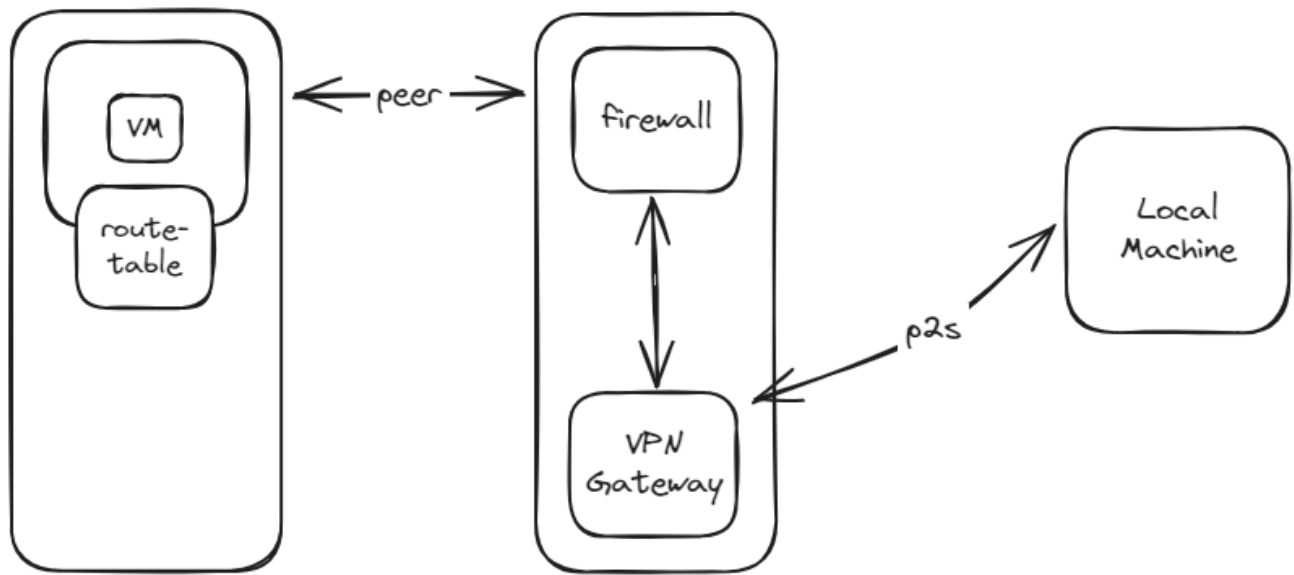


Firewalls documentation

Table of contents

- [LAB](#)
 - [Do's](#)
 - [AD Authentication to connect Local machine](#)
 - [vm](#)
 - [firewall](#)
 - [VPN](#)
 - [Resource Visualizer](#)
 - [firewall](#)
 - [DNAT](#)
 - [Network Rules](#)
 - [Routes](#)
 - [Route table at <u>VM subnet</u>](#)
 - [Communications](#)
 - [VM to Local Machine](#)
 - [Local Machine to VM through Firewall](#)
-

LAB



[arc-firewall-lab-architecture](#)

Do's

- ping through firewall.
 - Route table is associated to VM subnet
 - A P2S VPN is established to the VPN gateway subnet of Vnet.
-

AD Authentication to connect Local machine

AD authentication

- *Tenant* -

```
https://login.microsoftonline.com/30bf9f37-d550-4878-9494-1041656caf27/
```

- *Audience* -

```
41b23e61-6c1e-4545-b367-cd054e0ed4b4
```

- *Issuer* -

```
https://sts.windows.net/30bf9f37-d550-4878-9494-1041656caf27/
```

vm

vm username - Datha

vm password - Donotshare@vm

vm public ip - 172.203.249.54 (disassociated)

vm private ip - 10.0.1.4

firewall

private ip - 10.0.2.4

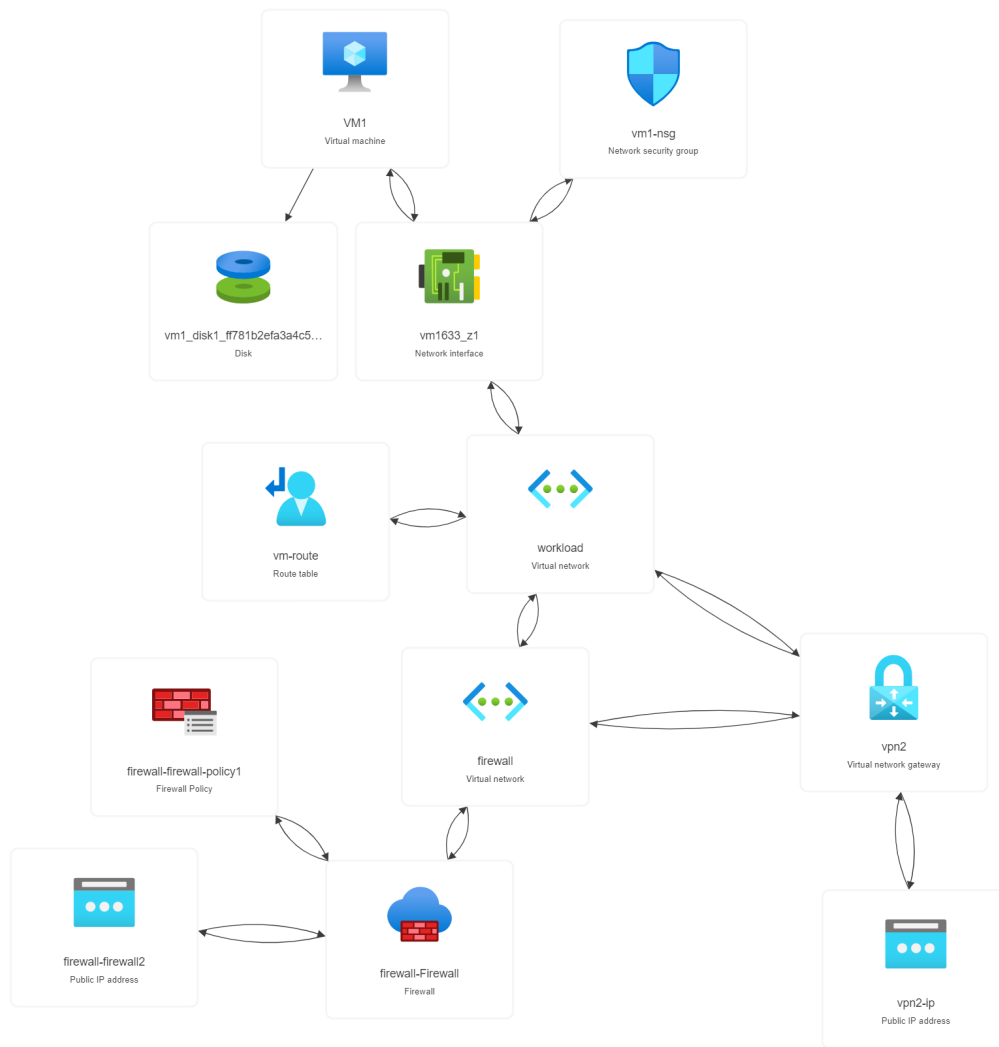
public ip - 20.124.209.186

VPN

address pool - 192.168.1.0/24

local machine ip allocated - 192.168.1.2

Resource Visualizer

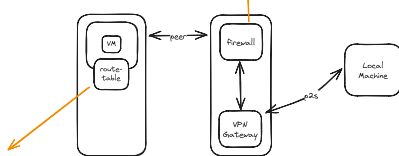


firewall-policy

firewall-firewall-policy1 | DNAT rules

Rules are shown in the order of evaluation. Rules are evaluated in order of priority. Within the same rule collection type, rules are evaluated in order of priority. Rules are evaluated in order of priority.

Rule Collection ID	Rule Collection Name	Rule Name	Source	Port	Protocol	Destination	Translated Address	Translated Port	Action	Matched from
10	collection 1	rule 1	10.0.0.0/0	8080	TCP	10.0.0.0/0	10.0.0.0	8080	DNAT	rule 1



Destination type * ☐ IP Addresses

Destination IP addresses/CIDR ranges * ☐ 0.0.0.0/0

Next hop type * ☐ Virtual appliance

Next hop address * ☐ 10.0.2.4

- 1) RDP
- 2) ping success on both side
- 3) SNAT rules
- 4) NAT rules

firewall

DNAT

olicy1 | DNAT rules ☆ ...

+ Add a rule collection + Add rule Edit Delete

Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.

Search to filter items...

Rule Collection Priority	Rule collection name	Rule name	Source	Port	Protocol	Destination	Translated Address or FQDN	Translated Port	Action	Inherited from
Rule Collection Group: DefaultDnatRuleCollectionGroup with priority 100.										
110	collection-1	rule-1	192.168.1.2	3389	TCP	10.0.2.4	10.0.1.4	3389	Dnat	***

Network Rules

mail-tirewall-policy1

policy1 | Network rules ☆ ...

« + Add a rule collection + Add rule Edit Delete

Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.

Search to filter items...

Rule Collection Pri...	Rule collection na...	Rule name	Source	Port	Protocol	Destination	Action	Inherited from
Rule Collection Group: DefaultDnatRuleCollectionGroup with priority 100.								
120	network-collection-1	rule-1	10.0.1.4	*	Any,TCP,UDP,ICMP	192.168.1.2	Allow	***
120	network-collection-1	rule-2	192.168.1.2	*	TCP,ICMP,UDP,Any	10.0.1.4	Allow	***

Routes

Route table at VM_subnet

Destination type * ⓘ

IP Addresses

Destination IP addresses/CIDR ranges * ⓘ

0.0.0.0/0

Next hop type * ⓘ

Virtual appliance

Next hop address * ⓘ

10.0.2.4

Communications

VM to Local Machine

```
C:\Users\Datha>hostname
vm1

C:\Users\Datha>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=277ms TTL=128
Reply from 192.168.1.2: bytes=32 time=502ms TTL=128
Reply from 192.168.1.2: bytes=32 time=414ms TTL=128
Reply from 192.168.1.2: bytes=32 time=411ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 277ms, Maximum = 502ms, Average = 401ms
```

Local Machine to VM through Firewall

```
C:\Users\DathaSaiChandu>ping 10.0.1.4

Pinging 10.0.1.4 with 32 bytes of data:
Reply from 10.0.1.4: bytes=32 time=252ms TTL=128
Reply from 10.0.1.4: bytes=32 time=238ms TTL=128
Reply from 10.0.1.4: bytes=32 time=358ms TTL=128
Reply from 10.0.1.4: bytes=32 time=273ms TTL=128

Ping statistics for 10.0.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 238ms, Maximum = 358ms, Average = 280ms

C:\Users\DathaSaiChandu>hostname
SNP-HYD-LPT-083
```
