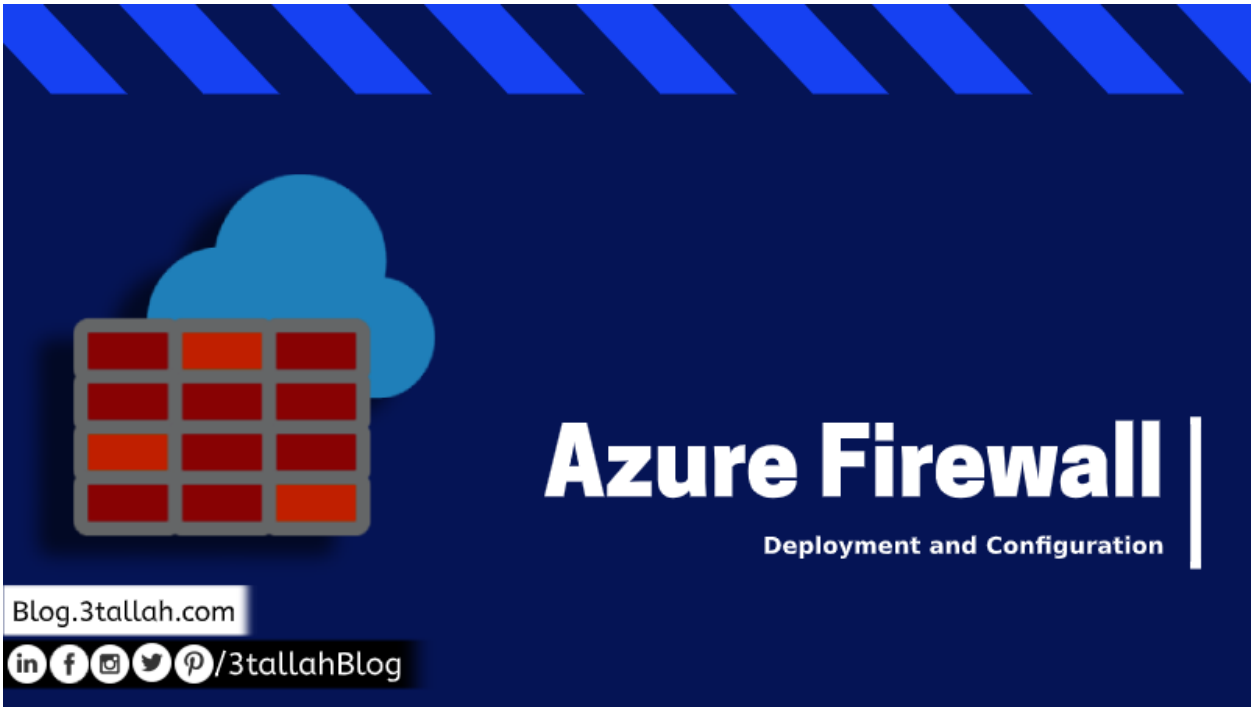
Azure Firewall Deployment



Contents

Step by Step: Deploy and configure Azure Firewall

Securing a network perimeter is one of the most important aspects for any organization, here in this blog we are going to demonstrate Azure Firewall deployment and basic configuration.

Before we start let's have a little brief about Azure Firewall and Its consideration.

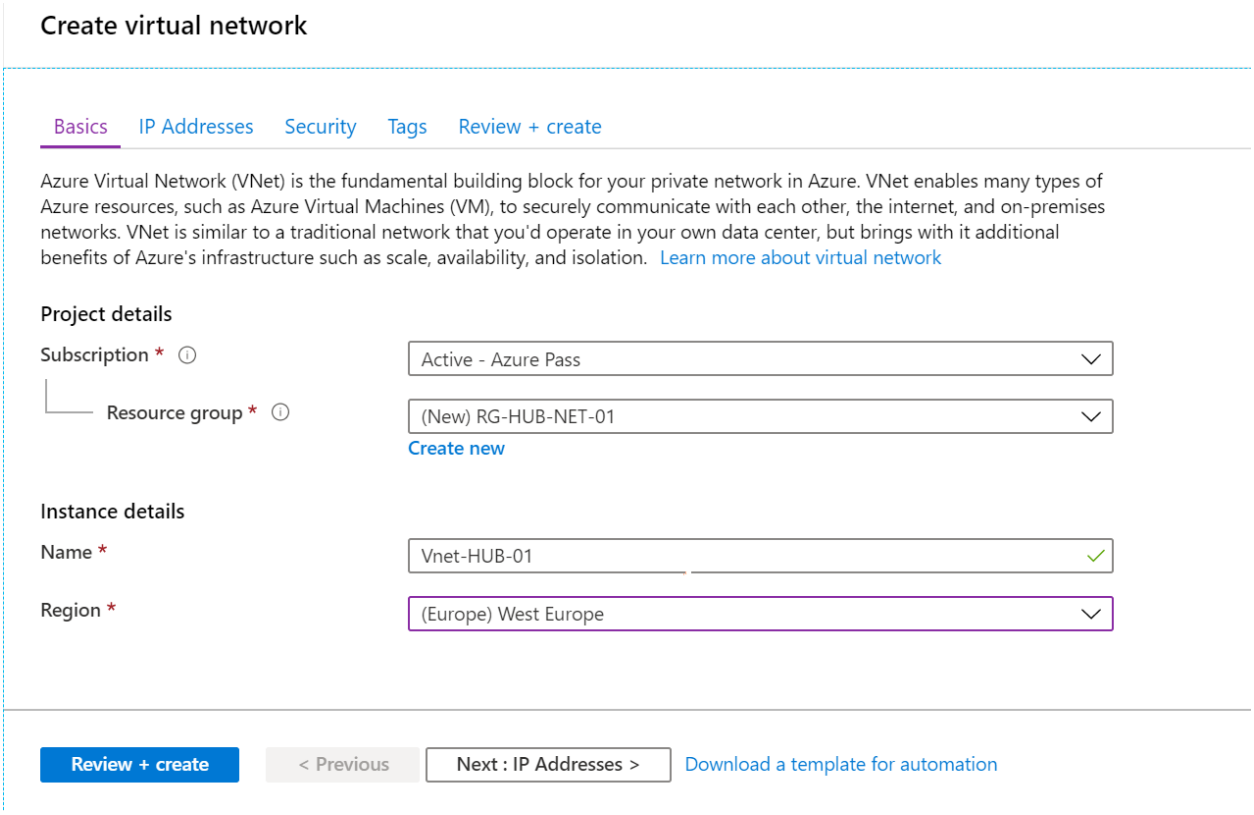
- Azure Firewall is stateful firewall as a Service with high availability integrated and unrestricted cloud scalability that protects Azure virtual network resources.
- You can deploy Azure Firewall on any virtual network, but customers typically deploy it on a central virtual network and peer other virtual networks to it in a **hub-and-spoke model.**
- Azure Firewall supports inbound and outbound filtering. Inbound protection is for non-HTTP/S protocols. For example, **RDP, SSH, and FTP** protocols.
- Azure Firewall needs a dedicated subnet "**AzureFirewallSubnet"**
- Azure Firewall is integrated with **Azure Monitor** for viewing and analyzing firewall logs.
- Azure Firewall supports rules and rule collections.
    - A rule collection is a set of rules that share the same order and priority.
    - Rule collections are executed in order of their priority.
    - Network rule collections are higher priority than application rule collections, and all rules are terminating.
- Azure Firewall cost:
    - Fixed fee: $1.25/firewall/hour,
    - Data Processing fee: $0.016 per GB processed by the firewall (ingress or egress)
    - A fixed hourly fee will be charged per a firewall deployment regardless of scale. In addition, data processing fee is billed per deployment for any date processed by your firewall.

In this post, you will learn step by step how to:

- Set up a network environment **(Vnets and SNets).**
- Deploy Azure Firewall
- Create a default route to route traffic through Azure firewall.
- Configure an application rule to allow access to www.3tallah.com
- Configure a network rule to allow access to Google DNS servers
- Create virtual machines for Test purpose.
- Create Azure Bastion to connect to Workload Servers
- Test the firewall

Set up the network

NOTE: Firewall and its Vnet should be in the same resource group.



Create virtual network

Basics | IP Addresses | Security | Tags | Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

172.17.128.0/23

Add IPv6 address space

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

Add subnet | Remove subnet

Subnet name	Subnet address range
AzureFirewallSubnet	172.17.128.128/26
SNet-HUB-MGMT	172.17.128.192/27

Review + create | < Previous | Next : Security > | Download a template for automation

Create virtual network

Validation passed

Basics | IP Addresses | Security | Tags | Review + create

Basics

Subscription	Active - Azure Pass
Resource group	(new) RG-HUB-NET-01
Name	Vnet-HUB-01
Region	West Europe

IP addresses

Address space	172.17.128.0/23
Subnet	AzureFirewallSubnet (172.17.128.128/26),SNet-HUB-MGMT (172.17.128.192/27)

Tags

None

Security

Create | < Previous | Next > | Download a template for automation

Deploy Azure Firewall

Firewall
Microsoft

Firewall Save for later
Microsoft

Create

Overview Plans

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subs Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your fully integrated with Azure Monitor for logging and analytics.

Create a firewall

Project details

Subscription *	Active - Azure Pass
Resource group *	RG-HUB-NET-01 Create new

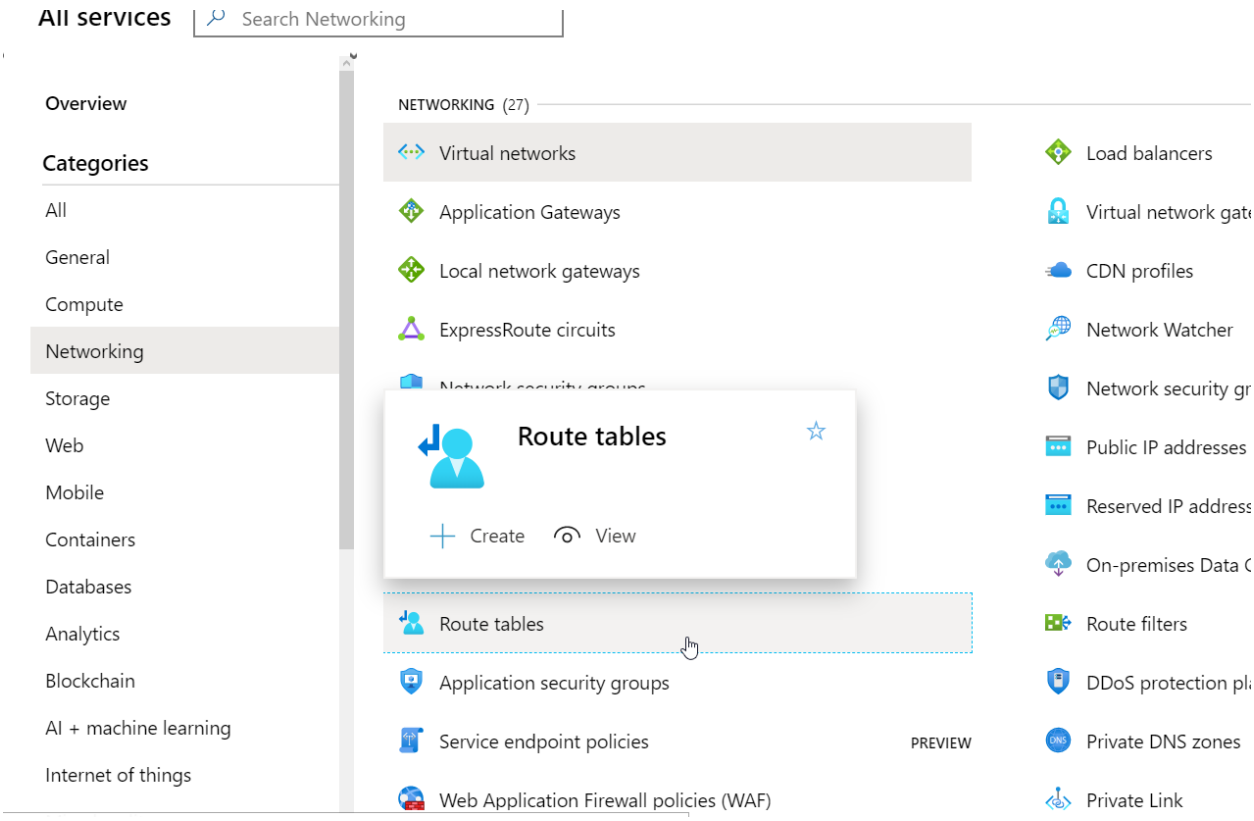
Instance details

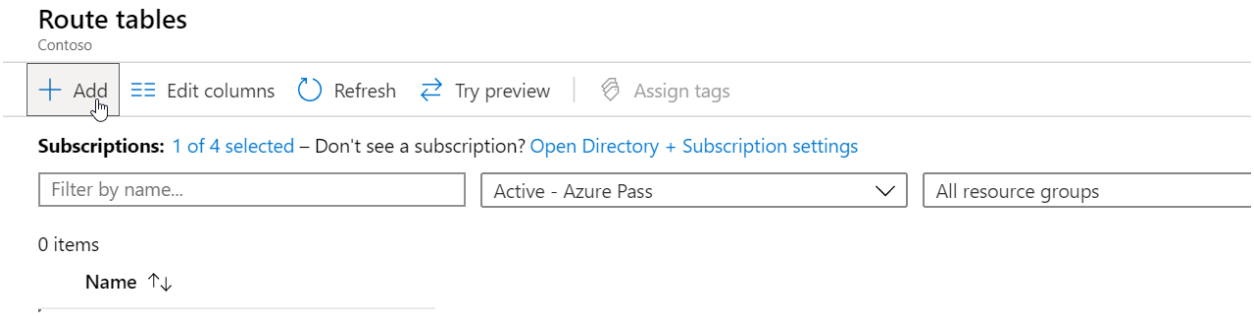
Name *	AzureFirewall
Region *	(Europe) West Europe
Availability zone	None
Choose a virtual network	Create new / Use existing
Virtual network	Vnet-HUB-01 (RG-HUB-NET-01)
Firewall public IP address *	(New) AzureFirewall-PIP01 Add new
Forced tunneling (preview)	Disabled

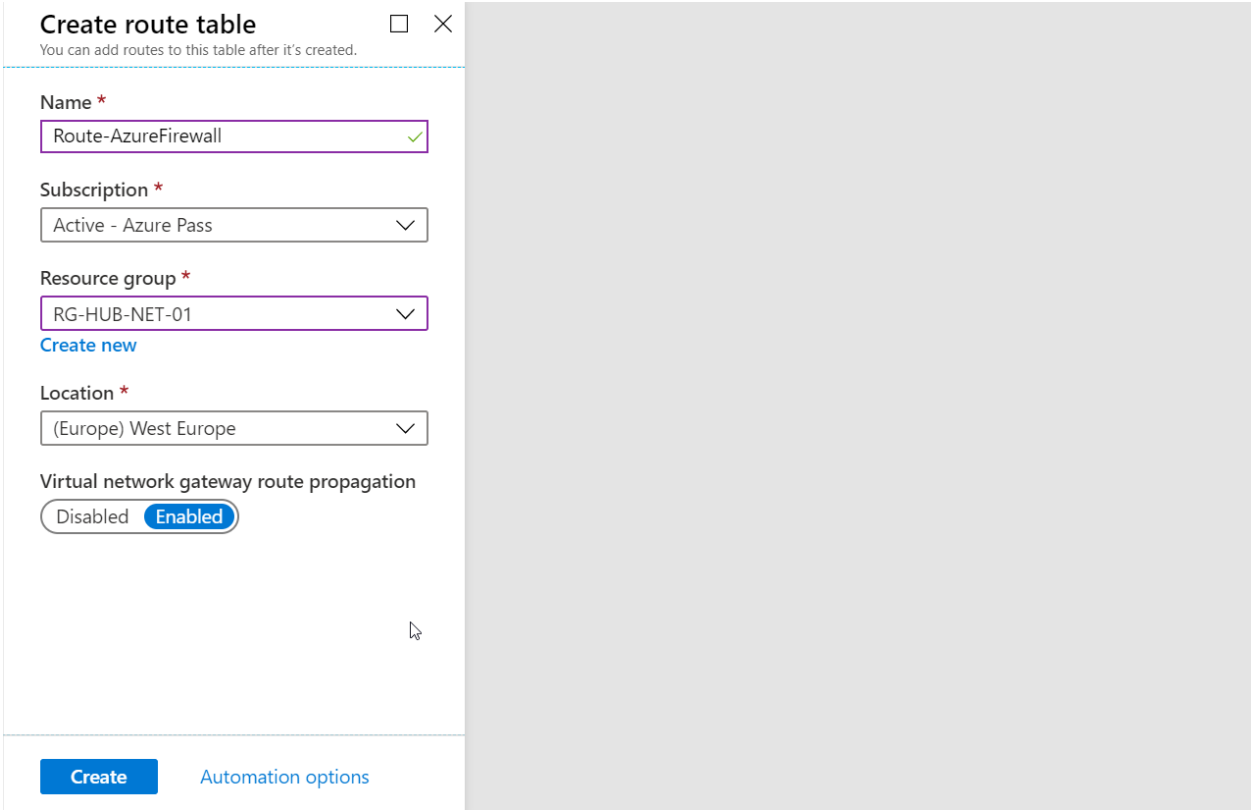
Review + create | Previous | Next : Tags > | Download a template for automation

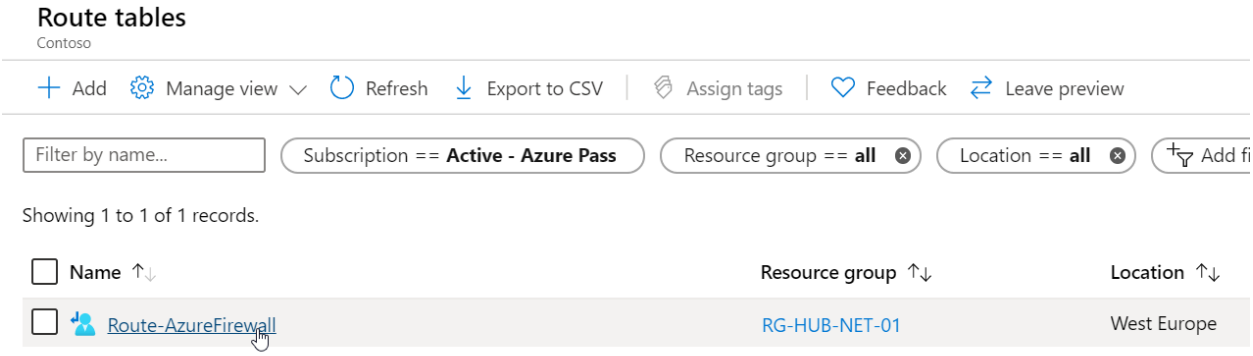
Create a default route

Configure the outbound default route to go through the firewall for **Servers Workload** subnet.

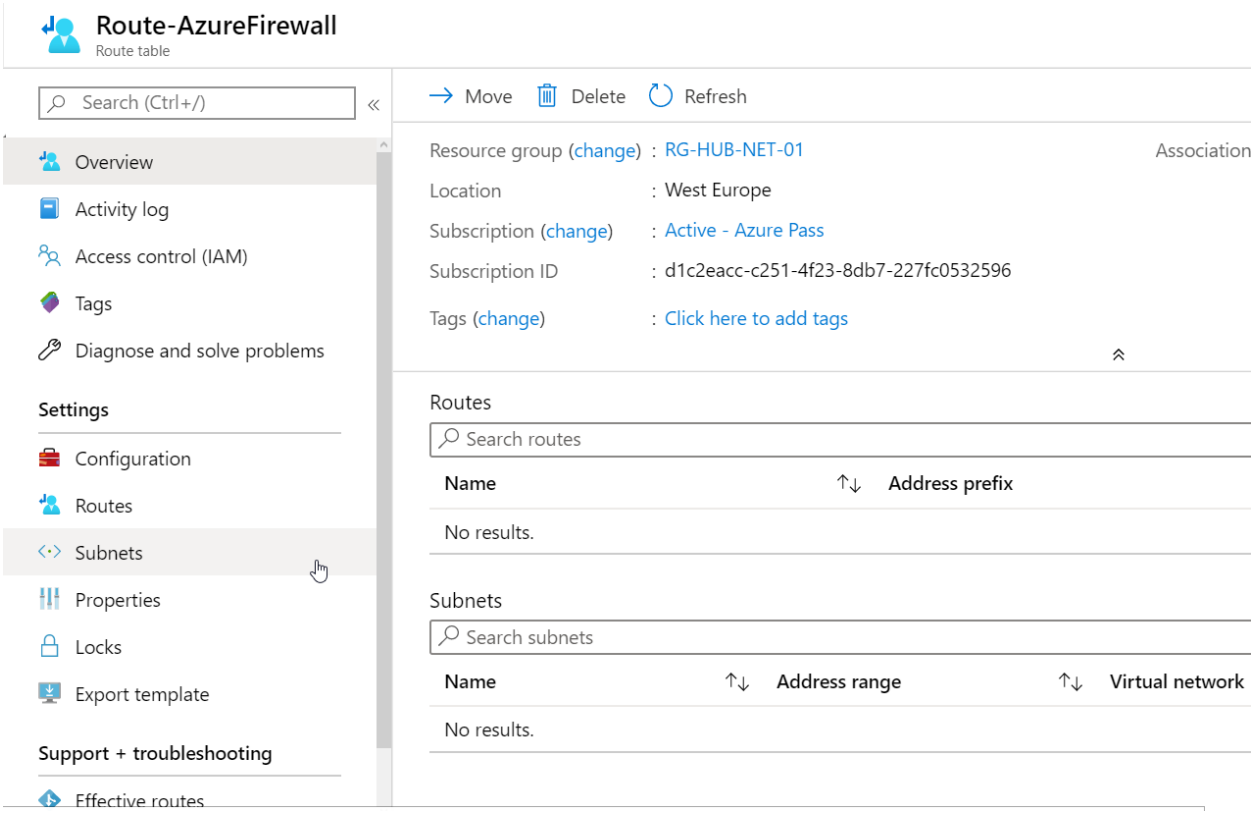


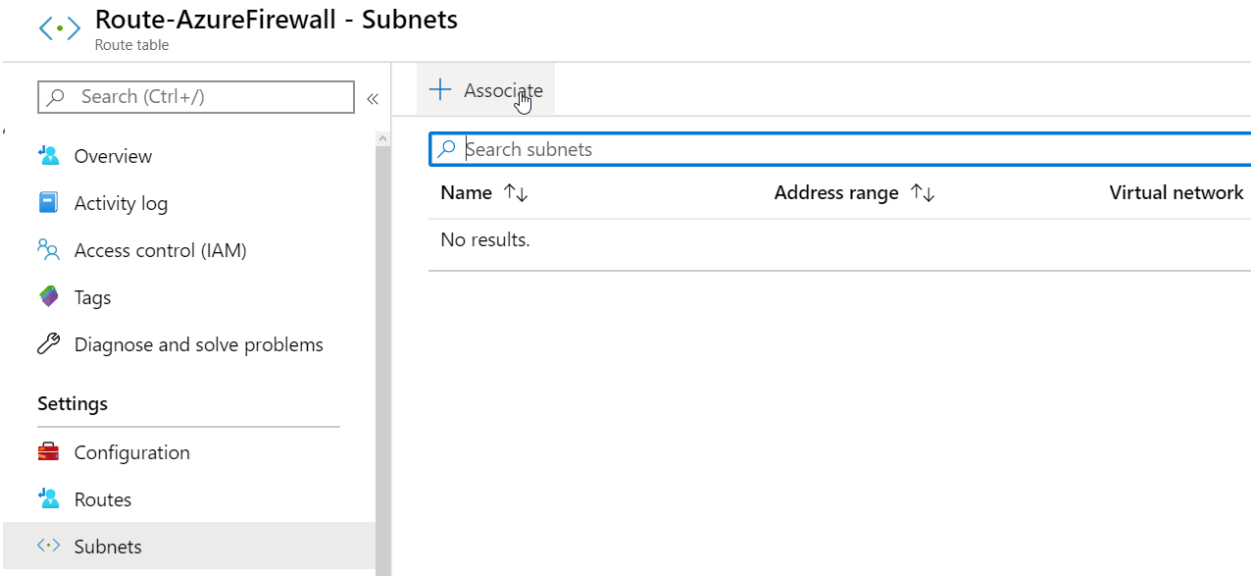


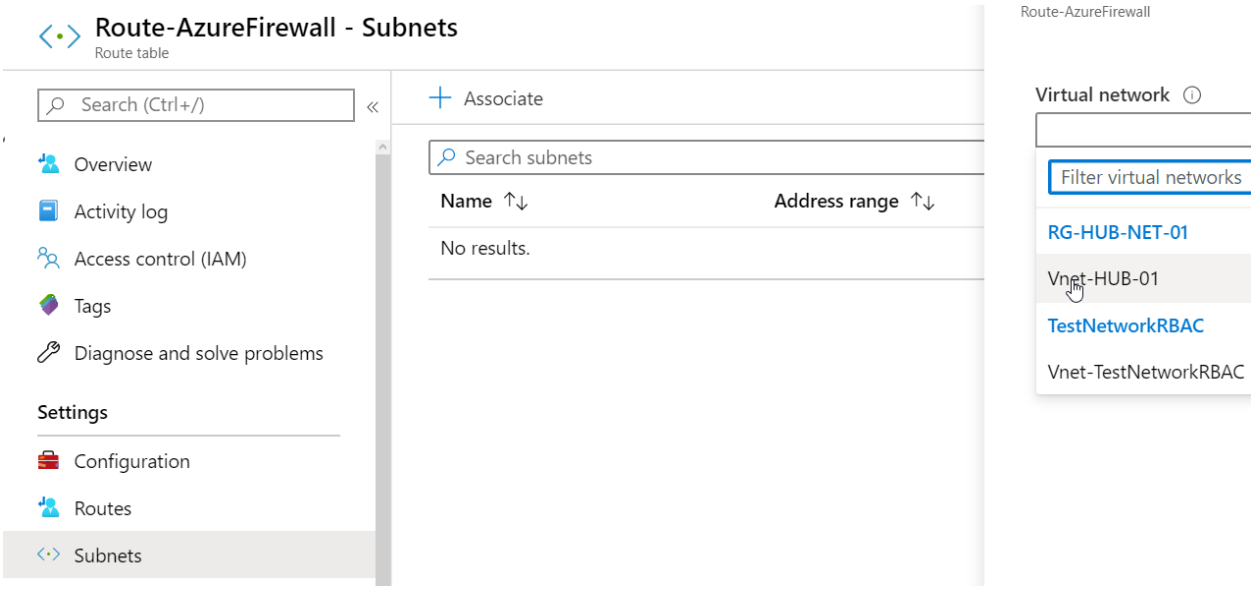

Create route table
You can add routes to this table after it's created.
Name *
Route-AzureFirewall
Subscription *
Active - Azure Pass
Resource group *
RG-HUB-NET-01
Create new
Location *
(Europe) West Europe
Virtual network gateway route propagation
Disabled
Enabled
Create
Automation options


Route tables
Contoso
Add
Manage view
Refresh
Export to CSV
Assign tags
Feedback
Leave preview
Filter by name...
Subscription == Active - Azure Pass
Resource group == all
Location == all
Showing 1 to 1 of 1 records.
Name
Resource group
Location
Route-AzureFirewall
RG-HUB-NET-01
West Europe

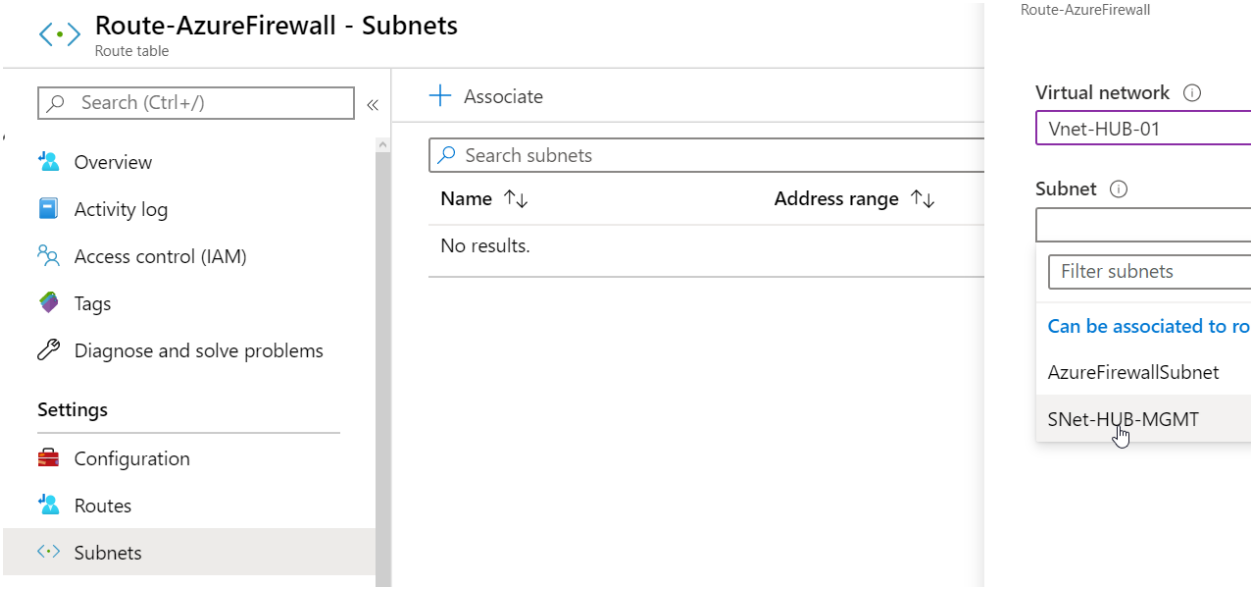
Let's Associate Azure firewall with **Servers Workload (Snet-HUB-MGMT)** subnet

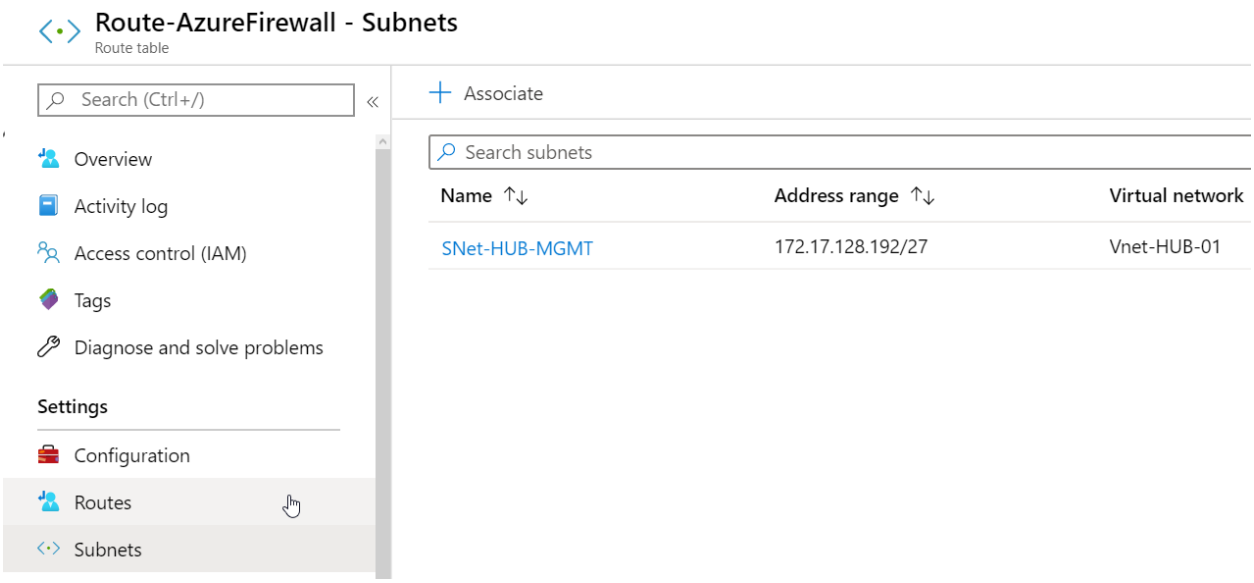




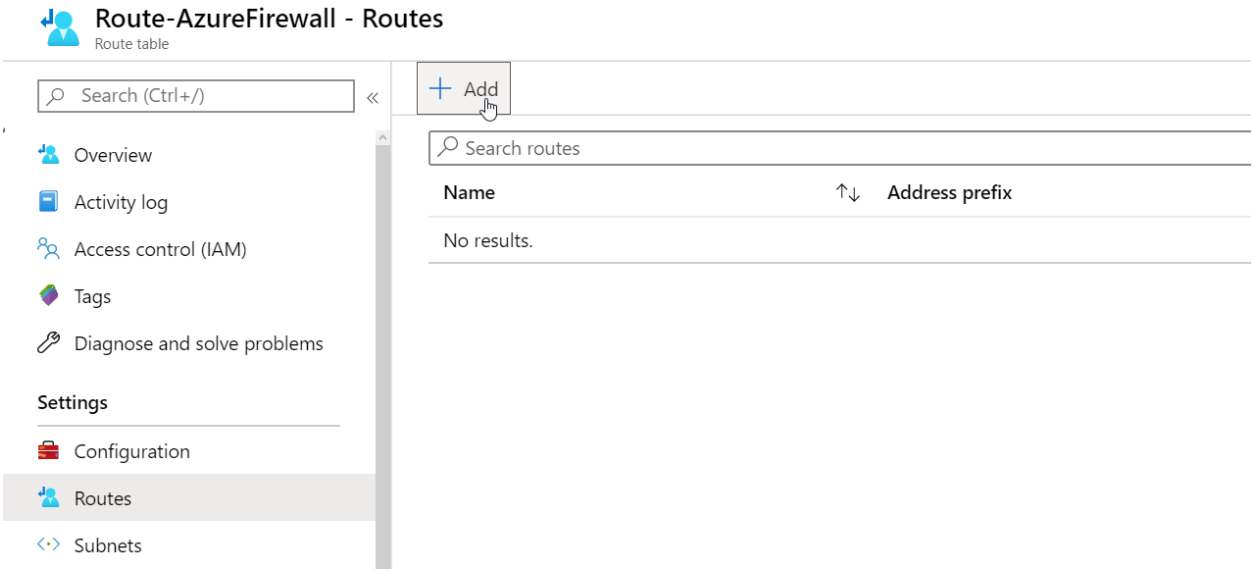


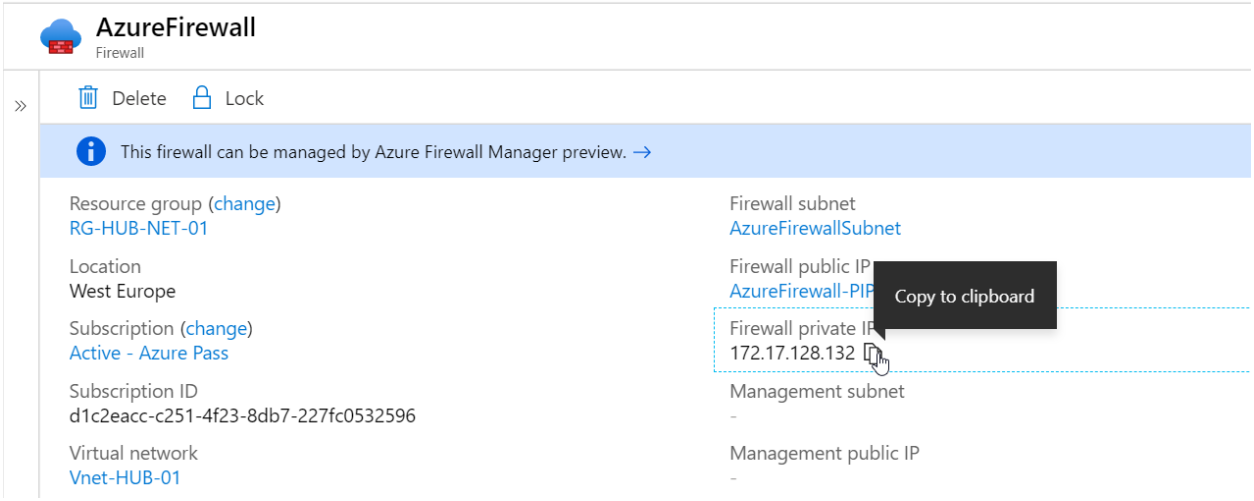
Under Azure firewall Subnet Settings, Associate **Servers Workload (Snet-HUB-MGMT)** subnet.



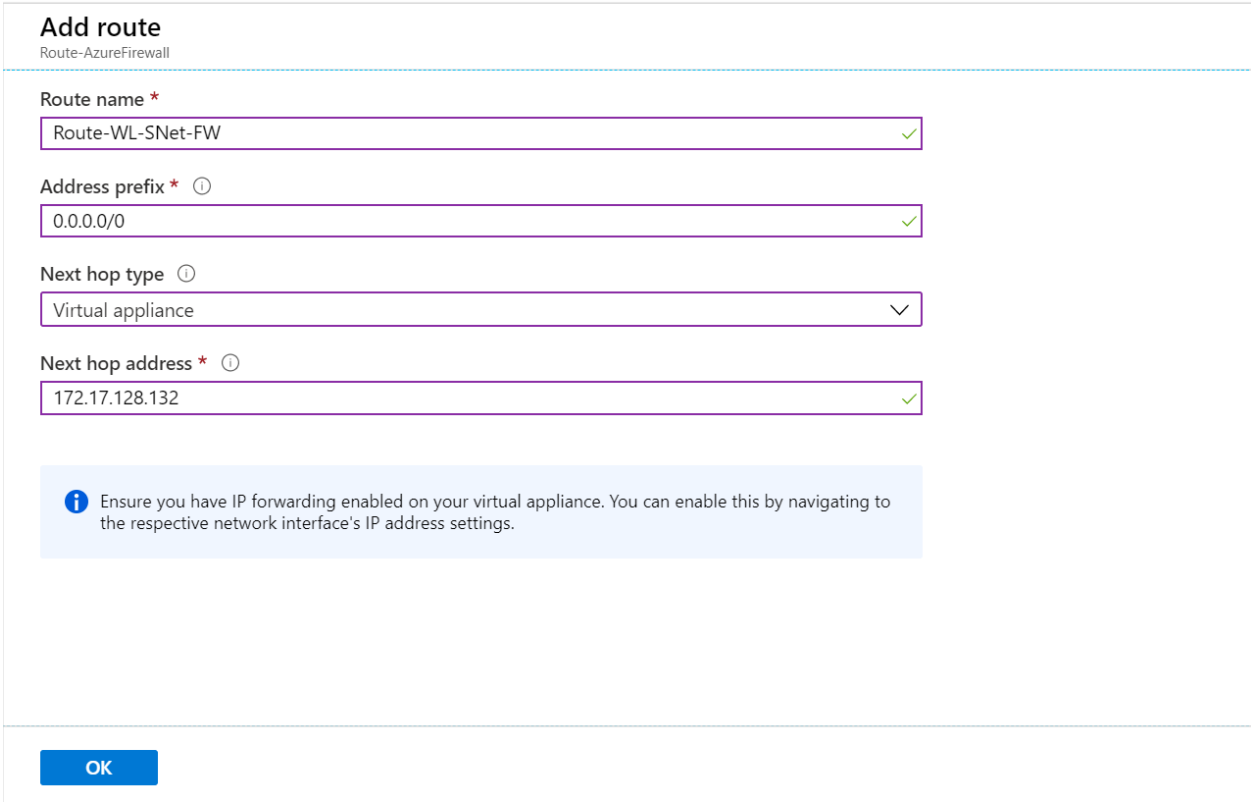


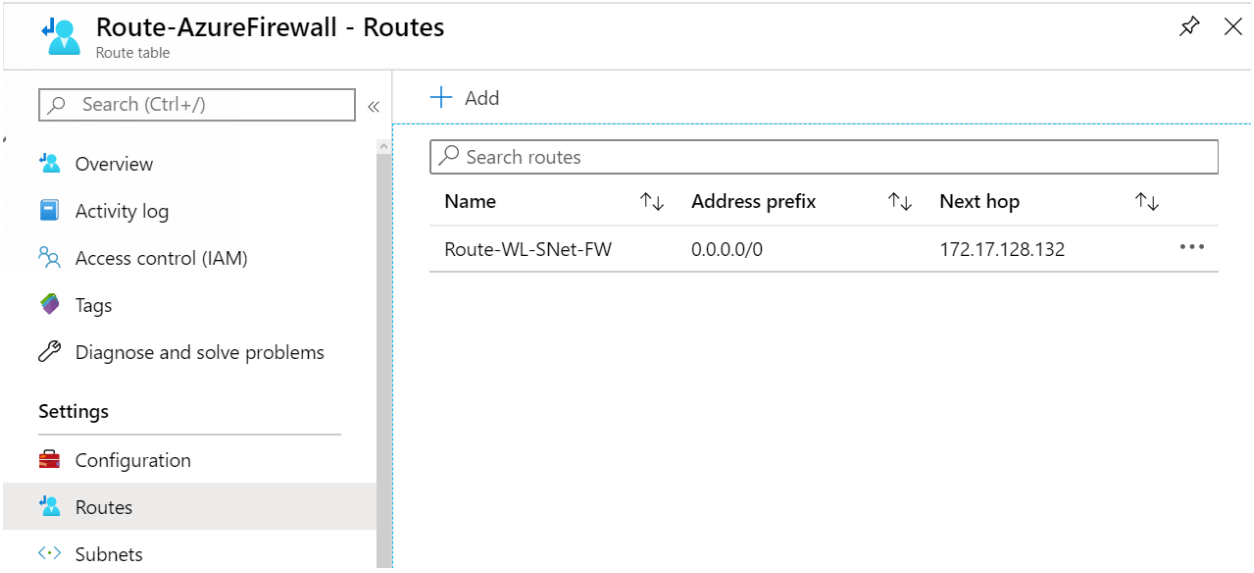
Now its time to add a route for routing all traffic from **Servers Workload** subnet to **Azure Firewall Appliance Private IP.**





- Azure Firewall is actually a managed service, but **virtual appliance** works in this situation.
- For **Next hop address**, type the private IP address for the firewall that you noted previously.



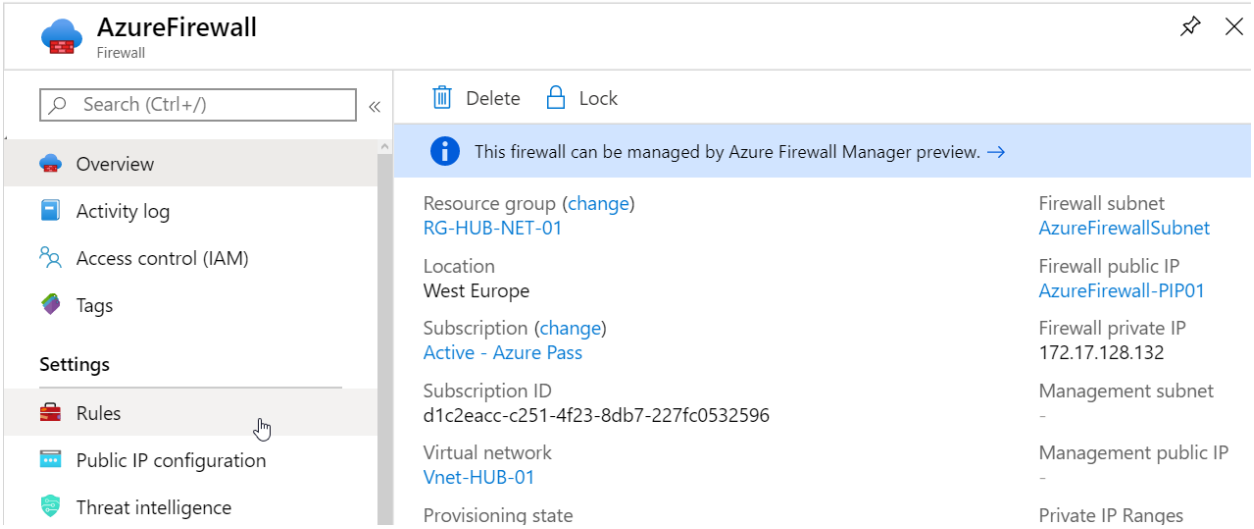


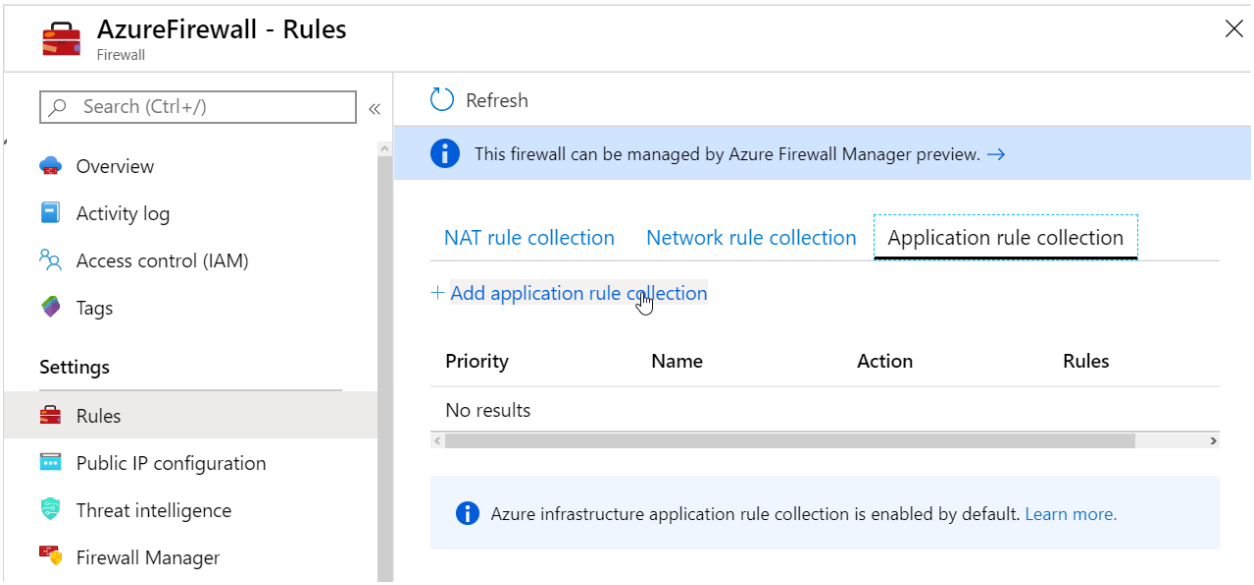
Configure an application rule

Application rules are used to block and allow a website access to a subnet.

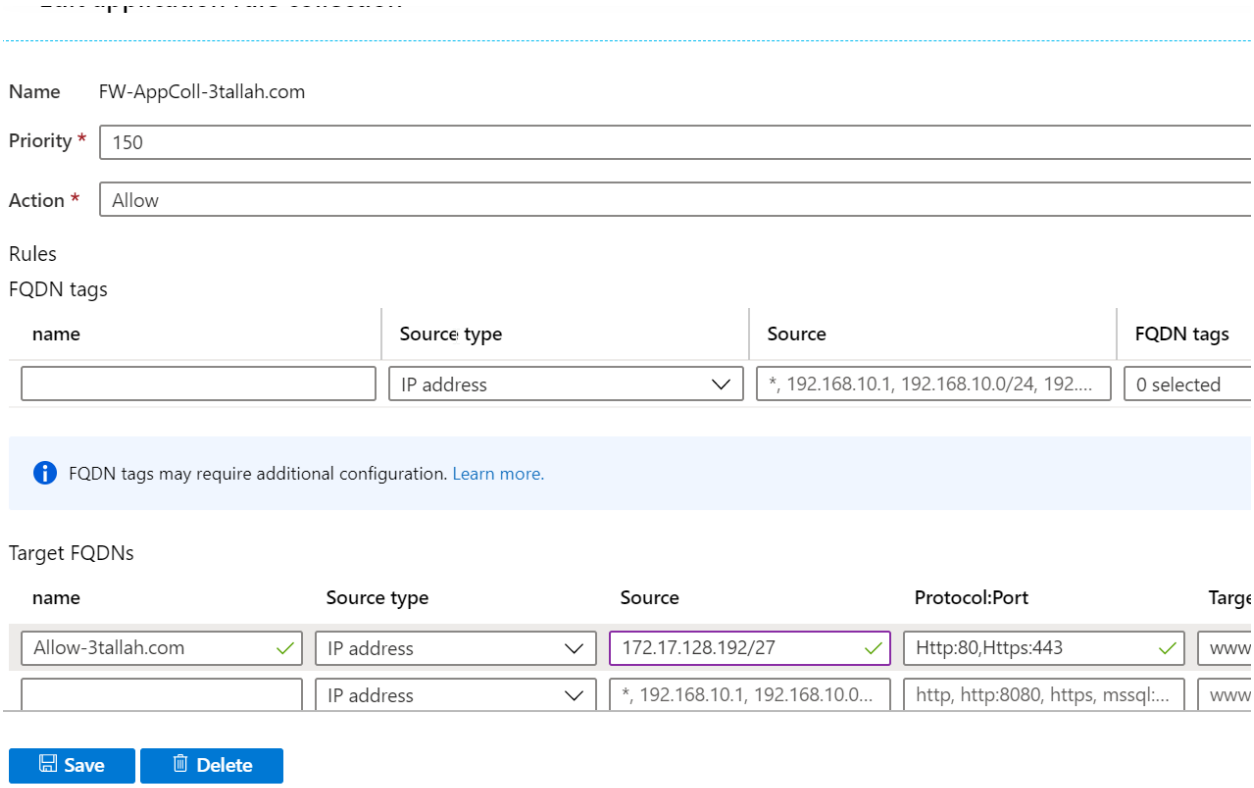
This is the application rule that allows outbound access to *.3tallah.com.

1. Open the **Azure Firewall** and select the **rules**.





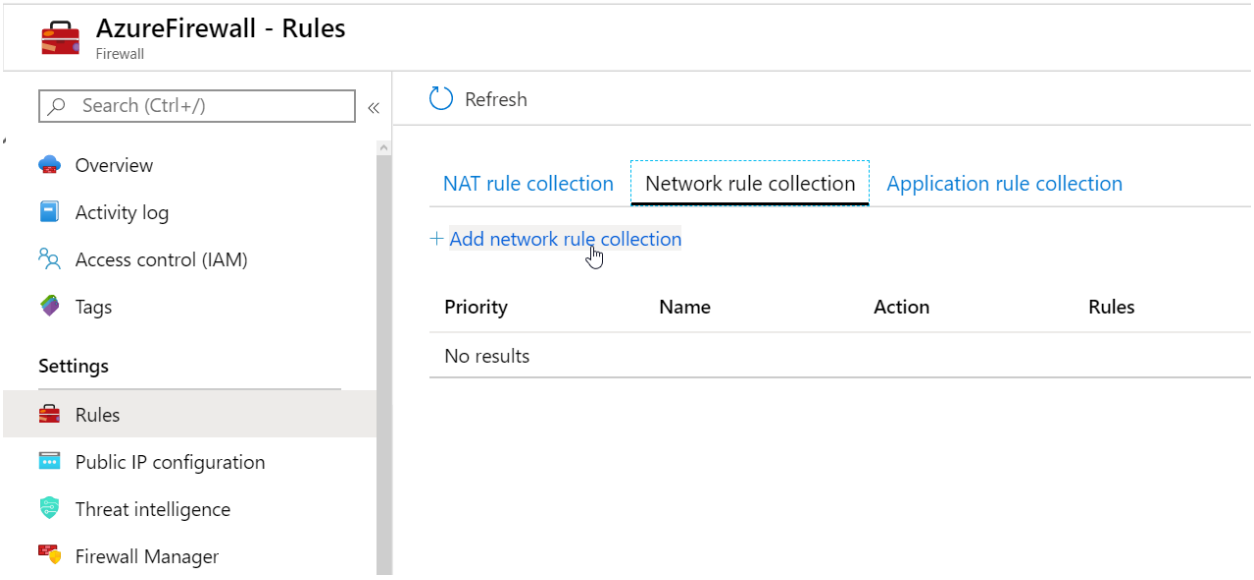
- For **Source**, type **172.17.128.192/27**. **(Internal Workload Servers IP Range)**
- For **Protocol:port**, type **http, https**.
- For **Target FQDNS**, type **www.3tallah.com**



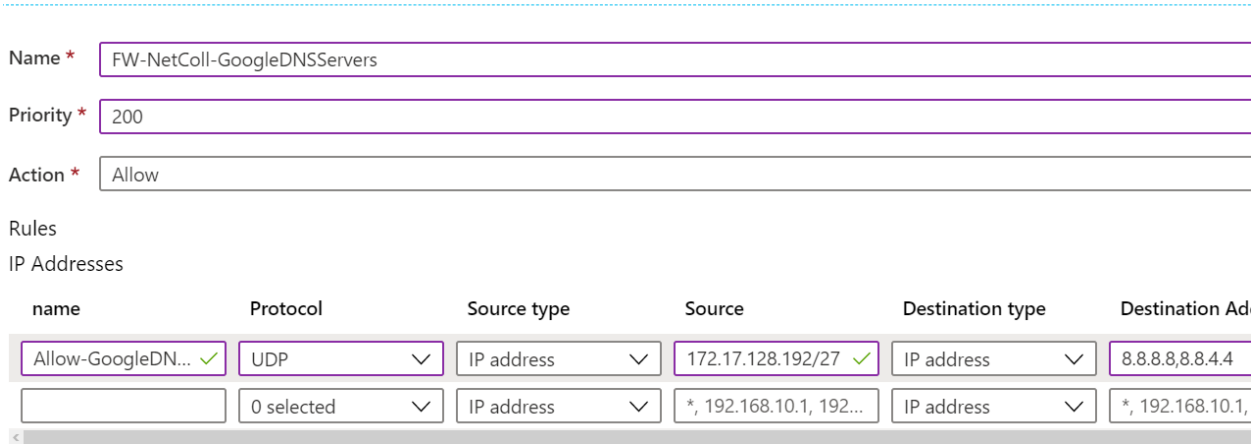
Configure a network rule

Network Rules are applied first then the application rules and it is containing source addresses, protocols, destination ports, and destination addresses.

Creating a network rule to allow outbound access to Google DNS Server on port 53.



- For **Protocol**, select **UDP**
- For **Destination address**, type **8.8.8.8,8.8.4.4**
- For **Destination Ports**, type **53**.



Create virtual machines

Create a virtual machine

Basics | Disks | Networking | Management | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.
Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? Create VM from Azure Marketplace

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Active - Azure Pass

Resource group * : (New) RG-HUB-MGMT-01
Create new

Instance details

Virtual machine name * : HUB-JUMP-1

Region * : (Europe) West Europe

Review + create | < Previous | Next : Disks >

Image * : Windows Server 2019 Datacenter
Browse all public and private images

Azure Spot instance : Yes / No

Size * : **Standard DS1 v2**
1 vcpu, 3.5 GiB memory ($49.57/month)
Change size

Administrator account

Username * : AZAdmin

Password * : ••••••••••••••

Confirm password * : ••••••••••••••

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Review + create | < Previous | Next : Disks >

Create a virtual machine

Basics | Disks | Networking | Management | 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 *	Vnet-HUB-01 Create new
Subnet *	SNet-HUB-MGMT (172.17.128.192/27) Manage subnet configuration
Public IP	None Create new
NIC network security group	None / Basic / Advanced
Accelerated networking	On / Off

Review + create | < Previous | Next : Management >

Create a virtual machine

Validation passed

Basics | Disks | Networking | Management | Advanced | Tags | Review + create

PRODUCT DETAILS

Standard DS1 v2
by Microsoft
Terms of use | Privacy policy

Subscription credits apply
0.0679 USD/hr
Pricing for other VM sizes

TERMS

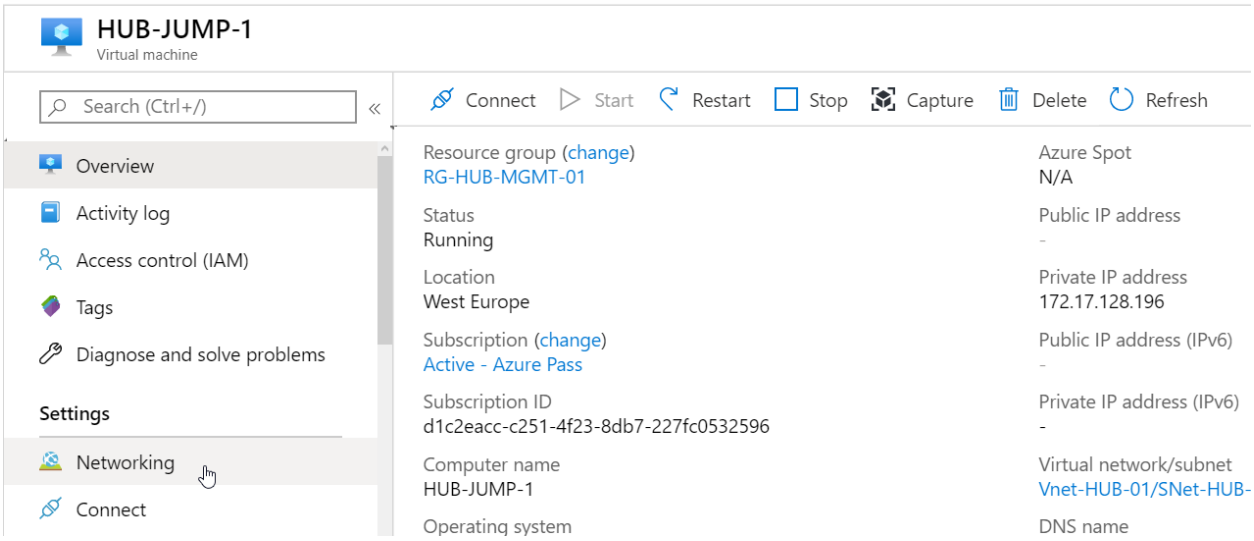
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

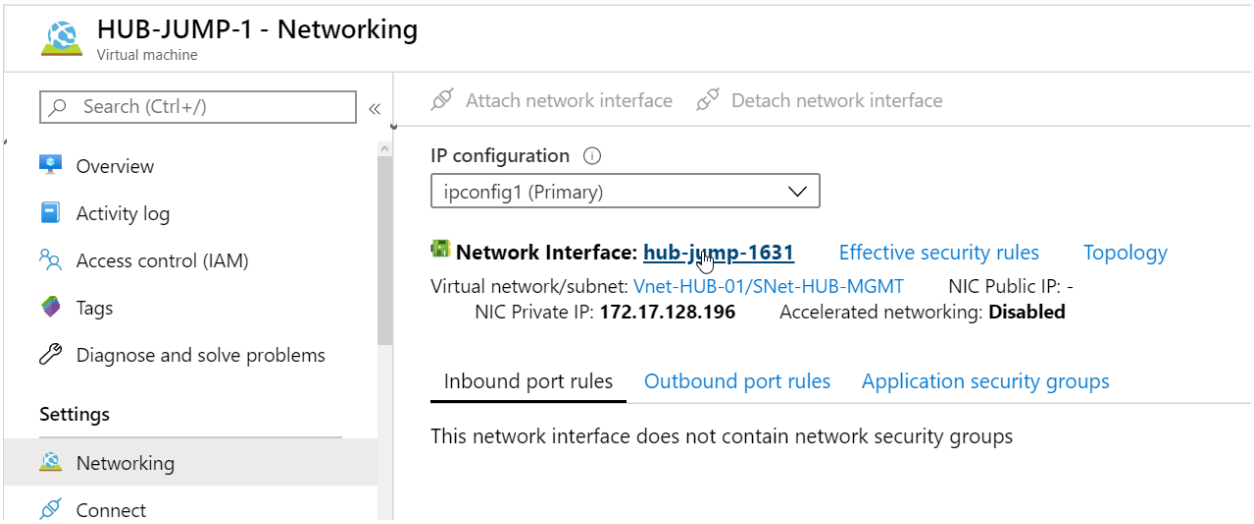
Basics

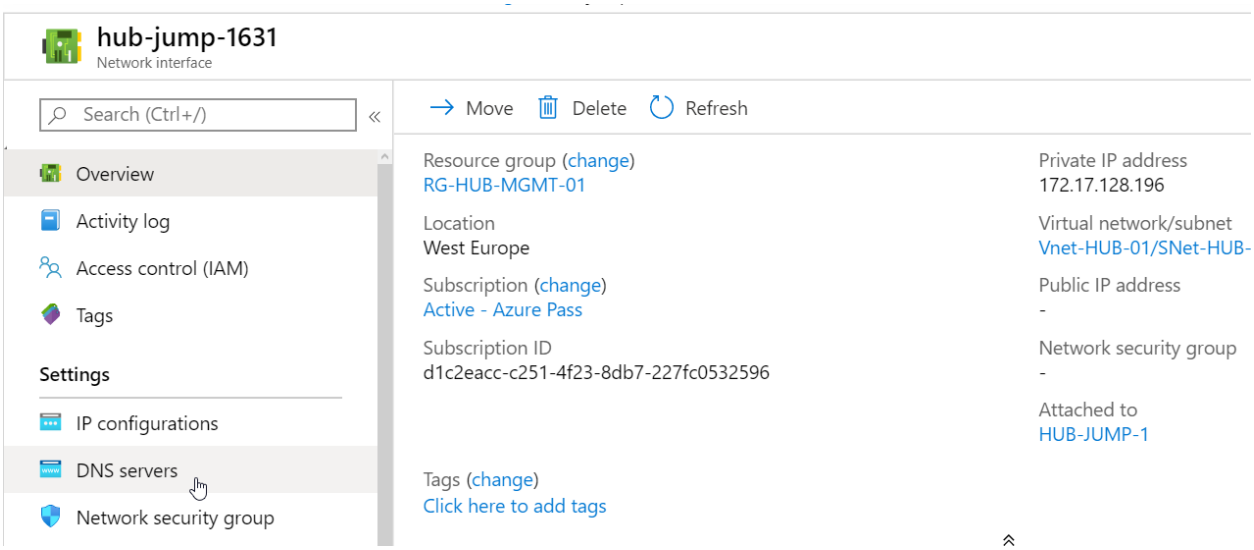
Subscription	Active - Azure Pass

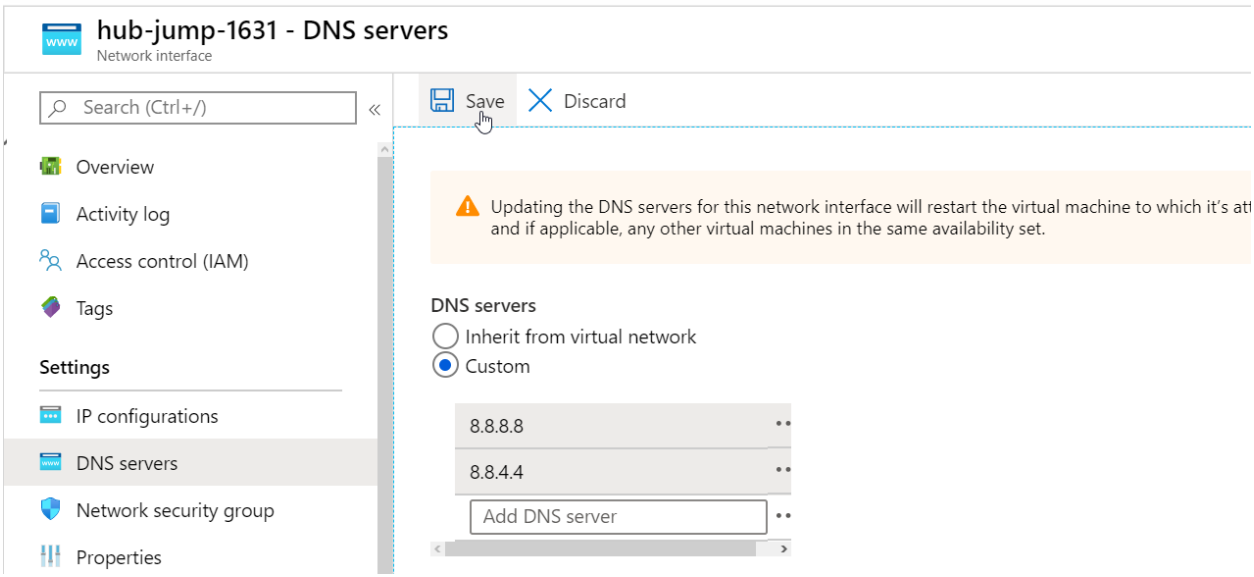
Create | < Previous | Next > | Download a template for automation

Change DNS addresses for the Workload Server NIC.






hub-jump-1631
Network interface
Search (Ctrl+/)
Move
Delete
Refresh
Overview
Activity log
Access control (IAM)
Tags
Settings
IP configurations
DNS servers
Network security group
Resource group (change)
RG-HUB-MGMT-01
Location
West Europe
Subscription (change)
Active - Azure Pass
Subscription ID
d1c2eacc-c251-4f23-8db7-227fc0532596
Tags (change)
Click here to add tags
Private IP address
172.17.128.196
Virtual network/subnet
Vnet-HUB-01/SNet-HUB-
Public IP address
-
Network security group
-
Attached to
HUB-JUMP-1


hub-jump-1631 - DNS servers
Network interface
Search (Ctrl+/)
Save
Discard
Overview
Activity log
Access control (IAM)
Tags
Settings
IP configurations
DNS servers
Network security group
Properties
Updating the DNS servers for this network interface will restart the virtual machine to which it's att
and if applicable, any other virtual machines in the same availability set.
DNS servers
Inherit from virtual network
Custom
8.8.8.8
8.8.4.4
Add DNS server

Create Azure Bastion to connect to Workload Servers

Bastion
Microsoft

Bastion Save for later
Microsoft

Create

Overview Plans

Bastion enables seamless secure RDP/SSH connectivity to Azure Virtual Machines in your Azure Virtual Networks directly in your web browser ar without the need of public IP on your Virtual Machines.

Useful Links
Documentation

Create a Bastion

Basics Tags Review + create

Bastion allows web based RDP access to your vnet VM. Learn more.

Project details

Subscription * Active - Azure Pass

Resource group * RG-HUB-NET-01
Create new

Instance details

Name * AzureBastion

Region * westeurope

Configure virtual networks

Virtual network * Vnet-HUB-01
Create new

Review + create Previous Next : Tags > Download a template for automation

Create a Bastion

Region * westeurope

Configure virtual networks

Virtual network * Vnet-HUB-01

Create new

Subnet * AzureBastionSubnet (172.17.128.96/27)

Manage subnet configuration

Public IP address

Public IP address * Create new / Use existing

Public IP address name * AzureBastion-PIP01

Public IP address SKU Standard

Assignment Dynamic / Static

Review + create | Previous | Next : Tags > | Download a template for automation

Create a Bastion

Validation passed

Basics | Tags | Review + create

Summary

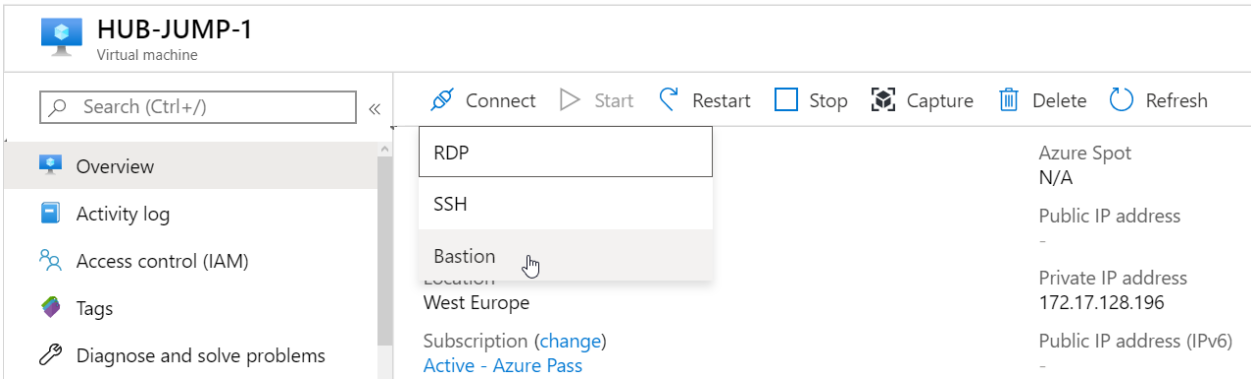
Basics

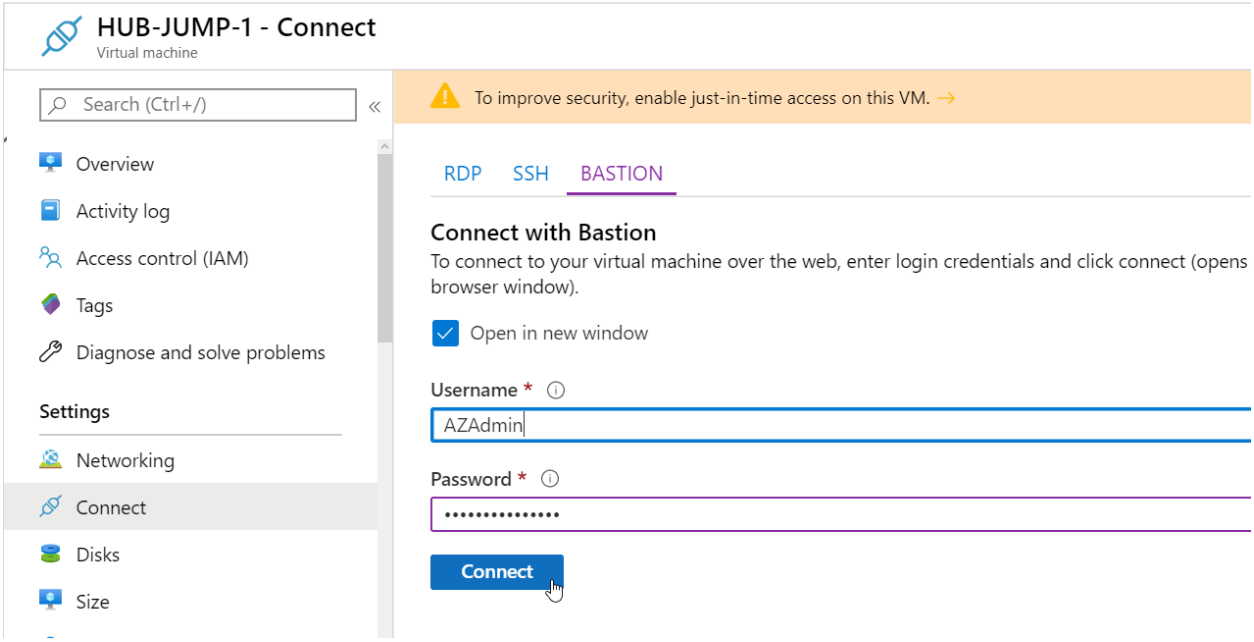
Name	AzureBastion
Subscription	Active - Azure Pass
Resource group	RG-HUB-NET-01
Region	West Europe
Virtual network	Vnet-HUB-01
Subnets	AzureBastionSubnet
Public IP address	AzureBastion-PIP01

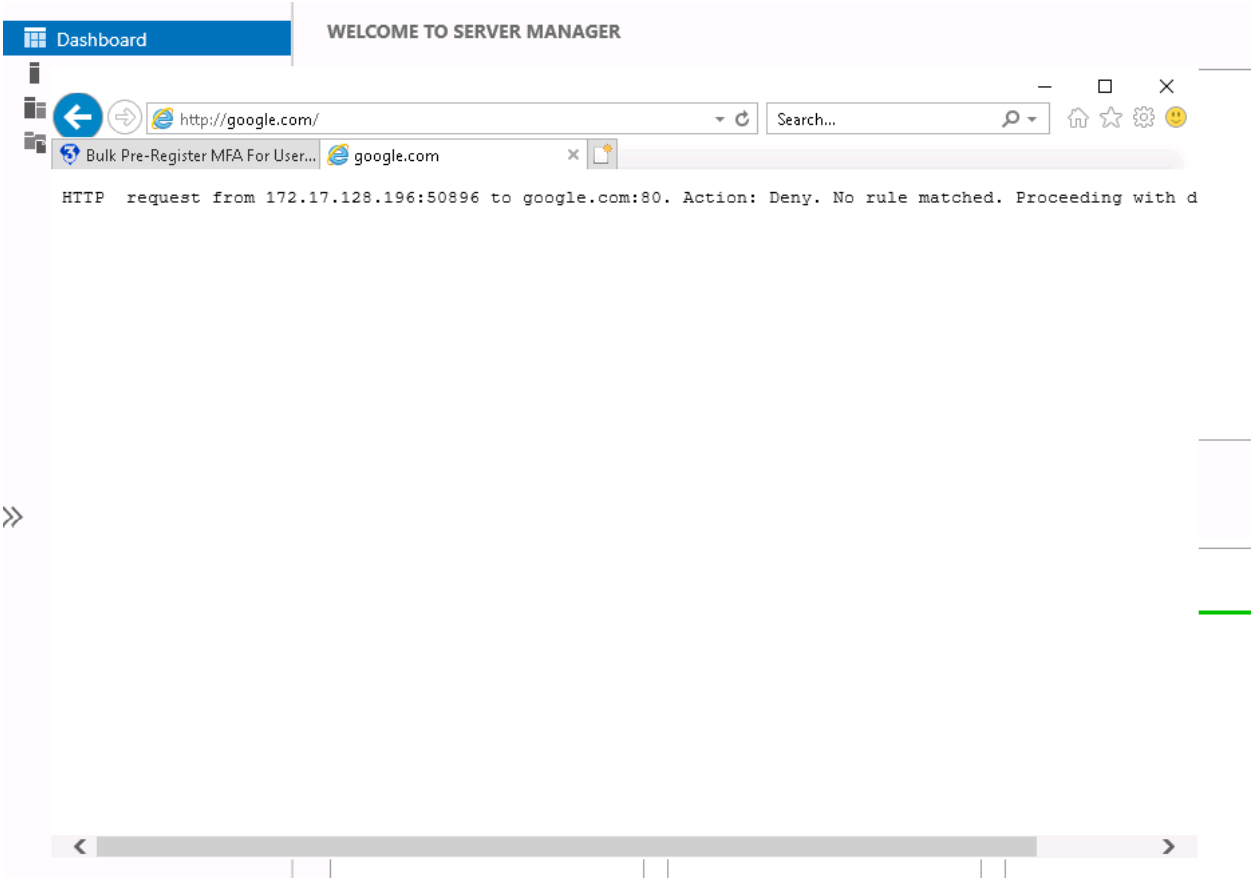
Create | Previous | Next | Download a template for automation

Test the firewall

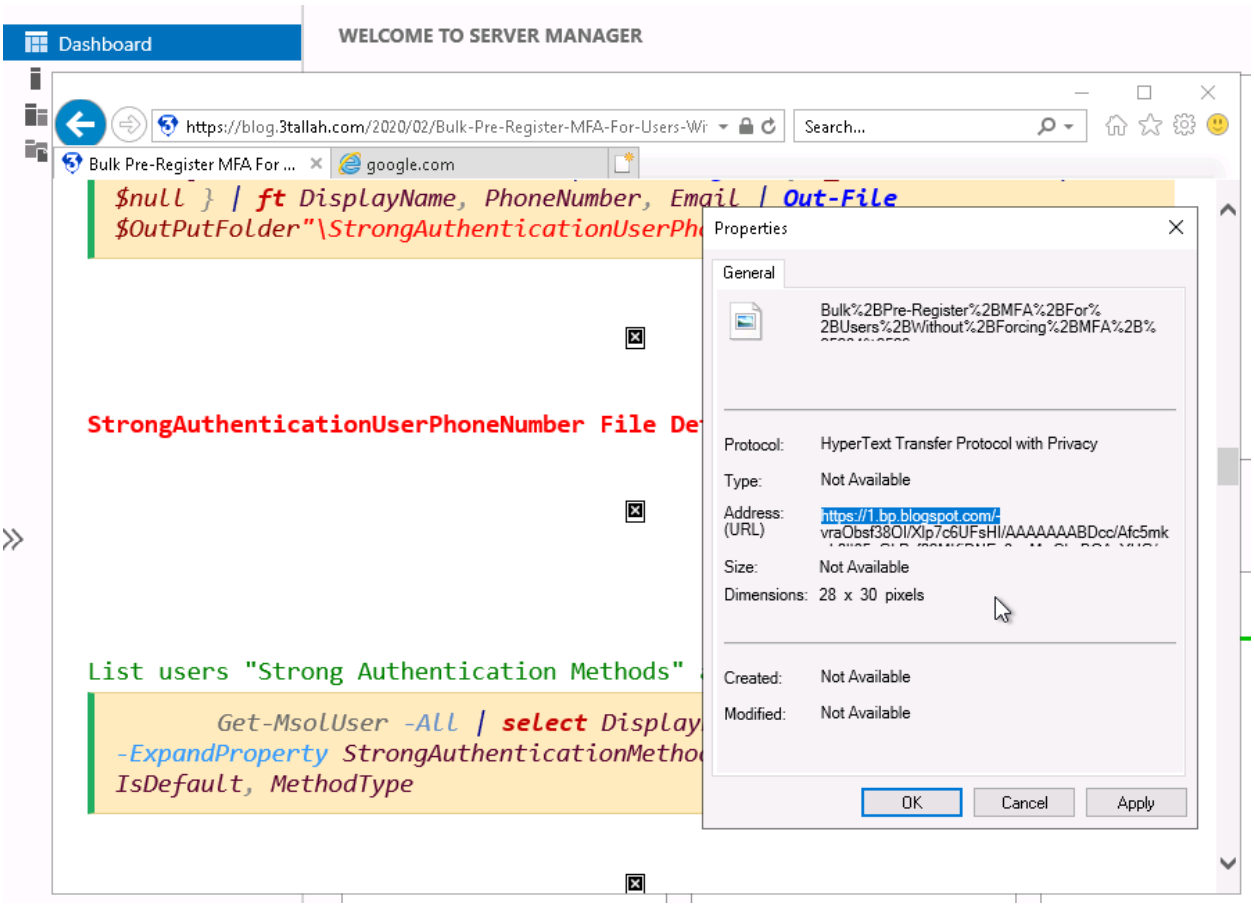
- Connect to **Workload Server** using **Azure Bastion**.
- Browse to https://www.google.com, You should be blocked by the
- Open Internet Explorer and browse to https://www.3tallah.com, You should see my website home page.



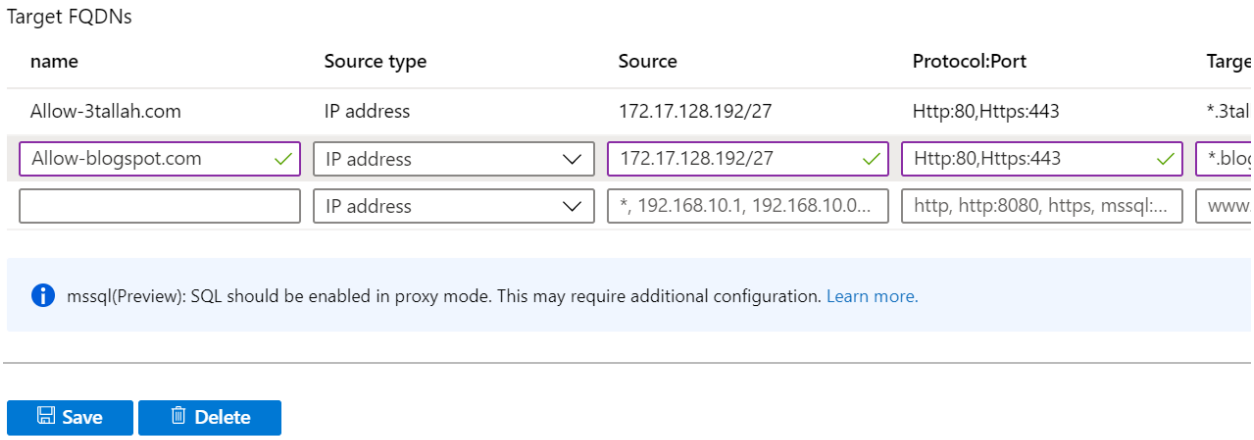




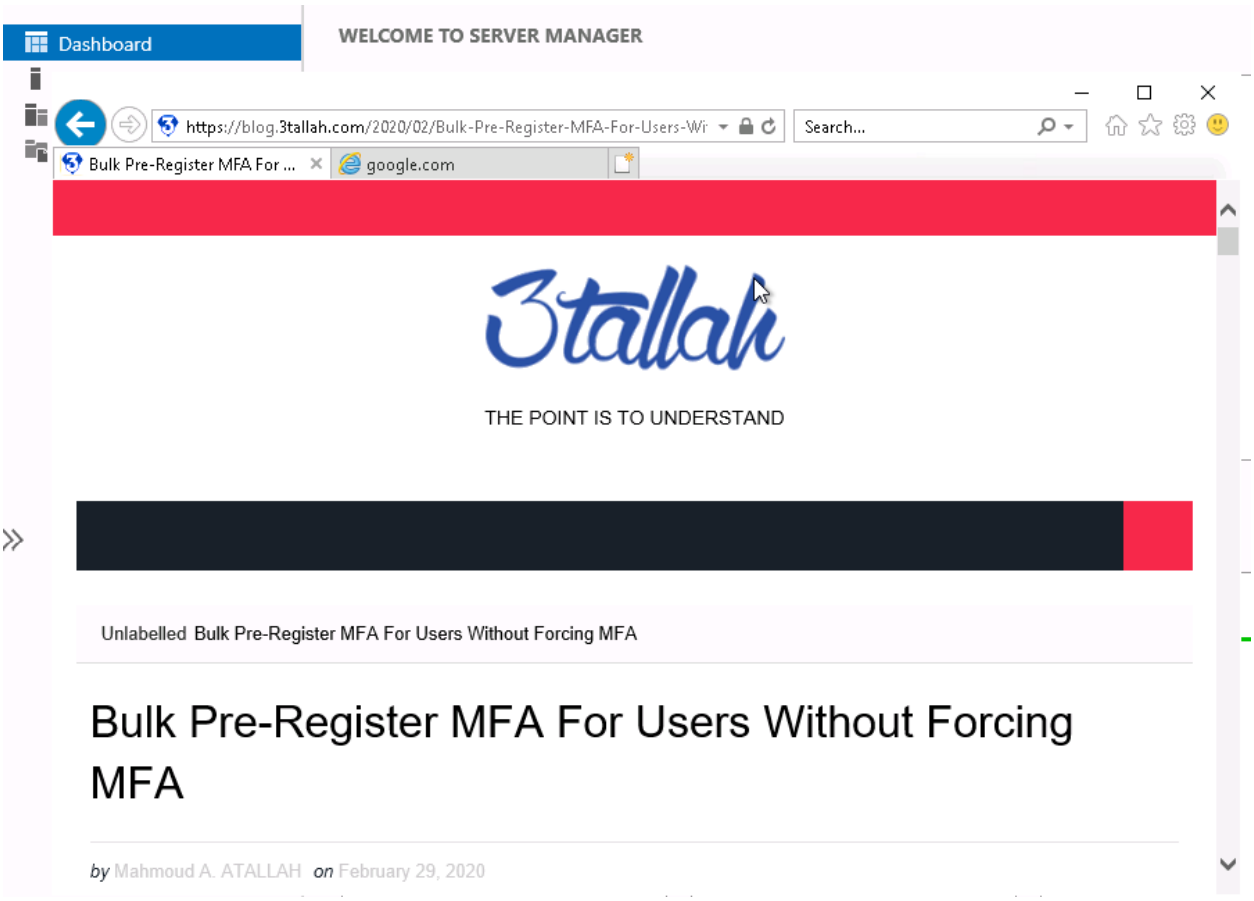
- As shown in the below Blog.3tallah.com is accessible but images are not loaded and this is because we created a rule to allow ***.3tallah.com** Only, and those images source is **blogspot.com.**



Let's Edit **"FW-AppColl-3tallah.com"** application rule collection and Allow **blogspot.com** then check the result.



As a result of allow both websites in the Azure Firewall, our website is accessible normally as shown below.



References:

https://docs.microsoft.com/en-us/azure/firewall/firewall-faq

https://azure.microsoft.com/en-us/pricing/details/azure-firewall/

https://azure.microsoft.com/en-us/blog/azure-firewall-and-network-virtual-appliances/