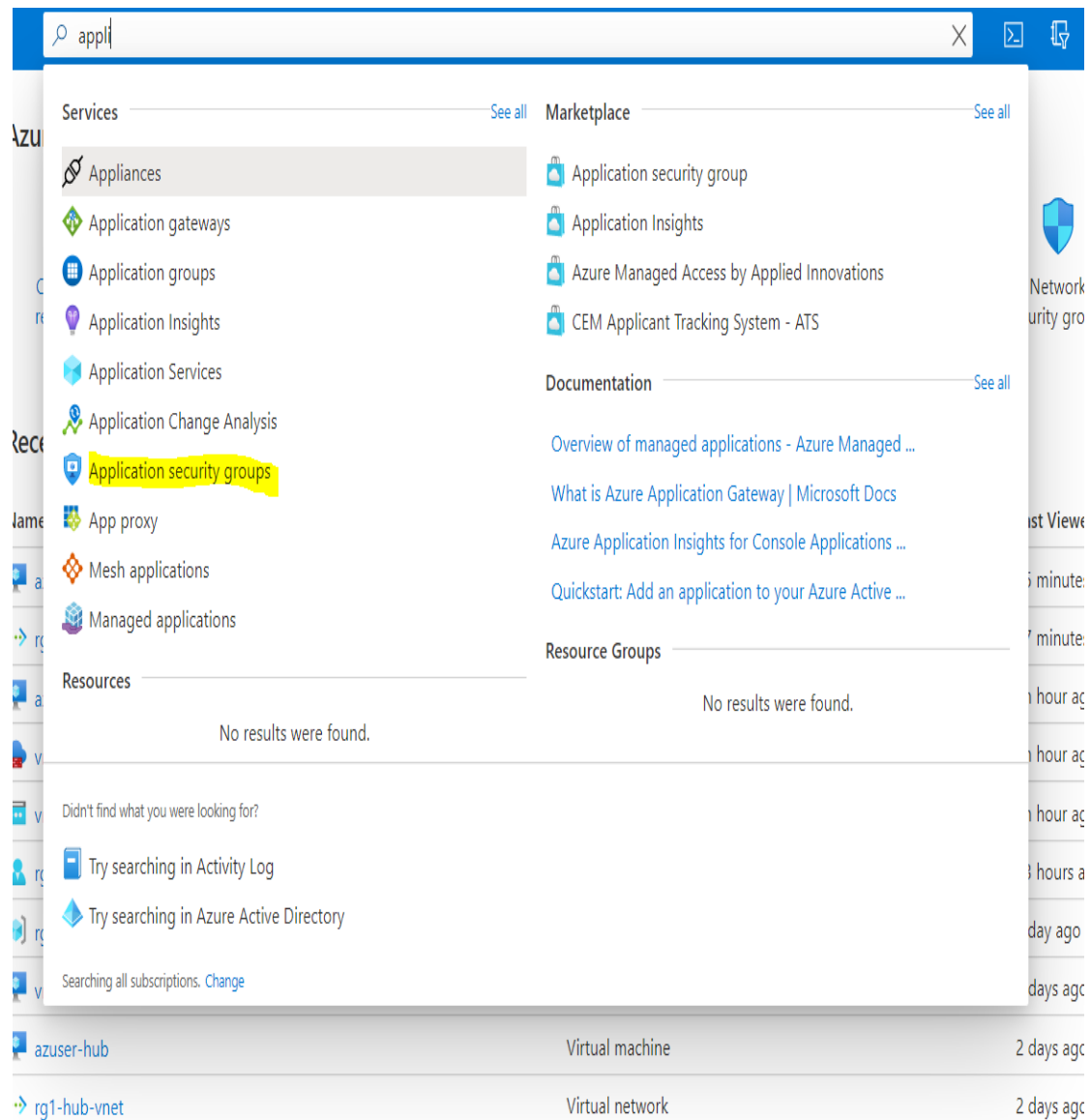




CREATING APPLICATION SECURITY GROUPS

Go to -> Search -> Application Security Group -> Create



- Resource group : Rg1
- Name : mgmt1
- Region : East US
- Follow same and create another ASG with Name : web1

REST ALL LEAVE AS DEFAULTS AND CLICK REVIEW & CREATE.

 mgmt	Application security group	rg1	East US	Free Trial
 web	Application security group	rg1	East US	Free Trial

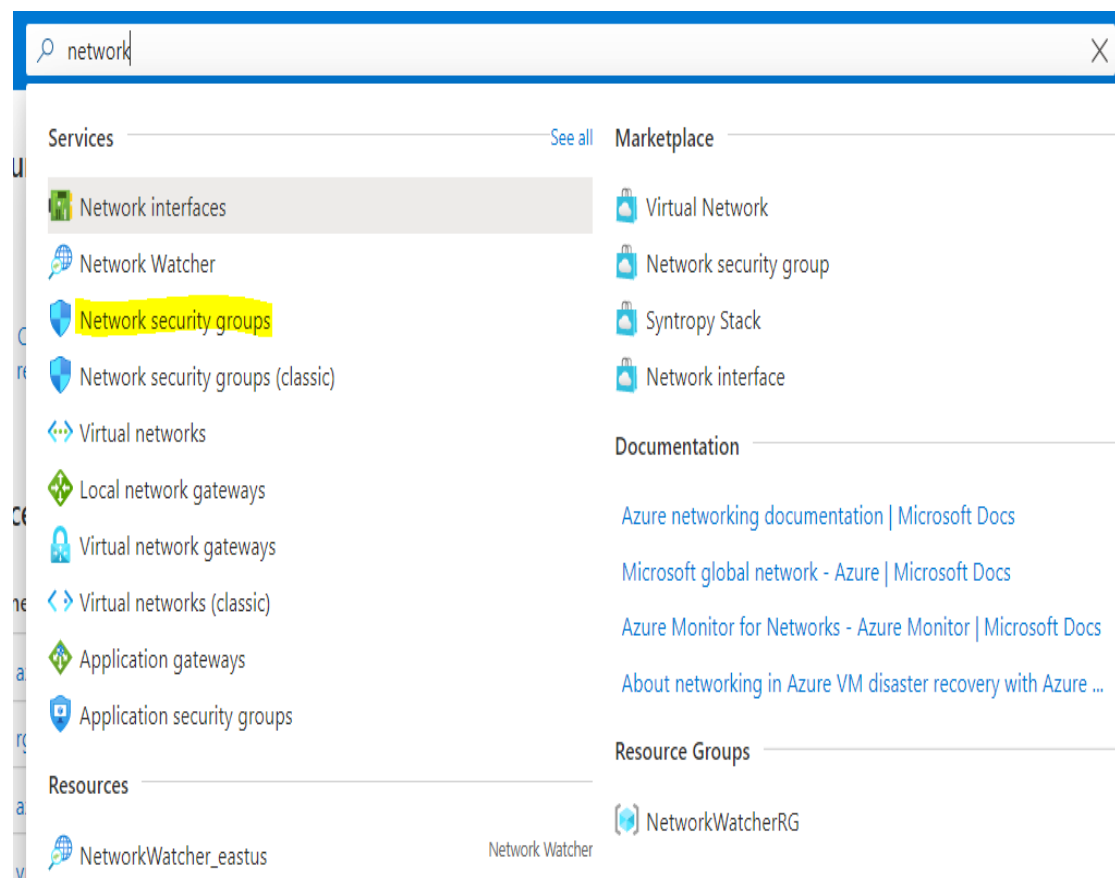
After creating ASGs,

Goto -> rg1-vm1-mgmt1 -> Networking -> Application Security Groups -> Configure the application security groups -> Select mgmt1 -> Save

Repeat same for rg1-vm1-web1 configuring with web1 ASG.

CREATING NETWORK SECURITY GROUPS

Go to -> Search -> Network Security Group -> Create



- Resource group : rg1
- Name : nsg1
- Region : East US

REST ALL LEAVE AS DEFAULTS AND CLICK REVIEW & CREATE.



After creating NSGs

Goto -> az-user-mgmt1-nsg -> inbound security rules -> add

- Source : Any
- Source port ranges : *
- Destination : Any
- Destination port ranges : 22,3389
- Protocol : TCP
- Action : Allow
- Priority : 300
- Name : allow ssh
- Repeat the same and create another NSG with Name : az-user-web-nsg

REST ALL LEAVE AS DEFAULTS AND CLICK SAVE.

The screenshot shows the 'Inbound security rules' page for the 'az-user-mgmt1-nsg' network security group. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Settings. The 'Inbound security rules' link is selected. The main area displays a table of rules with columns: Priority, Name, Port, Protocol, Source, and Destination. The rules are as follows:

Priority	Name	Port	Protocol	Source	Destination
300	SSH	22,3389	TCP	Any	Any
320	HTTP	80	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

The screenshot shows the 'Inbound security rules' page for the 'az-user-web-nsg' network security group. The layout is identical to the previous screenshot, showing the same set of inbound security rules for this NSG.

Priority	Name	Port	Protocol	Source	Destination
300	SSH	22,3389	TCP	Any	Any
320	HTTP	80	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

Now,

Goto -> Subnets in nsg1 -> Associate -> Select Rg1-vnet1-subnet1 -> Save

Goto -> Subnets in nsg1 -> Associate -> Select Rg1-vnet1-subnet2 -> Save

CREATING VNET PEERING

Now, we'll create another VM as using below details.

- Resource group - rg1
- Virtual Machine name: rg1-hub
- Region : East US
- Availability options : No infrastructure redundancy required.
- Image : Keep Default, i.e. Ubuntu server 18.04 LTS - Gen1
- Size : Standard_B1s
- Authentication Type: Password
- Username : azuser-hub
- Password : 16 character password of your choice.
- Select inbound ports: SSH, RDP
- Virtual network : Rg1-hub-vnet
- Subnet : Rg1-hub-subnet1

REST ALL LEAVE AS DEFAULTS AND CLICK REVIEW & CREATE.

Now, we'll create another VM as using below details.

- Resource group - rg1
- Virtual Machine name: rg1-vm2
- Region : East US
- Availability options : No infrastructure redundancy required.
- Image : Keep Default, i.e. Ubuntu server 18.04 LTS - Gen1
- Size : Standard_B1s
- Authentication Type: Password
- Username : azuser-vm2
- Password : 16 character password of your choice.
- Select inbound ports: SSH, RDP
- Virtual network : Rg1-vnet2
- Subnet : Rg1-vnet2-subnet1

REST ALL LEAVE AS DEFAULTS AND CLICK REVIEW & CREATE.

After creating VMs,

Goto -> rg1-vnet1 -> Peerings -> add

- Peering link name : peer-vnet1-to-hub
- Remote virtual network : peer-hub-to-vnet1
- Virtual network : Rg1-vnet1

Goto -> rg1-vnet2 -> Peerings -> add

- Peering link name : peer-vnet2-to-hub
- Remote virtual network : peer-hub-to-vnet2
- Virtual network : Rg1-vnet2

You can check the peering status in Peerings as Connected.

rg1-vnet1 | Peerings

Virtual network

Search (Ctrl+/)

+ Add Refresh

Filter by name...

Name	Peering status	Peer	Gateway transit
peer-vnet1-to-hub	Connected	rg1-hub-vnet	Disabled

rg1-vnet2 | Peerings

Virtual network

Search (Ctrl+/)

+ Add Refresh

Filter by name...

Name	Peering status	Peer	Gateway transit
peer-vnet2-to-hub	Connected	rg1-hub-vnet	Disabled

Another way to check Peering status is by

Goto -> rg1-user-mgmt1 (VM) -> Networking -> Network Interface -> Effective Routes -> Next Hop Type mentioned as Vnet Peering.

az-user-mgmt1351 | Effective routes

Network interface

Search (Ctrl+/) « Download Refresh

Showing only top 200 records, click Download above to see all.

Scope: Network interface (az-user-mgmt1351)

Associated route table: rg1-route1

Effective routes

Source	↑↓	State	↑↓	Address Prefixes	↑↓	Next Hop Type	↑↓	Next Hop Type IP Address	↑↓	User Defined Route Name	↑↓
Default		Active		10.0.0.0/16		Virtual network		-		-	
Default		Active		10.1.0.0/16		VNet peering		-		-	
Default		Invalid		0.0.0.0/0		Internet		-		-	
User		Active		0.0.0.0/0		Virtual appliance		10.1.1.4		rg1-firewall1	

Home > Virtual machines > vnet2-vm1 > vnet2-vm1375

vnet2-vm1375 | Effective routes

Network interface

Search (Ctrl+/) « Download Refresh

Showing only top 200 records, click Download above to see all.

Scope: Network interface (vnet2-vm1375)

Associated route table: -

Effective routes

Source	↑↓	State	↑↓	Address Prefixes	↑↓	Next Hop Type	↑↓	Next Hop Type IP Address	↑↓	User Defined Route Name	↑↓
Default		Active		10.2.0.0/16		Virtual network		-		-	
Default		Active		10.1.0.0/16		VNet peering		-		-	
Default		Active		0.0.0.0/0		Internet		-		-	

Now login to rg1-user-mgmt1 and ping rg1-hub public ip (ping successful).

Now login to rg1-vm2 and ping rg1-hub public ip (ping successful).