
Cloud & Virtualization Class

Lab 4 · Traffic Manager, Front Door, and Firewall

Adam Lahbib · M. Sofiene Barka · Mohamed Rafraf

4/20/2023 @ INSAT

Contents

1	Introduction	3
1.1	Lab Objectives	3
2	Lab Walkthrough	4
2.1	Task 1 · Azure Traffic Manager Profile	4
2.1.1	Subtask 1.	5
2.1.1.1	Deploy two virtual machines in different regions	5
2.1.1.2	IIS on both VMs	7
2.1.1.3	Create Traffic Manager Profile	7
2.1.1.4	Add VMs as external endpoints	8
2.1.1.5	Requesting the Traffic Manager profile	9
2.1.2	Subtask 2.	10
2.1.3	Subtask 3.	10
2.2	Task 2 · Azure Front Door	10
2.2.1	Azure Front Door Classic Offering Set-up	11
2.2.2	Accessing the Front Door in the browser	14
2.2.3	Delete Resource Group	15
2.3	Task 3 · Azure Firewall	15
2.3.1	Deploy a VM	16
2.3.2	Create a Firewall	17
2.3.3	Add DNAT Rules	17
2.3.4	Testing DNAT Translation	18
2.3.5	Access Microsoft dot com	19
2.3.6	Create new route table	19
2.3.7	Associate the route table with the subnet	21
2.3.8	Can you access Microsoft dot com now?	22
2.3.9	Create an Application Rule	23
2.3.10	Try Microsoft dot com again?	24
2.3.11	Add a network rule collection	24
2.3.12	Delete resource group	25

1 Introduction

In this lab, we will learn how to use Azure Traffic Manager, Azure Front Door, and Azure Firewall. we will also learn how to use Azure Traffic Manager to distribute traffic to services hosted in Azure and on-premises, and how to use Azure Front Door to improve the performance and security of your applications. Finally, we will use Azure Firewall to protect our Azure Virtual Network resources.

1.1 Lab Objectives

- Create a Traffic Manager profile.
- Add endpoints to a Traffic Manager profile.
- Create a Front Door.
- Create a Firewall.
- Create a DNAT rule.
- Create an application rule.
- Create a network rule collection.
- Create a route table.
- Associate a route table with a subnet.

2 Lab Walkthrough

2.1 Task 1 • Azure Traffic Manager Profile

Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services hosted in Azure, on-premises, or both. Traffic Manager can monitor the health of your endpoints and automatically reroute traffic to only healthy endpoints. Traffic Manager can also be used to improve the performance of your applications by routing users to the closest data center.

2.1.1 Subtask 1.

2.1.1.1 Deploy two virtual machines in different regions

Create a virtual machine

Validation passed

Subscription	Adam
Resource group	(new) traffic-rg
Virtual machine name	vmna
Region	North Europe
Availability options	Availability zone
Availability zone	1
Security type	Standard
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Username	admoun
Public inbound ports	RDP, HTTP
Already have a Windows license?	No
Azure Spot	No

Disks

OS disk type	Premium SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

[Create](#) [< Previous](#) [Next >](#) [Download a template for automation](#) [Give feedback](#)

Create a virtual machine - Micro

+

←

↺

🔒

https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM

🔍

🗑️

A

🌟

👤

⋮

💬

Microsoft Azure

🔍 Search resources, services, and docs (G+/I)

⋮

👤

Home > Virtual machines >

Create a virtual machine

✕

🟢 Validation passed

Subscription	Adam
Resource group	traffic-rg
Virtual machine name	vmuk
Region	UK South
Availability options	Availability zone
Availability zone	1
Security type	Standard
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Username	admoun
Public inbound ports	RDP, HTTP
Already have a Windows license?	No
Azure Spot	No

Disks

OS disk type	Premium SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Create

< Previous

Next >

Download a template for automation

🗨 Give feedback

2.1.1.2 IIS on both VMs



2.1.1.3 Create Traffic Manager Profile

The traffic manager profile is the first step in creating a Traffic Manager profile. It is the container for all of the settings that define the Traffic Manager profile.

The screenshot shows the 'Create Traffic Manager profile' form in the Microsoft Azure portal. The form is titled 'Create Traffic Manager profile' and includes the following fields:

- Name ***: labtrafficman123
- Routing method**: Performance
- Subscription ***: Adam
- Resource group ***: traffic-rg
- Resource group location**: North Europe

The form also includes a 'Create new' link and a 'Traffic Manager profile' link.

2.1.1.4 Add VMs as external endpoints

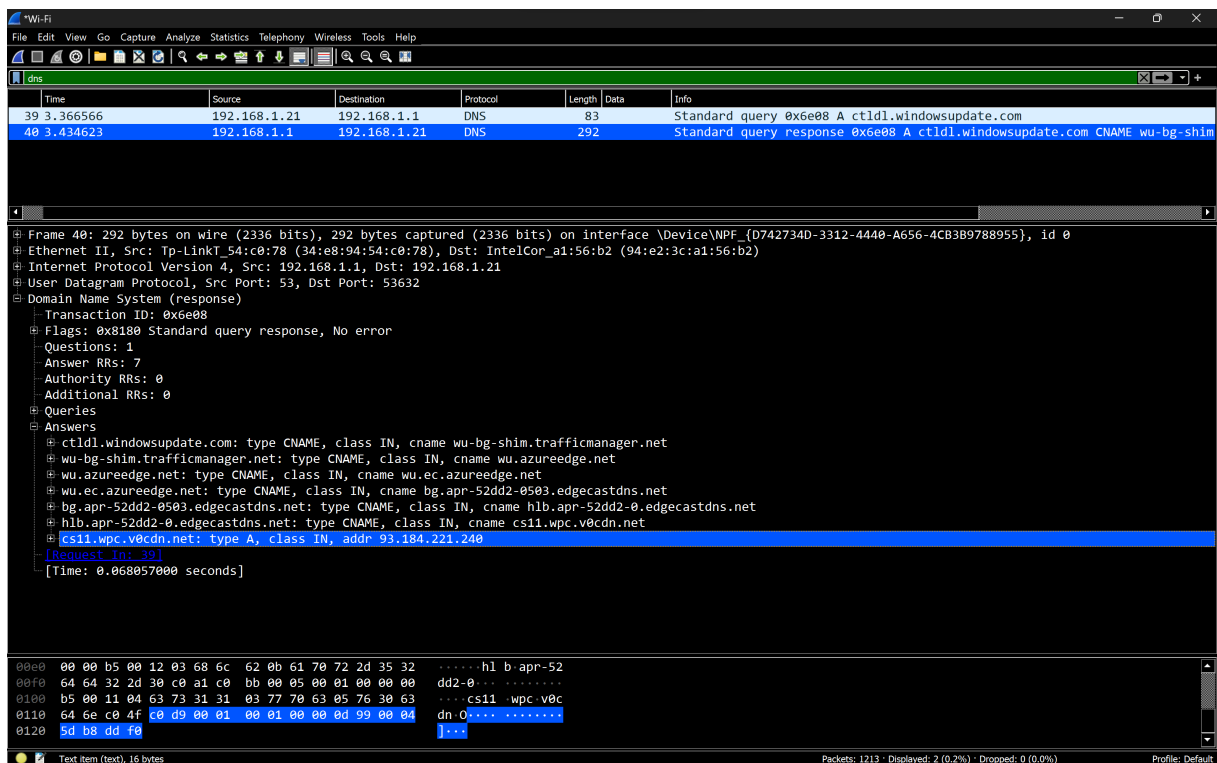
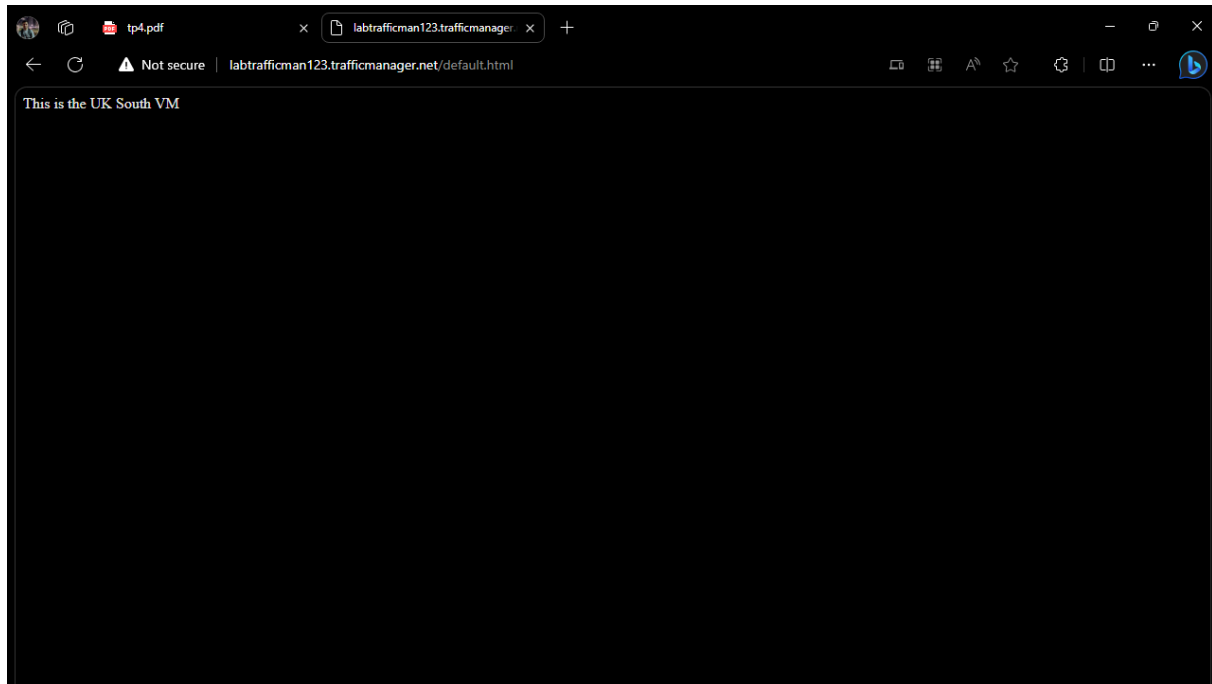
External endpoints are endpoints that are not hosted in Azure. You can add external endpoints to a Traffic Manager profile to distribute traffic to services that are hosted outside of Azure.

The screenshot shows the 'labtrafficman123 Endpoints' page in the Microsoft Azure portal. The page displays a table of endpoints for the Traffic Manager profile 'labtrafficman123'.

Name	Status	Monitor status	Type
uktmp	Enabled	Online	External endpoint
netmp	Enabled	Online	External endpoint

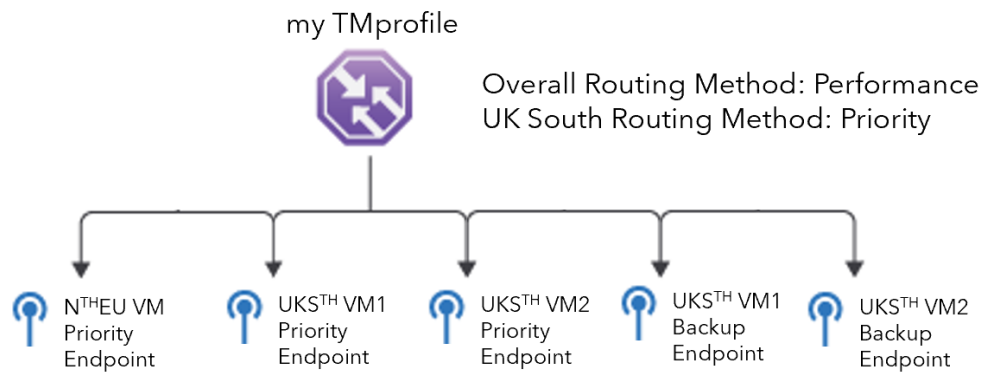
The page also includes a search bar, a '+ Add' button, and a 'Refresh' button. The left sidebar shows the 'Traffic Manager' section selected.

2.1.1.5 Requesting the Traffic Manager profile



2.1.2 Subtask 2.

Proposed Architecture with respect to the provided scenario:



2.1.3 Subtask 3.

Noted.

2.2 Task 2 • Azure Front Door

Azure Front Door is a global service that improves the performance and security of your applications. Front Door routes traffic to the optimal backend based on health, performance, and routing rules. Front Door also provides advanced security capabilities, including WAF, DDoS protection, and custom HTTPS.

2.2.1 Azure Front Door Classic Offering Set-up

Create a Front Door

⚠ Changing the Basic options may reset the selections you have made. Review all the options prior to creating the Front Door.

Basics Configuration Tags Review + create

Azure Front Door Service is Microsoft's highly available and scalable web application acceleration platform and global HTTP(S) load balancer. It provides built-in DDoS protection and application layer security and caching. Front Door enables you to build applications that maximize and automate high-availability and performance for your end-users. Use Front Door with Azure services including Web/Mobile Apps, Cloud Services and Virtual Machines – or combine it with on-premises services for hybrid deployments and smooth cloud migration. [Learn more about Front Door](#)

PROJECT DETAILS

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

Subscription *

Resource group *
[Create new](#)

Resource group location

Add a backend

← Go back to backend pool

Backends are your application servers where Front Door will route your client requests to. You can assign weights to your backends to define proportion of traffic to be sent and set priority for the backends to define active/stand-by kind of architectures. [Learn more](#)

Backend host type *

Backend host name *

Backend host header

HTTP port *

HTTPS port *

Priority *

Weight *

Status
☐ Disabled ☒ Enabled

Add

Add a backend

← Go back to backend pool

Backends are your application servers where Front Door will route your client requests to. You can assign weights to your backends to define proportion of traffic to be sent and set priority for the backends to define active/stand-by kind of architectures. [Learn more](#)

Backend host type *

Backend host name *

Backend host header

HTTP port *

HTTPS port *

Priority *

Weight *

Status
☐ Disabled ☒ Enabled

Add

The screenshot shows the Microsoft Azure portal interface for configuring a Front Door resource. The main heading is "Create a Front Door", with tabs for "Basics", "Configuration", "Tags", and "Review + create". The "Configuration" tab is active, showing a diagram of the Front Door architecture with a "Frontends/domains" section containing "myazurefrontdoor.azurefd.net" and a "Backend pools" section. A "Step 2" instruction states: "Now you can create a backend pool for your frontend connect to. Once you have a backend pool you will be able to create a routing rule." To the right, the "Add a backend pool" panel is open, providing details on how a backend pool works and a table of configured backends.

Frontends/domains

- myazurefrontdoor.azurefd.net

Backend pools

*** Step 2**
Now you can create a backend pool for your frontend connect to. Once you have a backend pool you will be able to create a routing rule.

Add a backend pool

A backend pool is a set of equivalent backends to which Front Door load balances your client requests. [Learn more](#)

Name *
mybackendpool ✓

BACKENDS

Backend host name	Status	Priority	Weight
20.13.136.85	Enabled	1	100
20.0.81.207	Enabled	1	100

+ Add a backend

HEALTH PROBES

Front Door sends periodic HTTP/HTTPS probe requests to each of your configured backends to determine the proximity and health of each backend to load balance your end user requests. [Learn more](#)

Status
Disabled Enabled

Path *
/

Protocol ⓘ
HTTP HTTPS

Probe method ⓘ
HEAD

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

Add a rule

PATTERNS TO MATCH

Set this to all the URL path patterns that this route will accept. For example, you can set this to /users/* to accept all requests on the URL www.contoso.com/users/*. [Learn more](#)

/*

/path

ROUTE DETAILS

Once a route for a Front Door is matched, the Rules Engine configuration associated with this routing rule is executed, followed by general route configuration defined below. [Learn more](#)

Route type ⓘ

Forward

Redirect

Backend pool *

mybackendpool

Forwarding protocol ⓘ

☐ HTTPS only

☐ HTTP only

☒ Match request

URL rewrite ⓘ

Enabled

Disabled

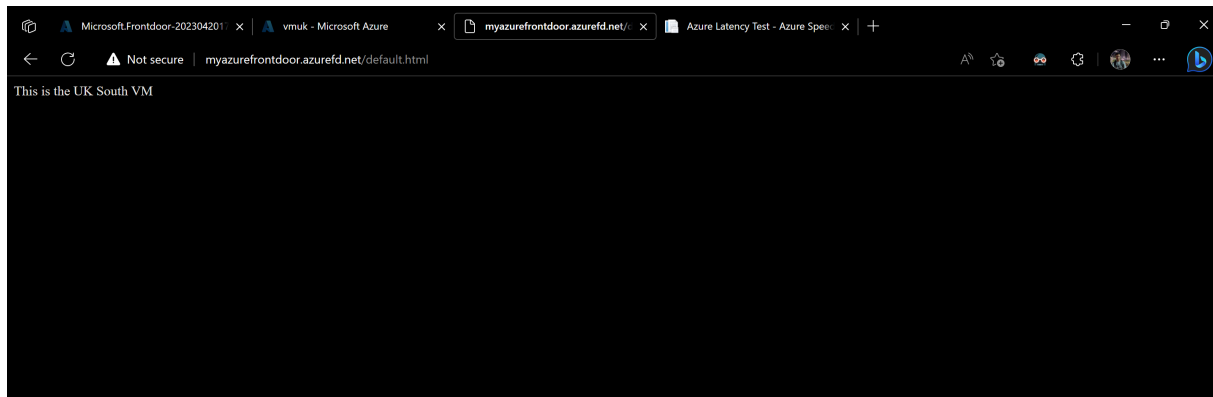
Caching ⓘ

Enabled

Disabled

Add

2.2.2 Accessing the Front Door in the browser

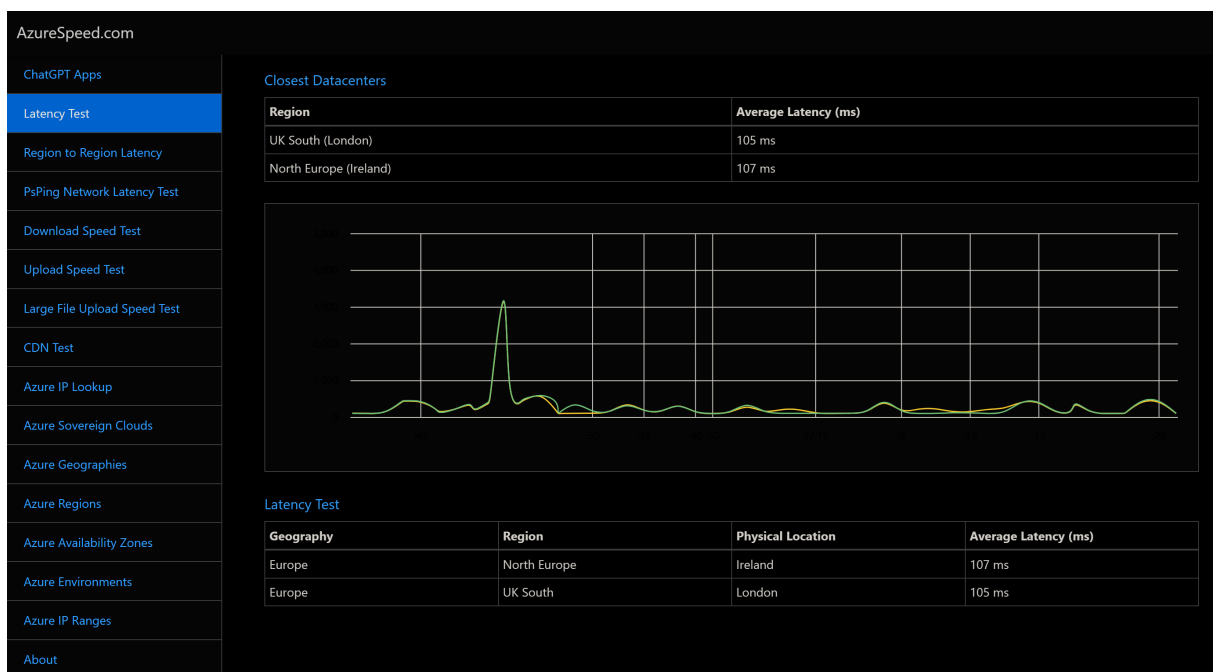


- Interpretations:

You can see here, as indicated in the lab sheet, I've got UK South (London) instead of North Europe (Ireland) and one reason for that is based on proximity to the VMs. I am based in North Tunisia and the VMs are in both in North Europe, However with a slightly lower latency for London over Ireland.

Latency refers to the time it takes for a data packet to travel from the user's device to the server and back. The lower the latency, the faster the application response time.

- Latency Test:



2.2.3 Delete Resource Group

The screenshot displays the Azure portal interface for a resource group named 'traffic-rg'. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Deployments, Security, Policies, Properties, Locks, Cost Management, Cost analysis, Cost alerts (preview), Budgets, and Advisor recommendations. The main content area is divided into 'Essentials' and 'Resources' sections. The 'Essentials' section shows the subscription 'Adam' with ID '97cd8887-e707-4ecb-8c73-4eef77a13527'. The 'Resources' section lists 14 resources, including 'labtrafficman123', 'myazurefrontdoor', 'vmna', 'vmna-ip', 'vmna-nsg', and 'vmna-vnet'. A notification banner at the top right indicates 'Deleting resource group traffic-rg' is running, with a 'Dismiss all' button.

2.3 Task 3 • Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. Azure Firewall provides stateful network traffic filtering to protect your Azure virtual network resources from common network threats. Azure Firewall is a fully stateful firewall as a service (FWaaS) that is centrally managed and can be deployed at scale.

2.3.1 Deploy a VM

The screenshot shows the Microsoft Azure portal interface. The left sidebar displays the navigation menu with 'Virtual machines' selected. The main content area shows the details for a virtual machine named 'demovm'. A warning banner at the top indicates that the virtual machine agent status is not ready. The 'Essentials' section provides key information about the VM, including its resource group, status, location, subscription, and tags. The 'Properties' section is expanded, showing details for the virtual machine and its networking configuration.

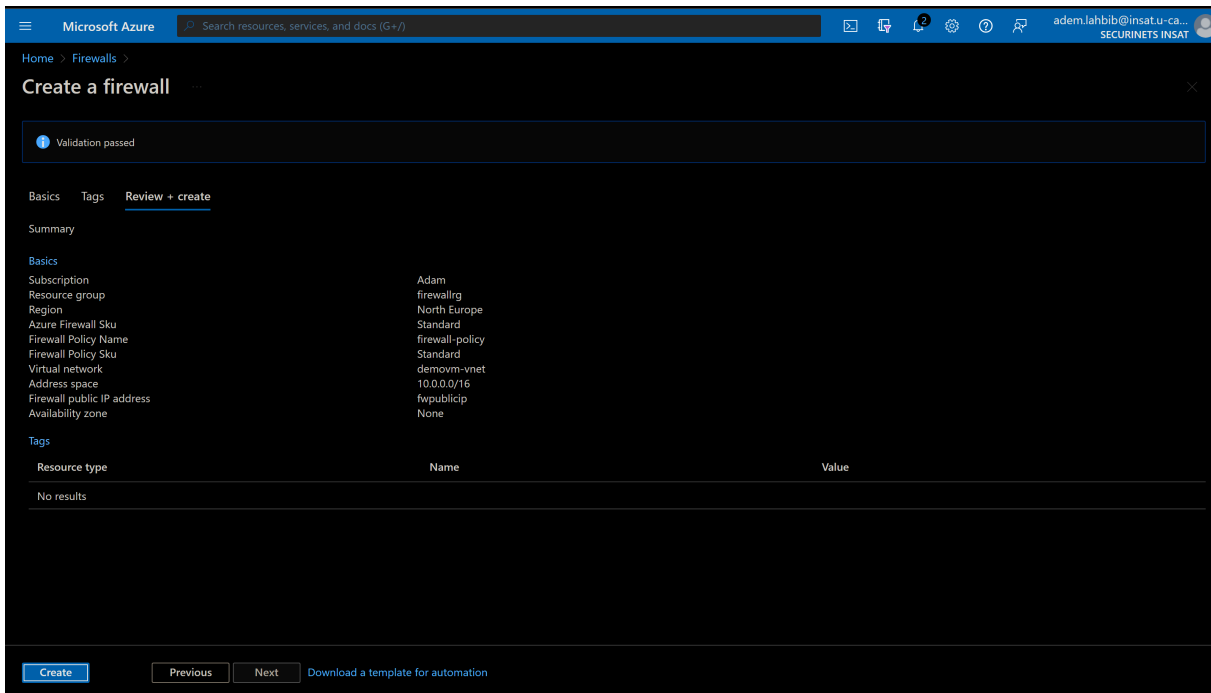
Essentials	
Resource group (move)	Operating system
FIREWALLRG	Windows
Status	Size
Running	Standard D2s v3 (2 vcpus, 8 GiB memory)
Location	Public IP address
North Europe (Zone 1)	-
Subscription (move)	Virtual network/subnet
Adam	demovm-vnet/default
Subscription ID	DNS name
97cd8887-e707-4ecb-8c73-4eef77a13527	-
Availability zone	
1	
Tags (edit)	
Click here to add tags	

Properties	
Virtual machine	Networking
Computer name	demovm
Health state	-
Operating system	Windows
Publisher	MicrosoftWindowsServer
Offer	WindowsServer
	Public IP address
	-
	Public IP address (IPv6)
	-
	Private IP address
	10.0.0.4
	Private IP address (IPv6)
	-

The screenshot shows the 'Add subnet' dialog in the Microsoft Azure portal. The dialog is for the 'demovm-vnet' virtual network. It allows adding a new subnet. The 'Name' field is set to 'AzureFirewallSubnet'. The 'Subnet address range' is set to '10.0.1.0/24'. The 'Add IPv6 address space' checkbox is unchecked. The 'NAT gateway' is set to 'None'. The 'Network security group' is set to 'None'. The 'Route table' is set to 'None'. The 'SERVICE ENDPOINTS' section is empty. The 'SUBNET DELEGATION' section is also empty. The 'Save' button is highlighted.

Name	IPv4	IPv6	Available IPs
default	10.0.0.0/24	-	250

2.3.2 Create a Firewall



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

Home > Firewalls >

Create a firewall

Validation passed

Basics Tags **Review + create**

Summary

Basics

Subscription	Adam
Resource group	firewallrg
Region	North Europe
Azure Firewall SKU	Standard
Firewall Policy Name	firewall-policy
Firewall Policy SKU	Standard
Virtual network	demovm-vnet
Address space	10.0.0.0/16
Firewall public IP address	fwpublicip
Availability zone	None

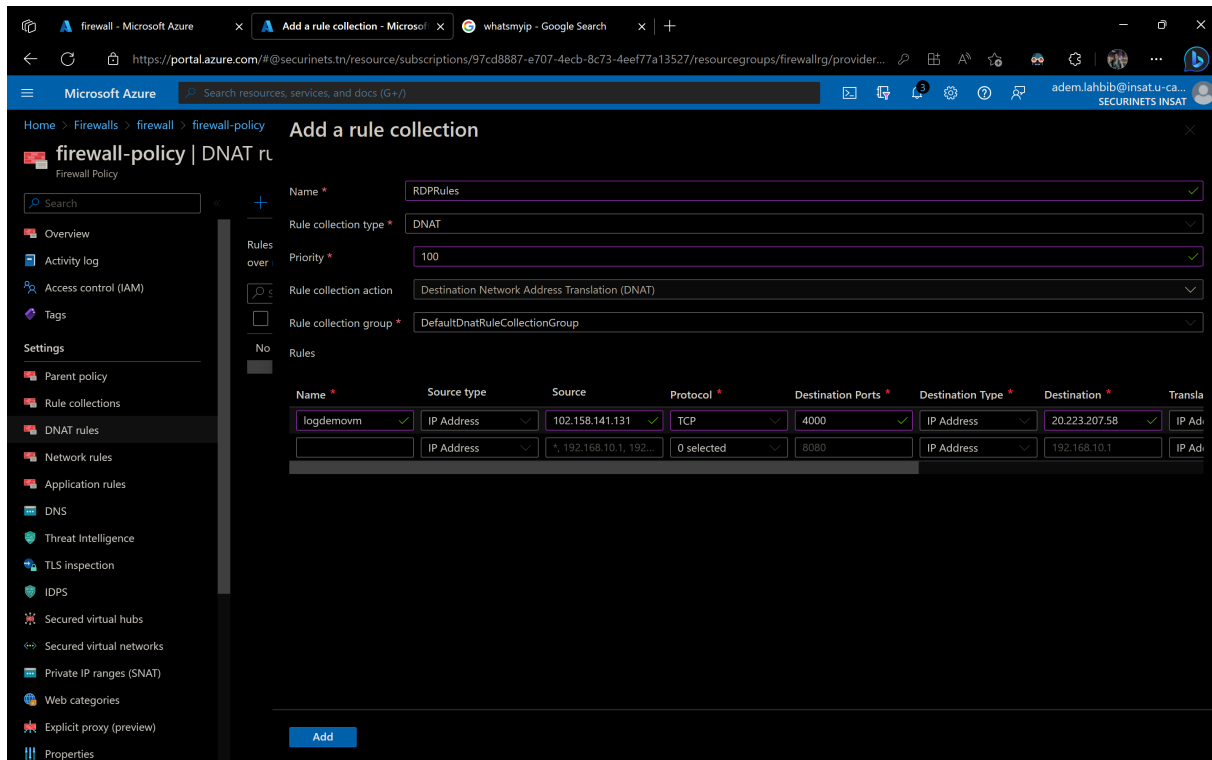
Tags

Resource type	Name	Value
No results		

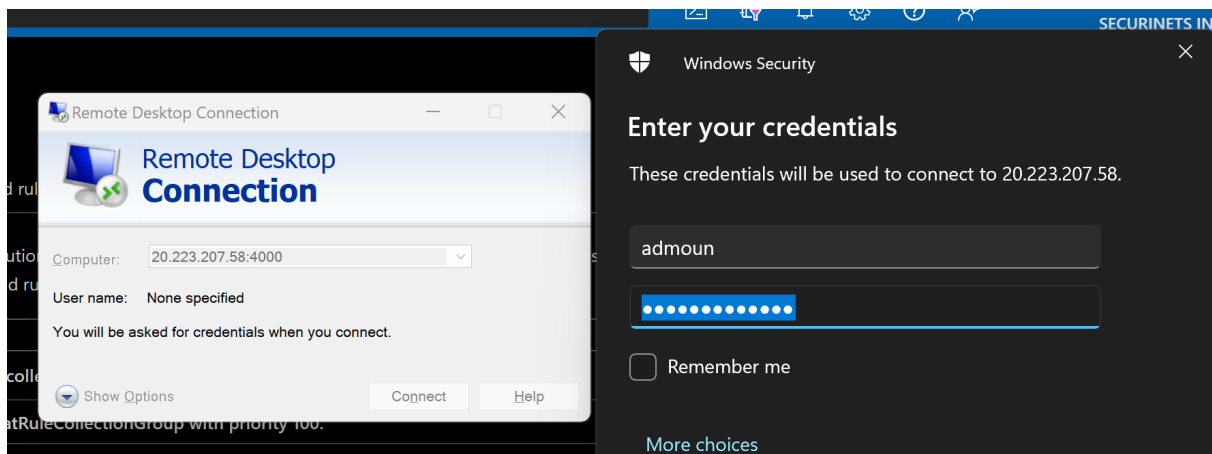
Create Previous Next Download a template for automation

2.3.3 Add DNAT Rules

DNAT rules are used to translate a public IP address and port to a private IP address and port. This is useful for scenarios where you want to expose a service that is running on a private IP address to the internet.

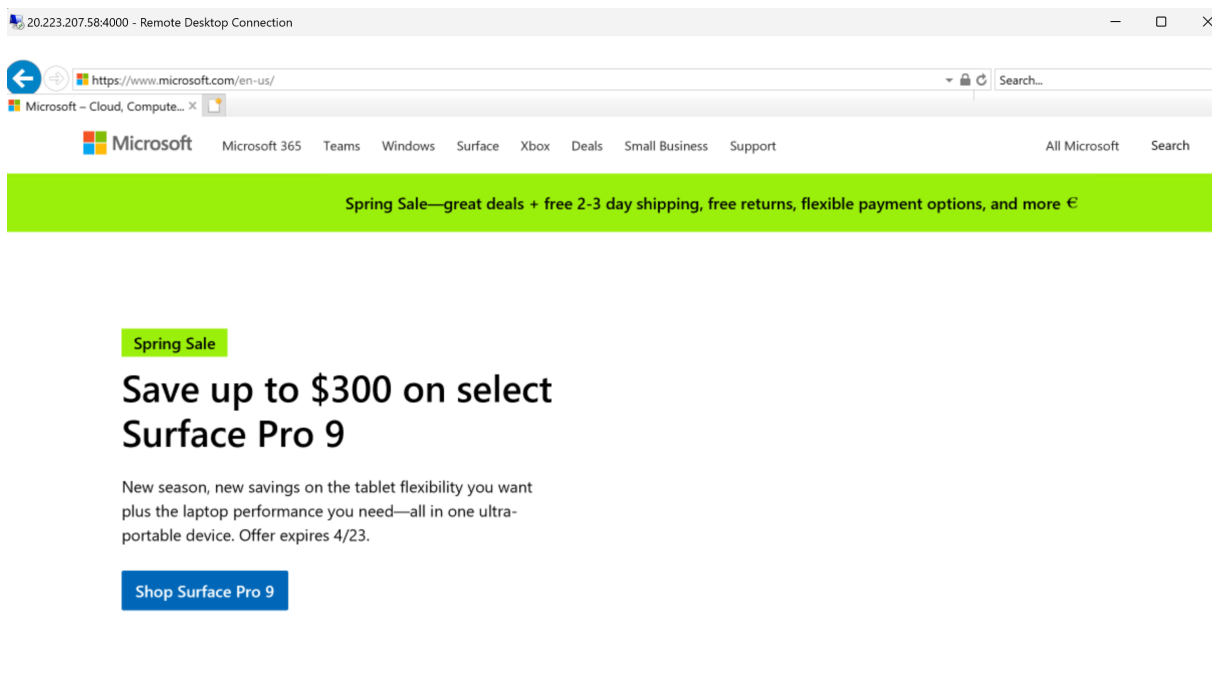


2.3.4 Testing DNAT Translation



Okay, that worked! Great!

2.3.5 Access Microsoft dot com



2.3.6 Create new route table

A route table contains a set of rules, called routes, that are used to determine where network traffic from your virtual network or subnet will be directed. You can associate a route table with one or more subnets, and thus control the routing for traffic destined for the subnet's network address space.

Microsoft Azure

Search resources, services, and docs (G+ /)

adem.lahbib@insat.u-ca...
SECURINETS INSAT

Home > Route tables >

Create Route table

Validation Passed

BasicsTagsReview + create

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	Adam
Resource group	firewallrg
Region	North Europe
Name	firewallroutetable
Propagate gateway routes	Yes

Create

< Previous

Next

Download a template for automation

2.3.7 Associate the route table with the subnet

The screenshot shows the Azure portal interface for configuring a subnet. On the left, the navigation pane is open, showing the 'Subnets' section under the 'Settings' tab for the virtual network 'demovm-vnet'. The main pane displays a table of subnets with two entries: 'default' (10.0.0.0/24) and 'AzureFirewallSubnet' (10.0.1.0/24). The 'default' subnet is selected, and its configuration details are shown on the right. The 'Route table' dropdown is set to 'firewallroutetable'. Other settings include 'Subnet address range' (10.0.0.0/24), 'NAT gateway' (None), 'Network security group' (None), and 'Service endpoints' (0 selected). The 'SUBNET DELEGATION' section shows 'Delegate subnet to a service' set to 'None'. The 'Save' button is highlighted in blue.

Name	IPv4
default	10.0.0.0/24
AzureFirewallSubnet	10.0.1.0/24

default
demovm-vnet

Name: default

Subnet address range: 10.0.0.0/24 (10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses))

☐ Add IPv6 address space

NAT gateway: None

Network security group: None

Route table: firewallroutetable

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

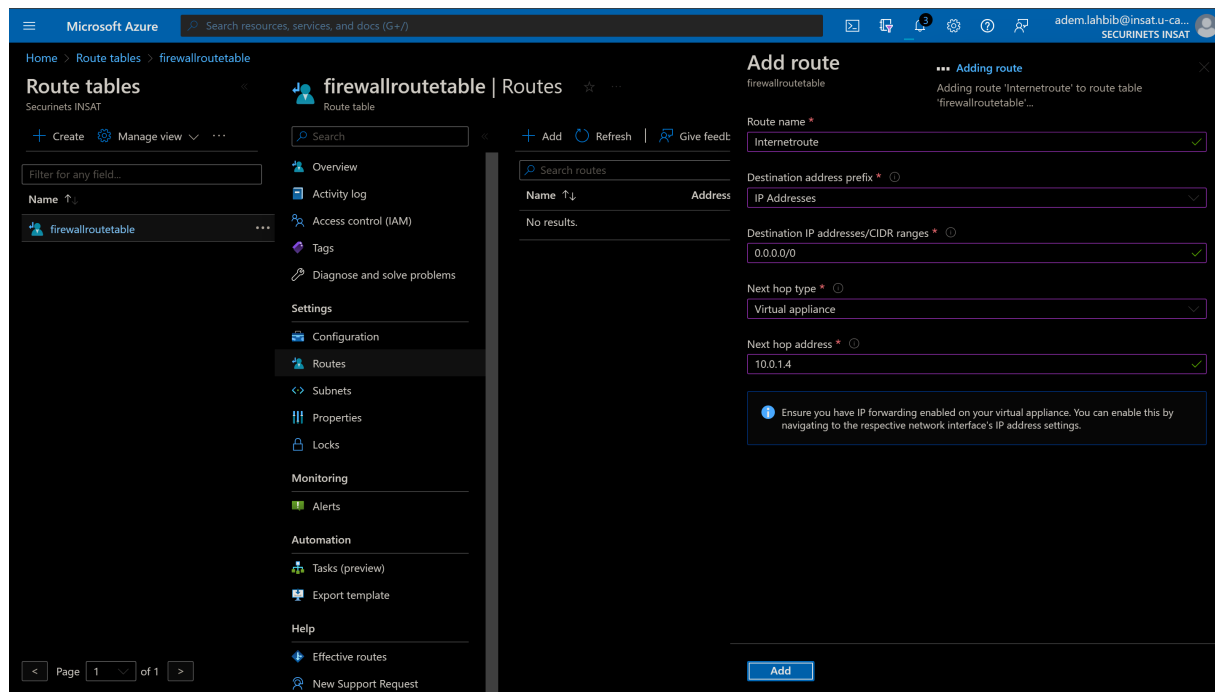
Services: 0 selected

SUBNET DELEGATION

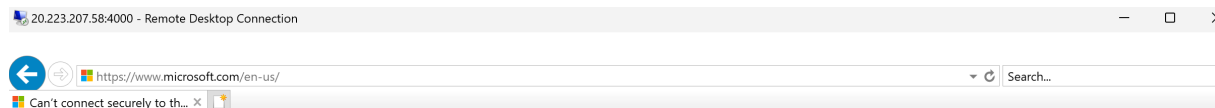
Delegate subnet to a service: None

Save **Cancel**

- Go to routes and add a route:



2.3.8 Can you access Microsoft dot com now?



Can't connect securely to this page

This might be because the site uses outdated or unsafe TLS security settings. If this keeps happening, try contacting the website's owner.

Try this:

- [Go back to the last page](#)

Denied!

2.3.9 Create an Application Rule

Application rules are used to allow or deny traffic based on the application layer protocol. For example, you can create an application rule to allow traffic to a specific port, or to a specific application.

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

Home > Firewalls > firewall > firewall-policy

firewall-policy | Application

Search

Overview

Activity log

Access control (IAM)

Tags

Settings

Parent policy

Rule collections

DNAT rules

Network rules

Application rules

DNS

Threat Intelligence

TLS inspection

IDPS

Secured virtual hubs

Secured virtual networks

Private IP ranges (SNAT)

Web categories

Explicit proxy (preview)

Properties

Add a rule collection

Name * AllowSites

Rule collection type * Application

Priority * 100

Rule collection action Allow

Rule collection group * DefaultApplicationRuleCollectionGroup

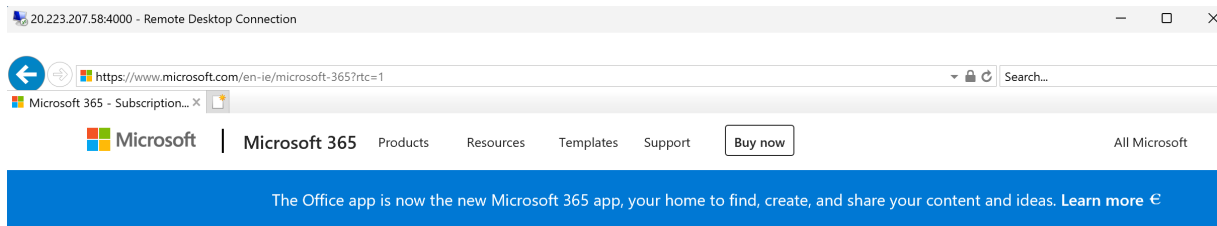
No Rules

Name *	Source type	Source	Protocol *	TLS inspection	Destination Type *	Destination *
allowmicrosoft	IP Address	10.0.0.4	http.https	<input checked="" type="checkbox"/> TLS inspection	FQDN	www.microsoft.co...
	IP Address	* 192.168.10.1, 192...	http.https.mssql...	<input checked="" type="checkbox"/> TLS inspection	FQDN	*.microsoft.com*

mssql: SQL should be enabled in proxy mode. This may require additional configuration. [Learn more](#)

Add

2.3.10 Try Microsoft dot com again?



Office is now Microsoft 365

Boost productivity with
Microsoft Teams, Word,
Excel, PowerPoint, and
more—all in one place

[Personal and family](#)[Business](#)

Works!

2.3.11 Add a network rule collection

Network rule collections are used to allow or deny traffic based on the source IP address, destination IP address, and destination port. For example, you can create a network rule collection to allow traffic from a specific IP address to a specific port.

The screenshot shows the 'Add a rule collection' dialog in the Microsoft Azure portal. The dialog is for a Firewall Policy named 'firewall-policy'. The 'Rule collection type' is set to 'Network'. The 'Priority' is 100, and the 'Rule collection action' is 'Allow'. The 'Rule collection group' is 'DefaultNetworkRuleCollectionGroup'. Below these fields, there is a table of rules. The first rule is named 'AllowDNS' and has the following details:

Name	Source type	Source	Protocol	Destination Ports	Destination Type	Destination
AllowDNS	IP Address	10.0.0.4	Any	53	IP Address	8.8.8.8
	IP Address	* 192.168.10.1, 192...	0 selected	80,8000-9000	IP Address	* 10.0.0.1, 10.1.0.0/1...

The 'Add' button is at the bottom right of the dialog.

2.3.12 Delete resource group

The screenshot shows the 'Delete resource group' dialog in the Microsoft Azure portal. The dialog is for a resource group named 'firewalling'. The 'Warning!' message states: 'Deleting the "firewalling" resource group is irreversible. The action you're about to take can't be undone. Going further will delete this resource group and all the resources in it permanently.' The 'Apply force delete for selected Virtual machines and Virtual machine scale sets' checkbox is checked. The 'TYPE THE RESOURCE GROUP NAME:' field contains 'firewalling'. Below this, a table lists the resources that will be deleted:

Name	Type	Location
demovm	Virtual machine	North Europe
demovm_OsDisk_1_f79f38a6015...	Disk	North Europe
demovm75_z1	Network interface	North Europe
demovm-nsg	Network security gr...	North Europe
demovm-vnet	Virtual network	North Europe
firewall	Firewall	North Europe
firewall-policy	Firewall Policy	North Europe
firewallroutetable	Route table	North Europe
twpublicip	Public IP address	North Europe

The 'Delete' button is at the bottom right of the dialog.