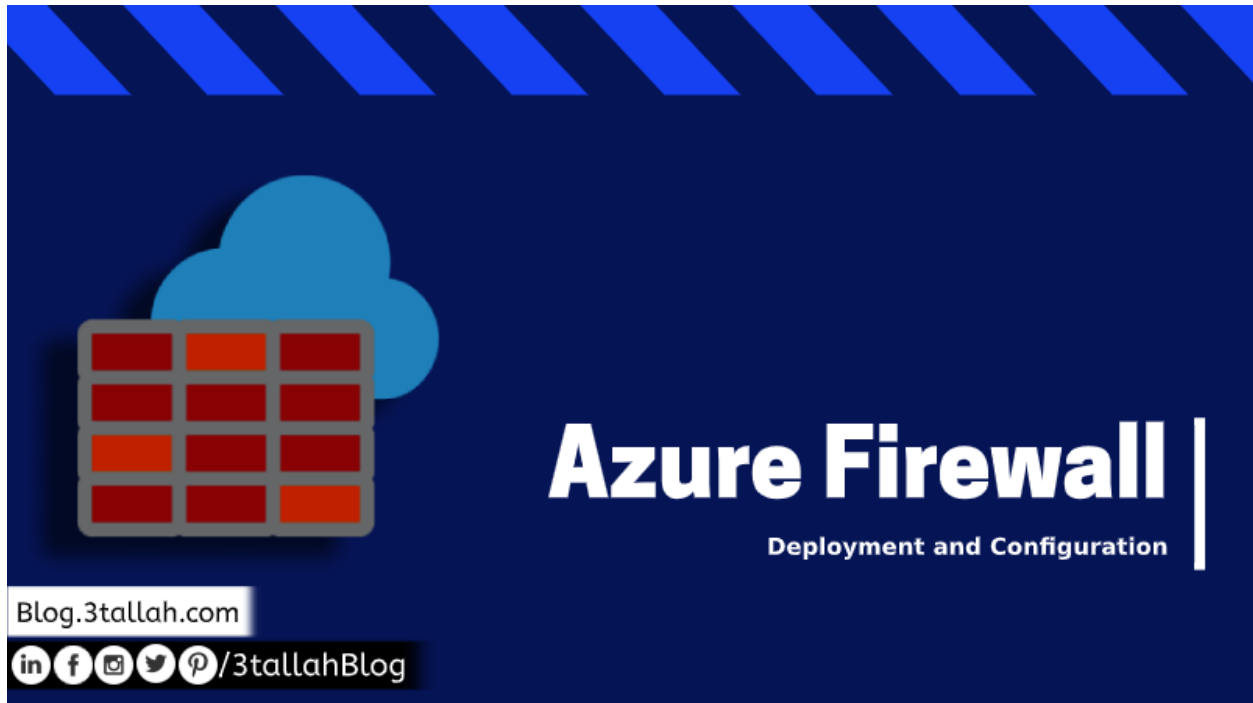


Azure Firewall Deployment



Contents

Step by Step: Deploy and configure Azure Firewall.....	2
Before we start let's have a little brief about Azure Firewall and Its consideration.....	2
In this post, you will learn step by step how to:.....	3
Set up the network	3
Deploy Azure Firewall	5
Create a default route.....	6
Configure an application rule.....	12
Configure a network rule	14
Create virtual machines	15
Change the primary and secondary DNS address for the Workload Server NIC.	17
Create Azure Bastion to connect to Workload Servers	19
Test the firewall	21

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 data 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](#)

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription *

Active - Azure Pass

Resource group *

(New) RG-HUB-NET-01

[Create new](#)

Instance details

Name *

Vnet-HUB-01

Region *

(Europe) West Europe

[Review + create](#)

< Previous

Next : IP Addresses >

[Download a template for automation](#)

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

Microsoft

♡ Save for later

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.

The screenshot shows the Azure portal interface. On the left, the 'Categories' sidebar has 'Networking' selected. The main area displays a list of networking resources under the heading 'NETWORKING (27)'. A modal window titled 'Route tables' is open, showing a '+ Create' button and a 'View' button. In the background, the 'Route tables' resource is highlighted in the list. Other visible resources include Virtual networks, Application Gateways, Local network gateways, ExpressRoute circuits, Network security groups, Load balancers, Virtual network gateways, CDN profiles, Network Watcher, Network security groups, Public IP addresses, Reserved IP addresses, On-premises Data Center, Route filters, DDoS protection plans, Private DNS zones, and Private Link.

The screenshot shows the 'Route tables' resource page in the Azure portal. The page title is 'Route tables' with the subscription 'Contoso' below it. The top bar contains buttons for '+ Add', 'Edit columns', 'Refresh', 'Try preview', and 'Assign tags'. Below this, the 'Subscriptions' section shows '1 of 4 selected' and a link to 'Open Directory + Subscription settings'. There are filters for 'Filter by name...', 'Active - Azure Pass', and 'All resource groups'. The main content area shows '0 items' and a table with a column header 'Name' and a sort icon.

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

+ Add filter

Showing 1 to 1 of 1 records.

<input type="checkbox"/>	Name ↑↓	Resource group ↑↓	Location ↑↓
<input type="checkbox"/>	 Route-AzureFirewall	RG-HUB-NET-01	West Europe

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

Route-AzureFirewall

Route table

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

Properties

Locks

Export template

Support + troubleshooting

Effective routes

Move Delete Refresh

Resource group (change) : RG-HUB-NET-01 Association

Location : West Europe

Subscription (change) : Active - Azure Pass

Subscription ID : d1c2eacc-c251-4f23-8db7-227fc0532596

Tags (change) : Click here to add tags

Routes

Search routes

Name

Address prefix

No results.

Subnets

Search subnets

Name

Address range

Virtual network

No results.

Route-AzureFirewall - Subnets

Route table

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

Associate

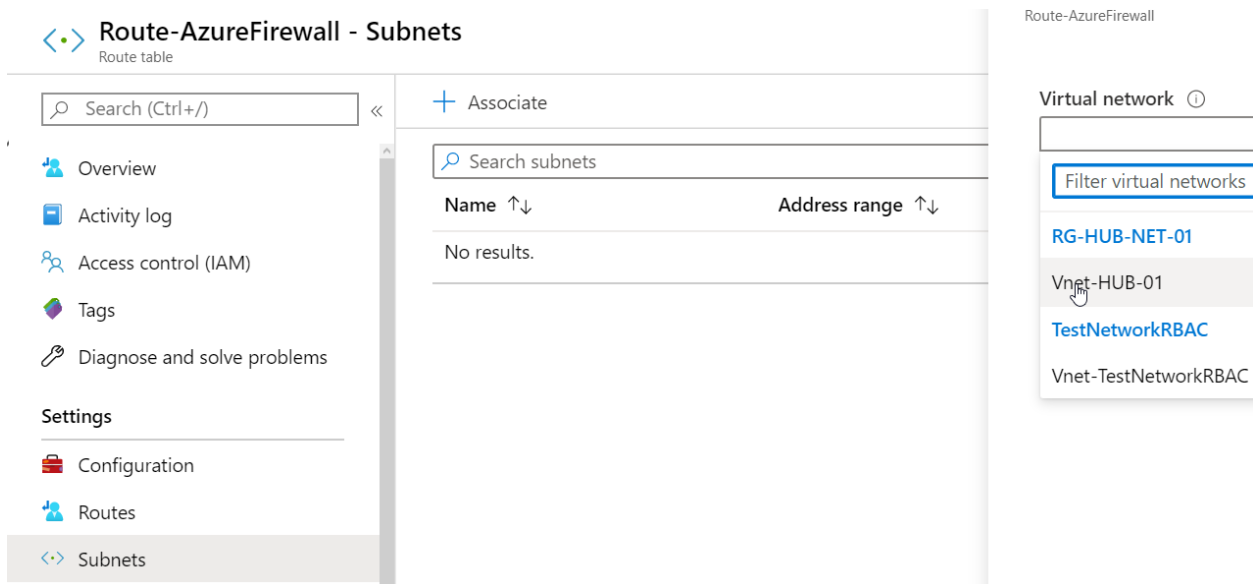
Search subnets

Name

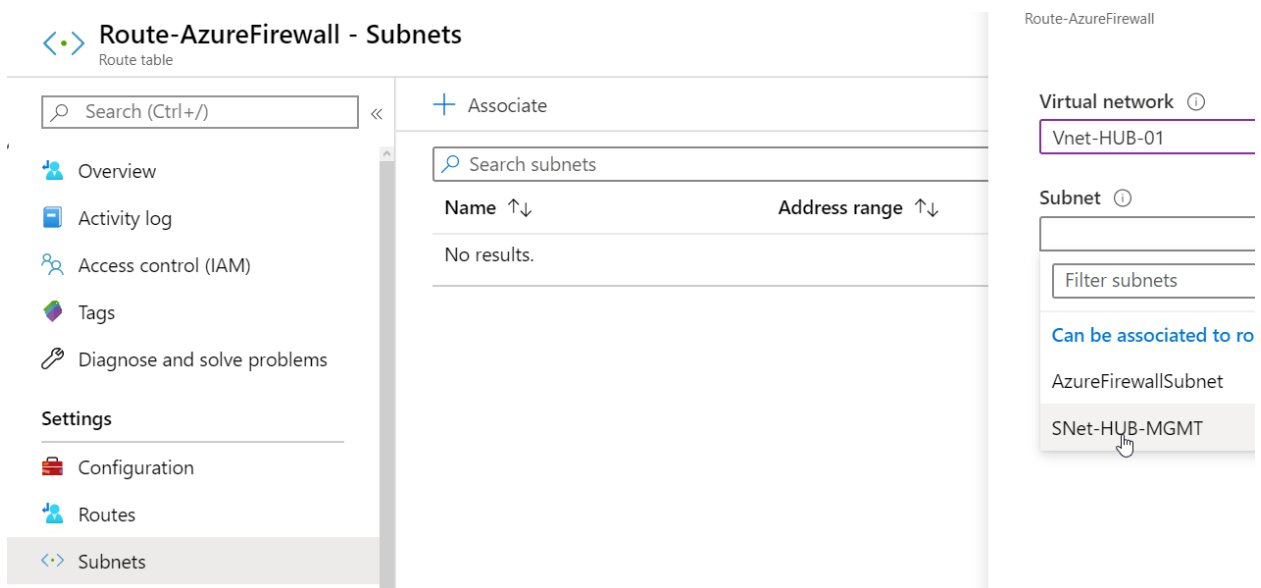
Address range

Virtual network

No results.



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



Route-AzureFirewall - Subnets

Route table

Search (Ctrl+ /)

<<

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

+ Associate

Search subnets

Name ↑↓	Address range ↑↓	Virtual network
SNet-HUB-MGMT	172.17.128.192/27	Vnet-HUB-01

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

Route-AzureFirewall - Routes

Route table

Search (Ctrl+ /)

<<

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

+ Add

Search routes

Name	Address prefix
No results.	

AzureFirewall
 Firewall

»

Delete
 Lock

This firewall can be managed by Azure Firewall Manager preview. →

Resource group (change)
 RG-HUB-NET-01

Location
 West Europe

Subscription (change)
 Active - Azure Pass

Subscription ID
 d1c2eacc-c251-4f23-8db7-227fc0532596

Virtual network
 Vnet-HUB-01

Firewall subnet
 AzureFirewallSubnet

Firewall public IP
 AzureFirewall-PIP

Firewall private IP
 172.17.128.132

Management subnet
 -

Management public IP
 -

Copy to clipboard

- 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.

Add route
 Route-AzureFirewall

Route name *

Route-WL-SNet-FW ✓

Address prefix * ⓘ

0.0.0.0/0 ✓

Next hop type ⓘ

Virtual appliance ▼

Next hop address * ⓘ

172.17.128.132 ✓

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.

OK

Route-AzureFirewall - Routes
Route table

+ Add

Name	↑↓ Address prefix	↑↓ Next hop	↑↓
Route-WL-SNet-FW	0.0.0.0/0	172.17.128.132	...

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

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**.

AzureFirewall
Firewall

Delete Lock

Overview

Activity log

Access control (IAM)

Tags

Settings

Rules

Public IP configuration

Threat intelligence

This firewall can be managed by Azure Firewall Manager preview. →

Resource group (change)
RG-HUB-NET-01

Location
West Europe

Subscription (change)
Active - Azure Pass

Subscription ID
d1c2eacc-c251-4f23-8db7-227fc0532596

Virtual network
Vnet-HUB-01

Provisioning state

Firewall subnet
AzureFirewallSubnet

Firewall public IP
AzureFirewall-PIP01

Firewall private IP
172.17.128.132

Management subnet
-

Management public IP
-

Private IP Ranges

AzureFirewall - Rules
Firewall

Overview

Activity log

Access control (IAM)

Tags

Settings

Rules

Public IP configuration

Threat intelligence

Firewall Manager

Refresh

This firewall can be managed by Azure Firewall Manager preview. →

NAT rule collection

Network rule collection

Application rule collection

+ Add application rule collection

Priority	Name	Action	Rules
No results			

Azure infrastructure application rule collection is enabled by default. [Learn more.](#)

- 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

FW-AppColl-3tallah.com

Priority *

150

Action *

Allow

Rules

FQDN tags

name	Source type	Source	FQDN tags
	IP address	*, 192.168.10.1, 192.168.10.0/24, 192....	0 selected

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

Target FQDNs

name	Source type	Source	Protocol:Port	Target
Allow-3tallah.com ✓	IP address	172.17.128.192/27 ✓	Http:80,Https:443 ✓	www
	IP address	*, 192.168.10.1, 192.168.10.0...	http, http:8080, https, mssql:...	www

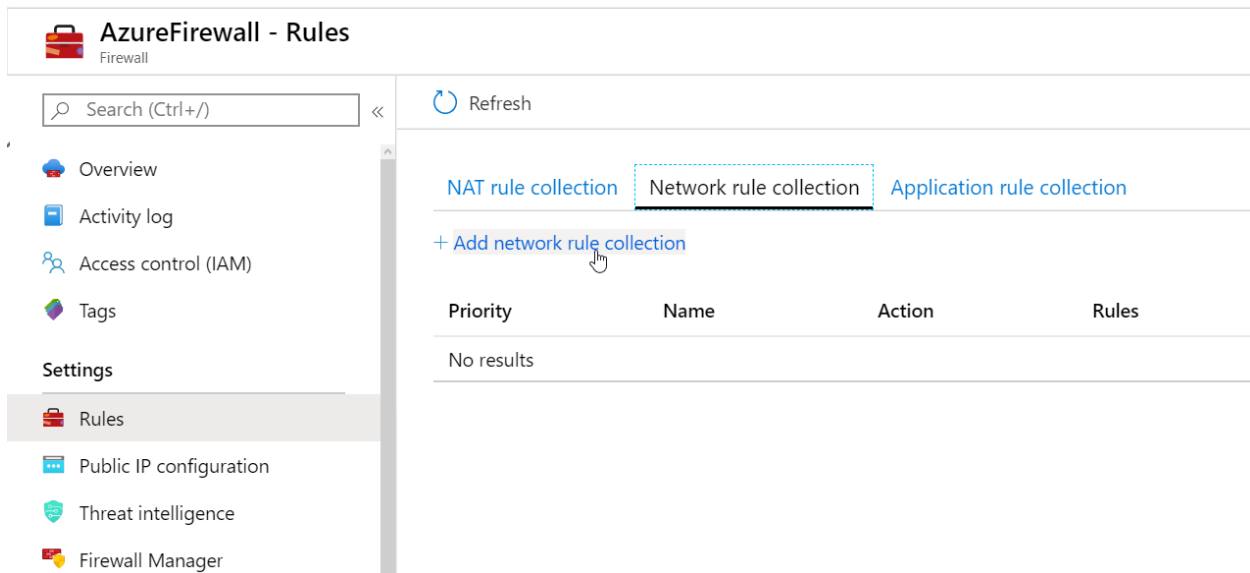
Save

Delete

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.



AzureFirewall - Rules

Search (Ctrl+/) Refresh

NAT rule collection **Network rule collection** Application rule collection

+ Add network rule collection

Priority	Name	Action	Rules
No results			

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

Name * FW-NetColl-GoogleDNSServers

Priority * 200

Action * Allow

Rules

IP Addresses

name	Protocol	Source type	Source	Destination type	Destination Ad
Allow-GoogleDN... ✓	UDP	IP address	172.17.128.192/27 ✓	IP address	8.8.8.8,8.8.4.4
	0 selected	IP address	*, 192.168.10.1, 192...	IP address	*, 192.168.10.1,

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 *	<input type="text" value="Active - Azure Pass"/>
Resource group *	<input type="text" value="(New) RG-HUB-MGMT-01"/>

[Create new](#)

Instance details

Virtual machine name *	<input type="text" value="HUB-JUMP-1"/>
Region *	<input type="text" value="(Europe) West Europe"/>

[Review + create](#)

[< Previous](#)

[Next : Disks >](#)

Image *	<input type="text" value="Windows Server 2019 Datacenter"/>
---------	---

[Browse all public and private images](#)

Azure Spot instance	<input type="radio"/> Yes <input checked="" type="radio"/> No
---------------------	---

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

Administrator account

Username *	<input type="text" value="AZAdmin"/>
Password *	<input type="password"/>
Confirm password *	<input type="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.

The image shows two screenshots from the Azure portal. The top screenshot displays the 'HUB-JUMP-1' virtual machine overview page. The left sidebar shows the 'Networking' tab selected. The main content area lists various properties of the VM, including its resource group, status, location, subscription, and network configuration. The bottom screenshot shows the 'HUB-JUMP-1 - Networking' page. The left sidebar shows the 'Networking' tab selected. The main content area displays the network interface configuration, including the IP configuration, network interface name, virtual network/subnet, and NIC details.

HUB-JUMP-1
Virtual machine

Search (Ctrl+ /) << >> Connect Start Restart Stop Capture Delete Refresh

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect

Resource group (change) [RG-HUB-MGMT-01](#) Azure Spot N/A

Status Running Public IP address -

Location West Europe Private IP address 172.17.128.196

Subscription (change) [Active - Azure Pass](#) Public IP address (IPv6) -

Subscription ID d1c2eacc-c251-4f23-8db7-227fc0532596 Private IP address (IPv6) -

Computer name HUB-JUMP-1 Virtual network/subnet [Vnet-HUB-01/SNet-HUB-](#)

Operating system DNS name

HUB-JUMP-1 - Networking
Virtual machine

Search (Ctrl+ /) << >> Attach network interface Detach network interface

IP configuration ⓘ

ipconfig1 (Primary) ▾

Network Interface: [hub-jump-1631](#) [Effective security rules](#) [Topology](#)

Virtual network/subnet: [Vnet-HUB-01/SNet-HUB-MGMT](#) NIC Public IP: -

NIC Private IP: **172.17.128.196** Accelerated networking: **Disabled**

[Inbound port rules](#) [Outbound port rules](#) [Application security groups](#)

This network interface does not contain network security groups

hub-jump-1631
 Network interface

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

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 attached 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


Step by Step Azure Firewall Deployment and Configuration

18

Create Azure Bastion to connect to Workload Servers

Bastion

Microsoft



Bastion

Microsoft

Save for later

Create

Overview Plans

Bastion enables seamless secure RDP/SSH connectivity to Azure Virtual Machines in your Azure Virtual Networks directly in your web browser and 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 *

Configure virtual networks

Virtual network * ⓘ [Create new](#)

Subnet * [Manage subnet configuration](#)

Public IP address

Public IP address * ⓘ ☒ Create new ☐ Use existing

Public IP address name * ✓

Public IP address SKU

Assignment ☐ Dynamic ☒ Static

[Review + create](#)[Previous](#)[Next : Tags >](#)[Download a template for automation](#)

Create a Bastion

i 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

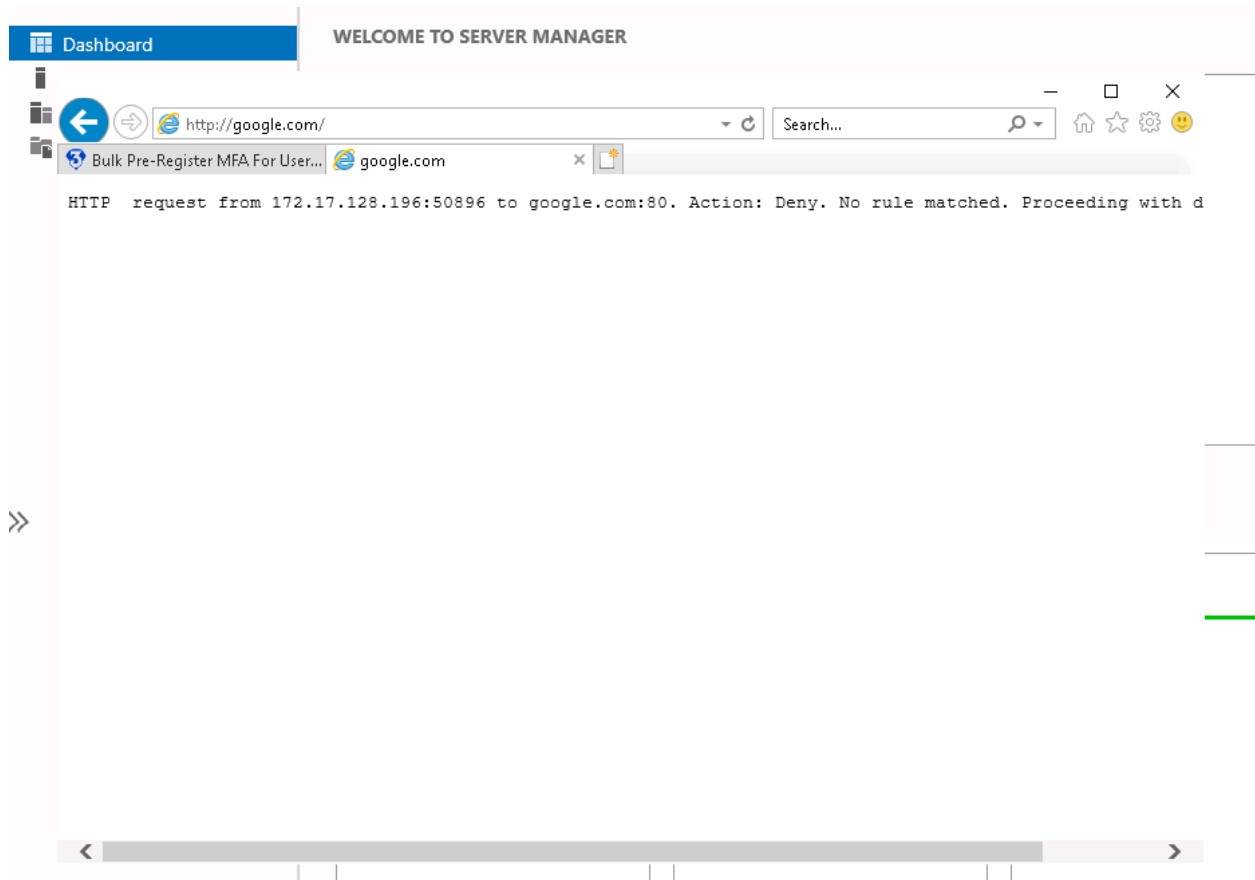
[Create](#)[Previous](#)[Next](#)[Download a template for automation](#)

Test the firewall

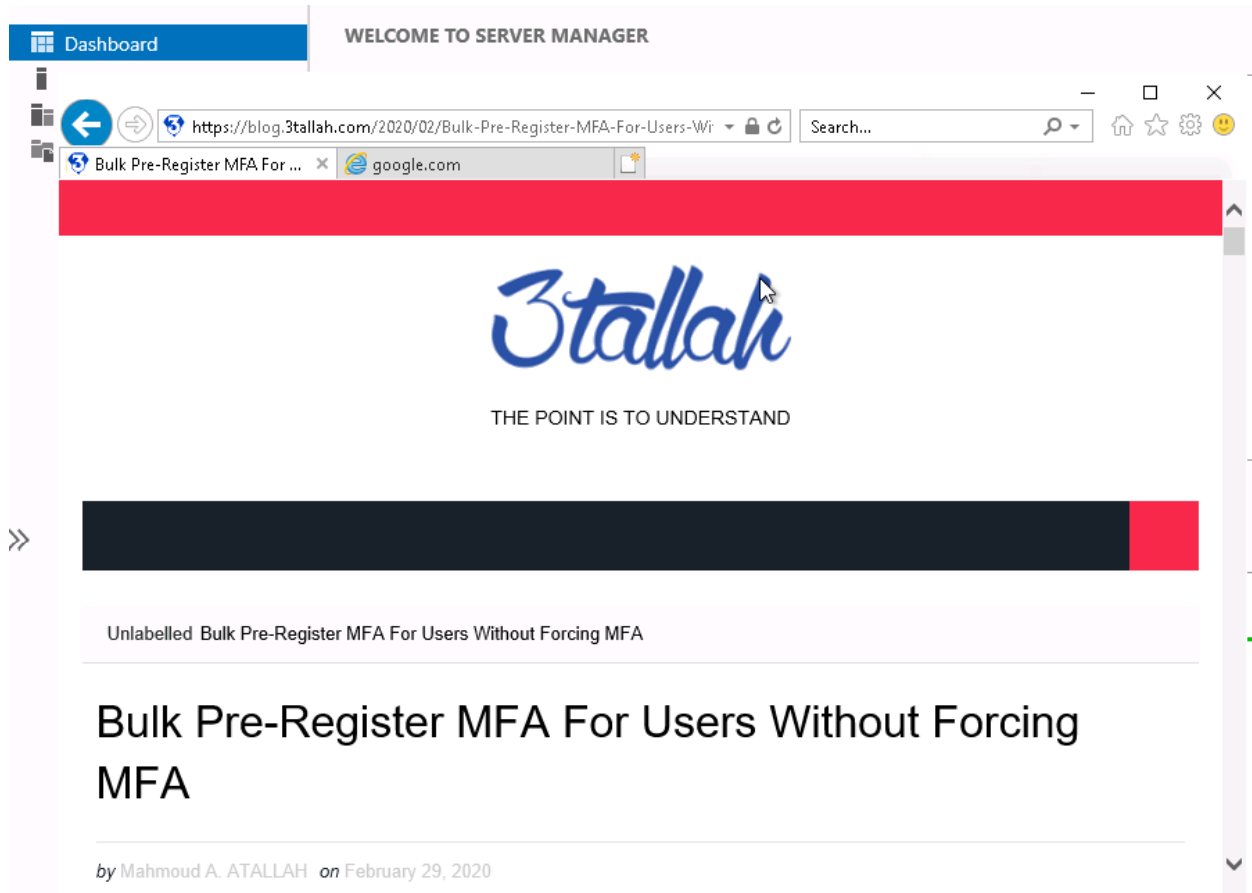
- Connect to **Workload Server** using **Azure Bastion**.
- Browse to <https://www.google.com>, You should be blocked by the
- Open Internet Explorer and browse to <https://www.3tallah.com>, You should see my website home page.

The image shows two screenshots from the Azure portal. The top screenshot displays the 'HUB-JUMP-1' virtual machine overview page. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main area shows a toolbar with 'Connect', 'Start', 'Restart', 'Stop', 'Capture', 'Delete', and 'Refresh'. A dropdown menu is open under 'Connect', showing options: RDP, SSH, Bastion (highlighted), and Location. The location is 'West Europe'. Below this, it shows 'Subscription (change)' and 'Active - Azure Pass'. On the right, there are details for 'Azure Spot' (N/A), 'Public IP address' (172.17.128.196), and 'Private IP address' (172.17.128.196).

The bottom screenshot shows the 'HUB-JUMP-1 - Connect' page. The left sidebar is the same as the top screenshot, but with 'Settings' expanded, showing 'Networking', 'Connect' (highlighted), 'Disks', and 'Size'. The main area has a warning banner: 'To improve security, enable just-in-time access on this VM. →'. Below this, there are tabs for 'RDP', 'SSH', and 'BASTION' (selected). The 'Connect with Bastion' section explains that it connects to the VM over the web. There is a checkbox 'Open in new window' which is checked. Below this are fields for 'Username' (AZAdmin) and 'Password' (masked with dots). A 'Connect' button is at the bottom.



- 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**.



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/>