

## **FIREWALL:**

- while creating vnet enable firewall in security =created vnet
- create a new vm and default subnet
- inbound port rules :none
- public ip: none
- create
- resourcegrp->firewall u created-> private ip=note public and private ip

## **nsg rules are statefull:**

- when u make an inbound connection,default allow outbound connection
- when u make 80,response is ok
- somebody can come frm the door,and ok to go back
- incoming req allowed,response?(ok if stateful)

## **firewall rules are not stateful:**

outbound is required in stateless

## **search route table:**

- create +
  - ur routetable->settings->subnets->associate
  - **route**->ip address->0.0.0.0/0->virtual appliance->next hop address=prv ip of firewall
  - next hop address = **priv ip of firewall**
  - rule:allow to respond to whom
  - create a default route of 0.0.0.0/0 -so anyone can?
- 
- this is at vnet level

## **Added route:**

### Add route

abhiroutetable

Route name \*

Destination type \*

Destination IP addresses/CIDR ranges \*

Next hop type \*

Next hop address \*

**Info** Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

**Add** [Give feedback](#)

go to firewall->settings->rules->application rule collection->add

### Adding application rule : change it to 10.0.0.0/24

### Add application rule collection

Name \*

Priority \*

Action \*

Rules

FQDN tags

name	Source type	Source	FQDN tags
<input type="text"/>	<input type="text" value="IP address"/>	<input type="text" value="*, 192.168.10.1, 192.168.10.0/24, 192.1..."/>	<input type="text" value="0 selected"/>

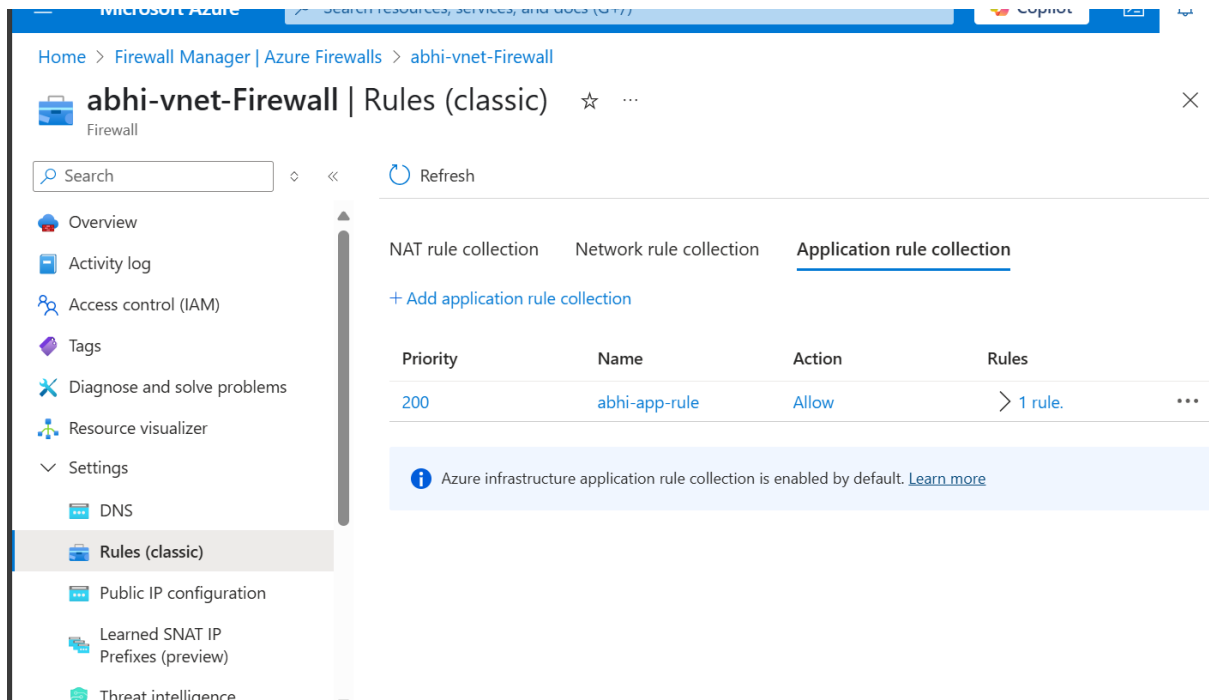
**Info** FQDN tags may require additional configuration. [Learn more](#)

Target FQDNs

name	Source type	Source	Protocol:Port	Target FQDNs
<input type="text" value="allowgoogle"/>	<input type="text" value="IP address"/>	<input type="text" value="10.0.2.0/24"/>	<input type="text" value="https"/>	<input type="text" value="www.google.com"/>

**Add**

**Created:**



Added network rule: worked(subnet range also should be same)

### Add network rule collection

Name \*  ✓

Priority \*  ✓

Action \*  ✓

Rules

IP Addresses

	Protocol	Source type	Source	Destination type	Destination Addr...	Destination
✓	UDP	IP address	10.0.0.0/24 ✓	IP address	209.244.0.3,209.2... ✓	53
	0 selected	IP address	*, 192.168.10.1, 192...	IP address	*, 192.168.10.1, 192...	8080, 8080-

Service Tags

name	Protocol	Source type	Source	Service Tags	Destination Por
	0 selected	IP address	*, 192.168.10.1, 192...	0 selected	8080, 8080-809

create network rule:

10.0.0.0/24:source =the subnet range and this should be same

209.244.0.3,209.244.0.4:destination=dns

53=destination Port

Add

### NAT rule:

translated address:10.0.0.4(private ip of vm)

Protocol:TCP

source:\*

Destination Addr:4.213.32.56(public ip of firewall)

Destination Ports:22

Translated address:10.0.0.4(priv ip of vm)

Translated port:22

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

Copilot

### Add NAT rule collection

Name \* abhi-natrul ✓

Priority \* 300 ✓

Action Destination Network Address Translation (DNAT) ▾

Rules

	Source type	Source	Destination Addr...	Destination Ports	Translated address	Translated port
▾	IP address ▾	* ✓	4.213.32.56 ✓	22 ✓	10.0.1.4 ✓	22
▾	IP address ▾	*, 192.168.10.1, 192... ✓	192.168.10.0	8080	192.168.10.0	8080

Add

### Notifications

More events in...

- ✓ Success  
Successfully updated Firewall'
- ✓ Success  
Successfully updated Firewall'
- ! Failed to update Firewall'  
Failed to update Firewall'. Error: Error retrieving status: https://management.azure.com/subscriptions/e819-49ca-b6-69c32a235312/resourceGroups/285c-44c4-a.../providers/Microsoft.Network/firewalls/285c-44c4-a.../version=2022-01-01

try to connect to public ip of firewall:

```
ssh -i abhi-vm_key\ (2).pem azureuser@4.213.32.56 =worked
```

try to curl inside vm:

```
curl https://www.google.com =worked
```