

firewall

create the RG and deployed

2 vnets

each has 1 subnet default

hubvnet has firewallGW subnet

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the 'Workspace 1' tab and the 'network_task - Microsoft Azure' title. The main content area displays the 'network_task' resource group. The 'Resources' tab is selected, showing a list of resources. The list includes:

Name	Type	Location
FW1	Firewall	East US
FWip	Public IP address	East US
hubvnet	Virtual network	East US
policyFW	Firewall Policy	East US
vm1	Virtual machine	East US
vm1-ip	Public IP address	East US
vm1-nsa	Network security group	East US

The interface also shows a search bar, a left-hand navigation menu with options like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Resource visualizer', 'Events', 'Settings', 'Deployments', 'Security', 'Deployment stacks', 'Policies', 'Properties', 'Locks', and 'Cost Management'. The bottom status bar displays the temperature (26°C), weather (Mostly cloudy), and the date (06-12-2023).

created Firewall

The screenshot displays the Microsoft Azure portal interface. The left sidebar shows the navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Settings, Public IP configuration, Learned SNAT IP Prefixes (preview), Firewall Manager, Properties, Locks, Monitoring, Metrics, Diagnostic settings, and Logs. The main content area shows the 'FW1 Firewall' overview page. The 'Essentials' section lists various properties: Resource group (network_task), Location (East US), Subscription (ARCHIT JAIN - MPN), Subscription ID (f2825f7a-c276-40b0-b8a1-bac639219628), Virtual network (hubvnet), Firewall policy (policyFW), and Provisioning state (Succeeded). The 'Firewall policy' section indicates that the policy is 'policyFW' and 'Auto-learn IP Prefixes' are 'Disabled'. The 'Rules' section is partially visible at the bottom.

Firewall policy

1. DNAT rule

The screenshot shows the 'hubnet-firewall-policy | DNAT rules' configuration page in the Microsoft Azure portal. The left sidebar is expanded to show 'DNAT rules' under the 'Settings' section. The main content area displays a table of DNAT rules. The table has columns for Rule Collection P., Rule collection n..., Rule name, Source, Port, Protocol, Destination, and Translated Address. A single rule is listed with the following details:

Rule Collection P.	Rule collection n...	Rule name	Source	Port	Protocol	Destination	Translated Address
101	dnat	L2VM	20.20.20.0/24	3389	UDP,TCP	157.56.182.111	10.1.0.4

2. Network Rule

Workspace 1 hubnet-firewall-policy - Microsoft Azure

https://portal.azure.com/#@snp.com/resource/subscriptions/f2825f7a-c276-40b0-b8a1-... Search resources, services, and docs (G+)

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

Home > hubnet-firewall-policy

hubnet-firewall-policy | Network rules

Firewall Policy

Search

+ 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 P...	Rule collection n...	Rule name	Source	Port	Protocol	Destination	Action
Rule Collection Group: DefaultNetworkRuleCollectionGroup with priority 200.							
<input type="checkbox"/>	102	netrule	netrul1-L2VM	10.20.20.2	*	Any	10.1.0.4 Allow
<input type="checkbox"/>	102	netrule	netrule2-vm2L	10.1.0.4	*	Any	10.20.20.2 Allow

30°C Haze Search ENG IN 15:57 13-12-2023

Workspace 1 vpnGW - Microsoft Azure

https://portal.azure.com/#@snp.com/resource/subscriptions/f2825f7a-c276-40b0-b8a1-bac639... Search resources, services, and docs (G+)

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

Home > vpnGW

vpnGW | Point-to-site configuration

Virtual network gateway

Search

Save Discard Delete Download VPN client

Address pool

20.20.20.0/24

Tunnel type

OpenVPN (SSL)

Authentication type

Azure Active Directory

Azure Active Directory

Tenant *

https://login.microsoftonline.com/30bf9f37-d550-4878-9...

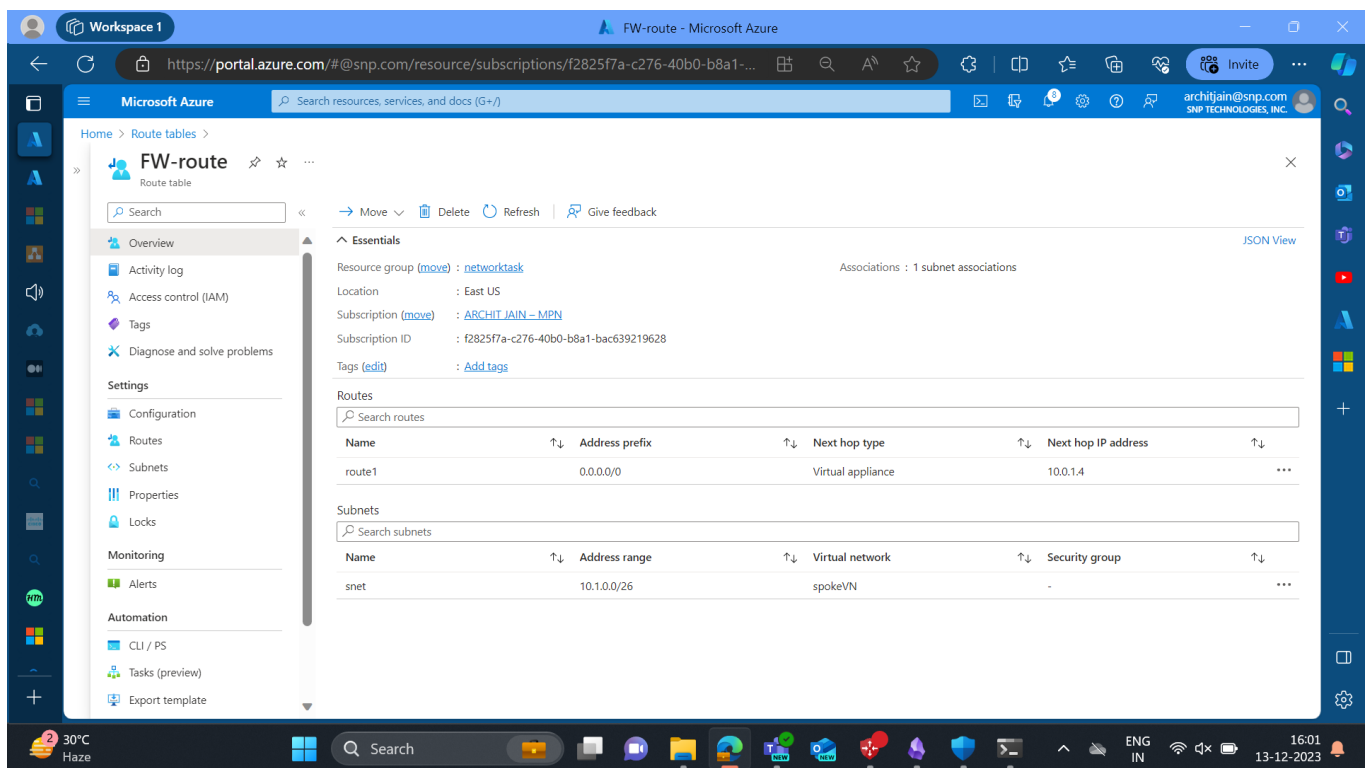
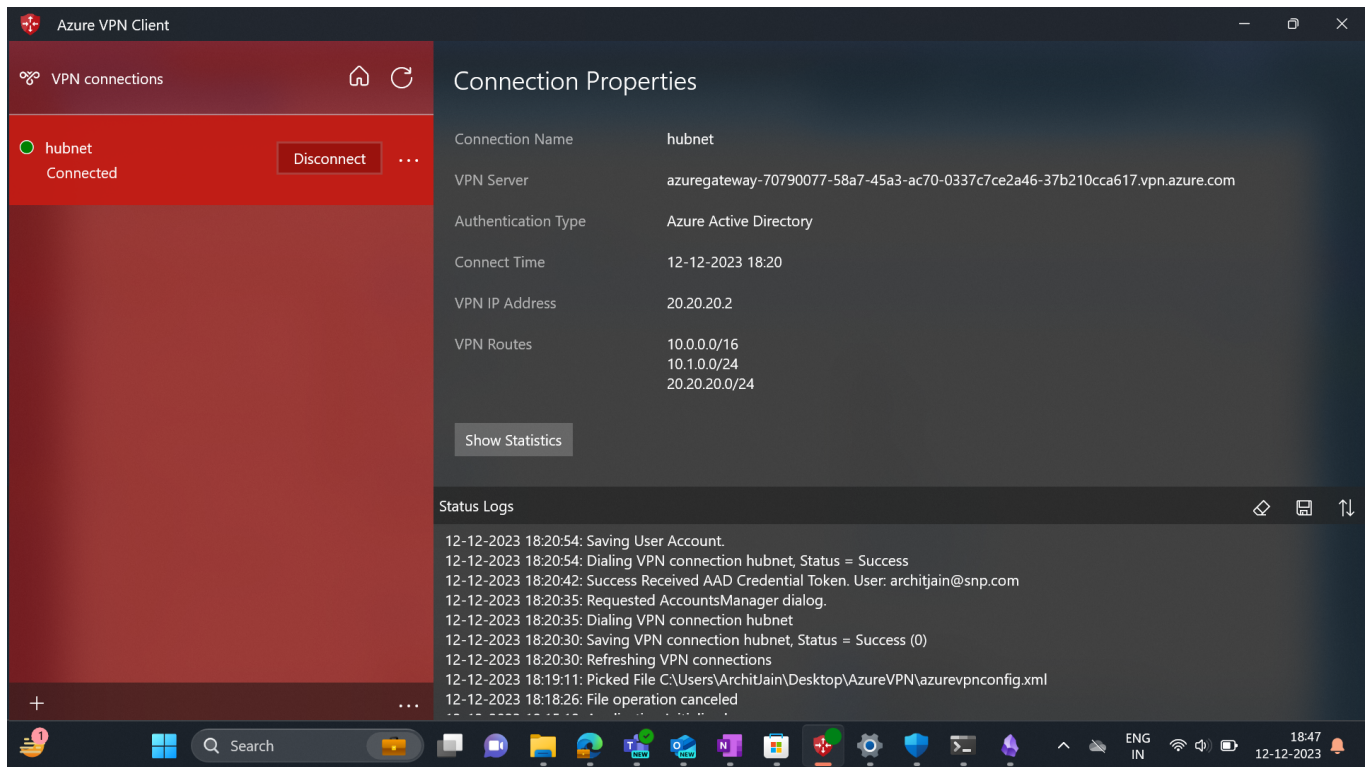
Audience *

41b23e61-6c1e-4545-b367-cd054e0ed4b4

Issuer *

https://sts.windows.net/30bf9f37-d550-4878-9494-1041...

18:48 12-12-2023



results

1. local to VM

```
Workspace 1 hubnet-firewall-policy - Microsoft Azure
Command Prompt
Connection-specific DNS Suffix . : 
IPv4 Address. . . . . : 20.20.20.2
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

C:\Users\ArchitJain>ping 10.1.0.4

Pinging 10.1.0.4 with 32 bytes of data:
Reply from 10.1.0.4: bytes=32 time=323ms TTL=128
Reply from 10.1.0.4: bytes=32 time=346ms TTL=128
Reply from 10.1.0.4: bytes=32 time=355ms TTL=128
Reply from 10.1.0.4: bytes=32 time=268ms TTL=128

Ping statistics for 10.1.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 268ms, Maximum = 355ms, Average = 323ms

C:\Users\ArchitJain>
```

2. vm to local

```
Workspace 1 hubnet-firewall-policy - Microsoft Azure
10.1.0.4 - Remote Desktop Connection
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3693]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : 1a3imyjode1exevlv3iztbwsbe.bx.internal.cloudapp.net
Link-local IPv6 Address . . . . . : fe80::e81d:c36a:b3f9:270f%6
IPv4 Address. . . . . : 10.1.0.4
Subnet Mask . . . . . : 255.255.255.192
Default Gateway . . . . . : 10.1.0.1

C:\Windows\system32>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:
Reply from 20.20.20.2: bytes=32 time=316ms TTL=128
Reply from 20.20.20.2: bytes=32 time=558ms TTL=128
Reply from 20.20.20.2: bytes=32 time=376ms TTL=128
Reply from 20.20.20.2: bytes=32 time=250ms TTL=128

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 250ms, Maximum = 558ms, Average = 375ms

C:\Windows\system32>
```

