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

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.

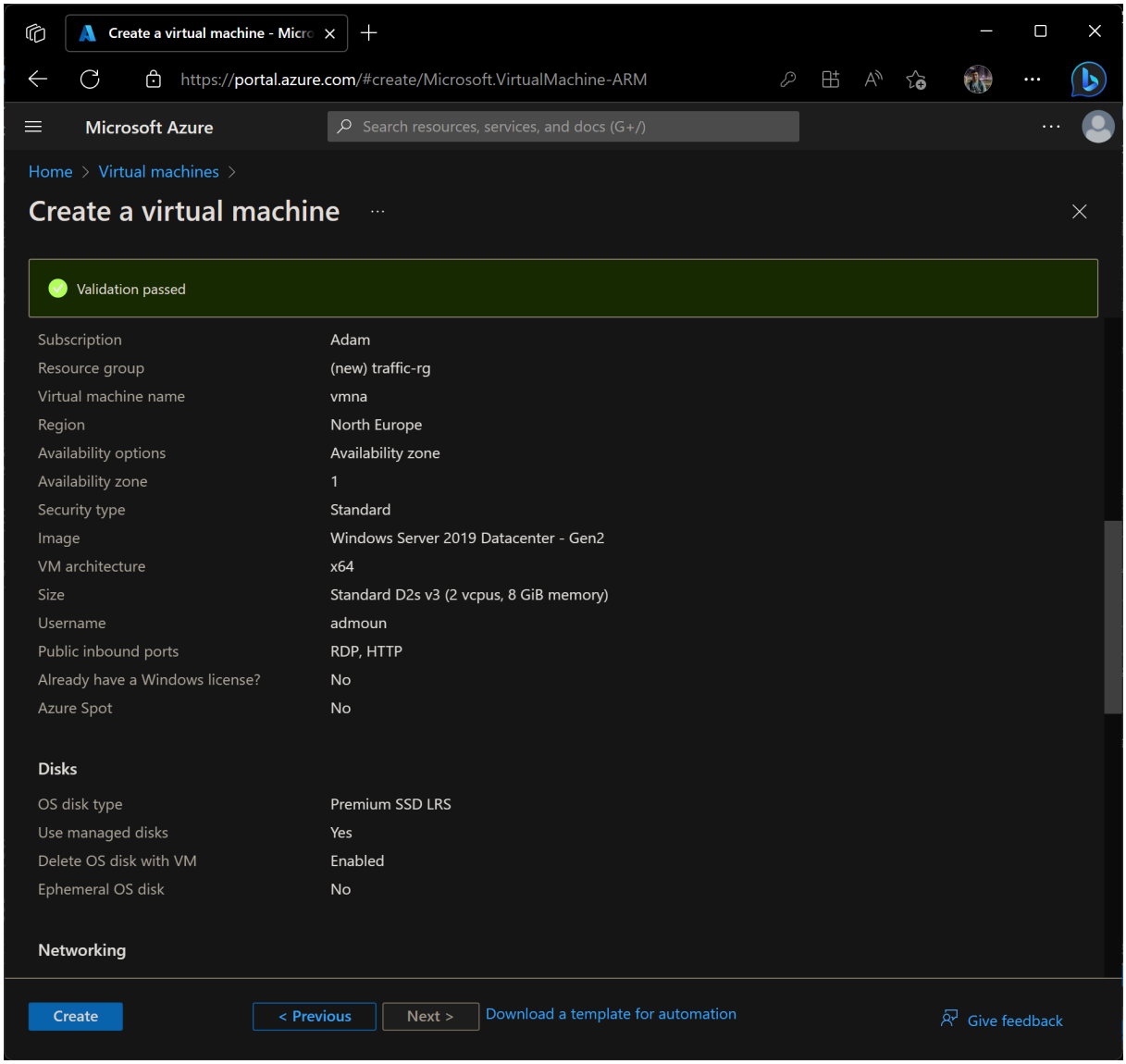
2 Lab Walkthrough

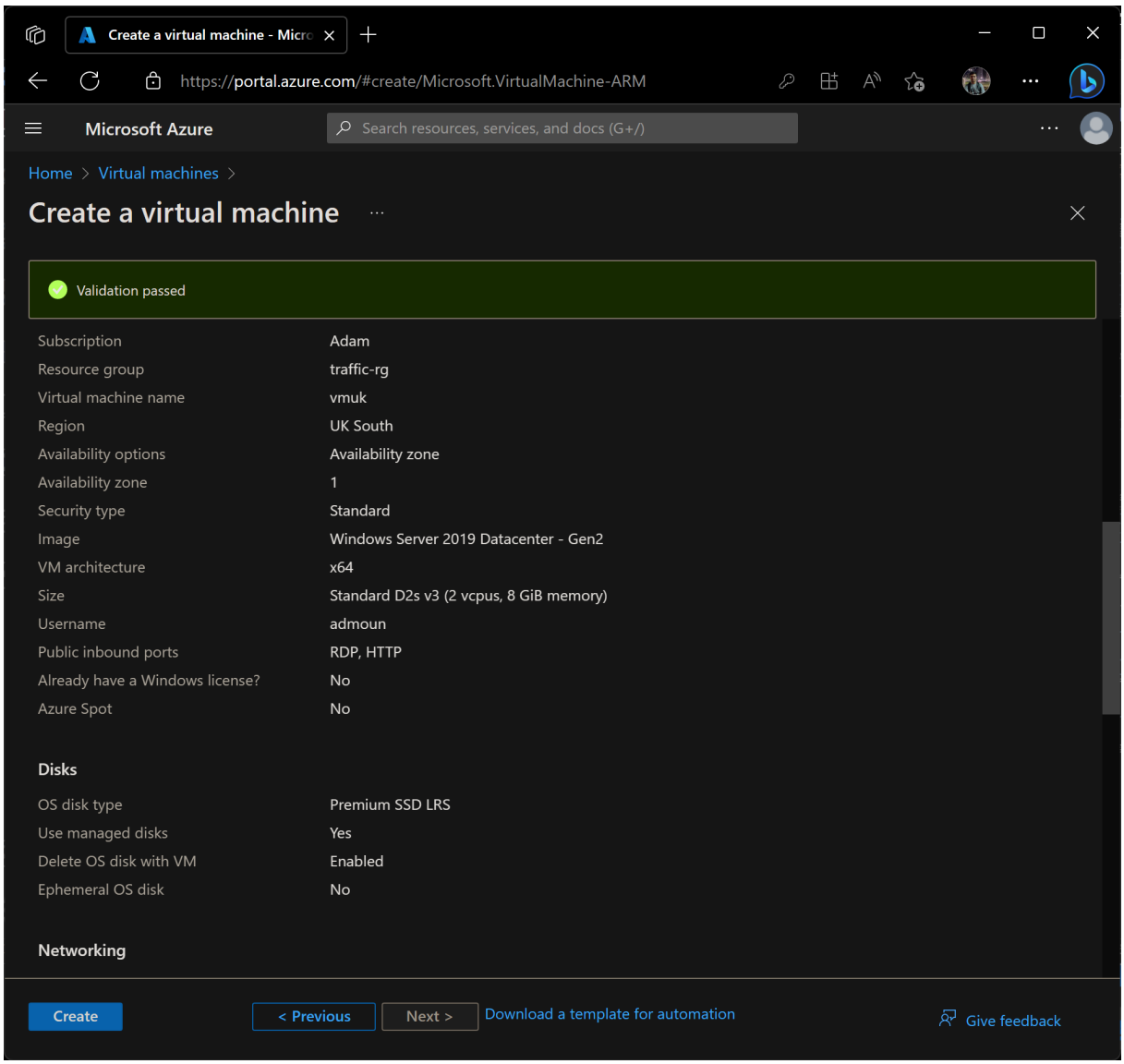
2.1 Task 1 · Azure Traffic Manager Profile

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

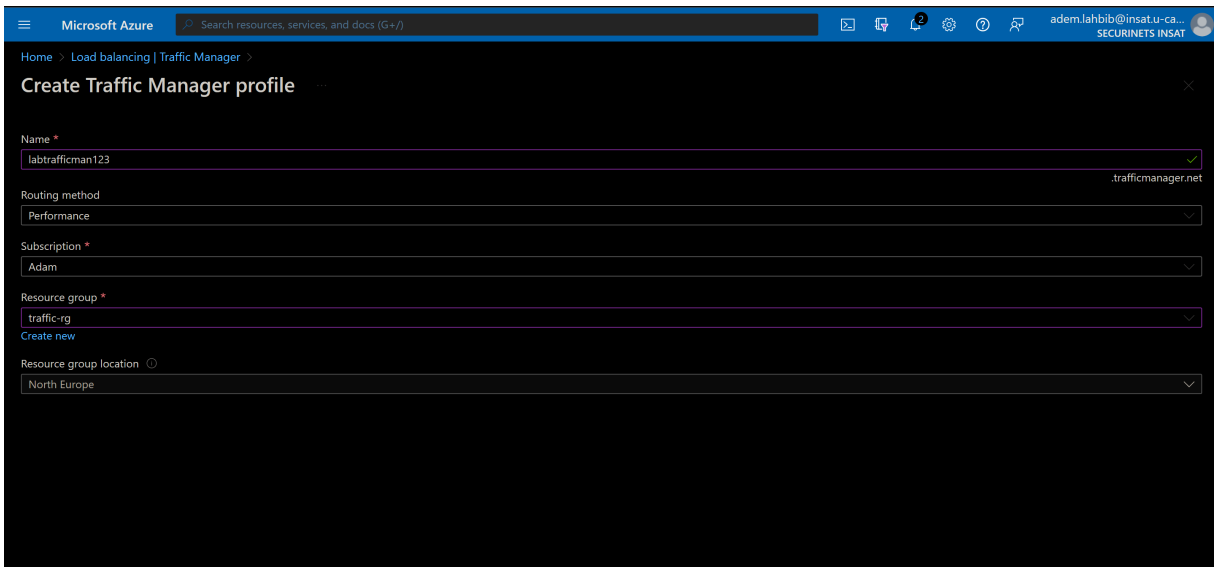



Create a virtual machine - Micro
https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual machines >
Create a virtual machine
Validation passed
Subscription Adam
Resource group traffic-rg
Virtual machine name vmuk
Region UK 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

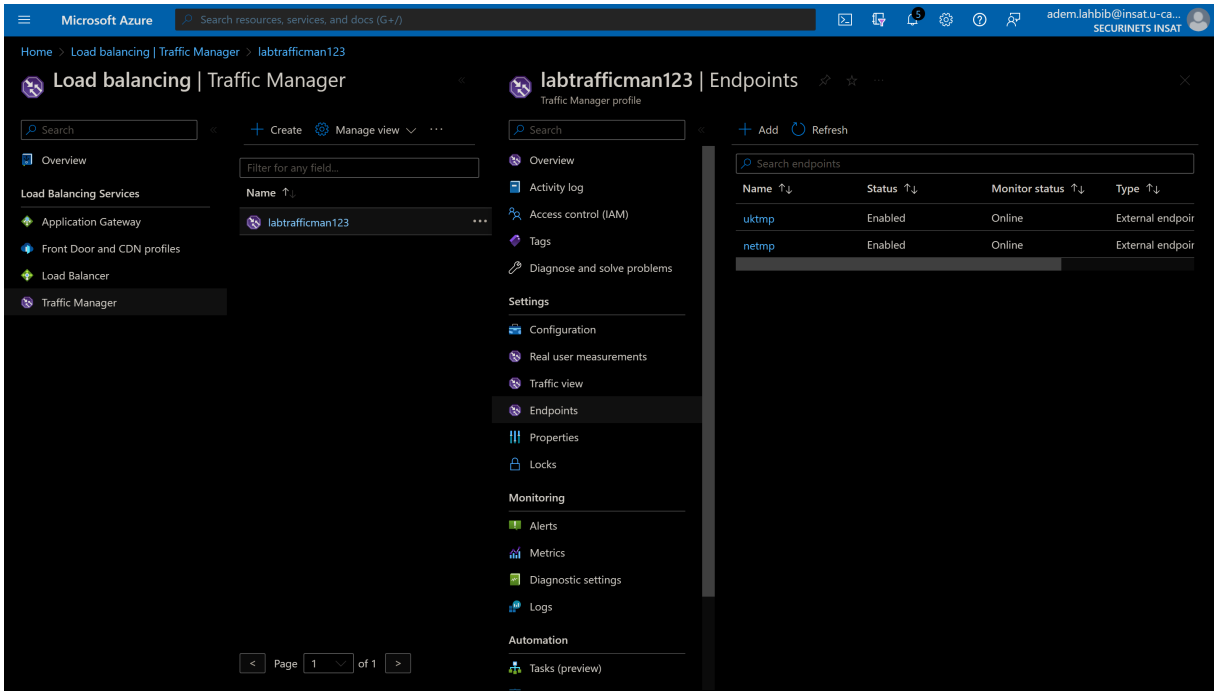
2.1.1.3 Create Traffic Manager Profile

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.

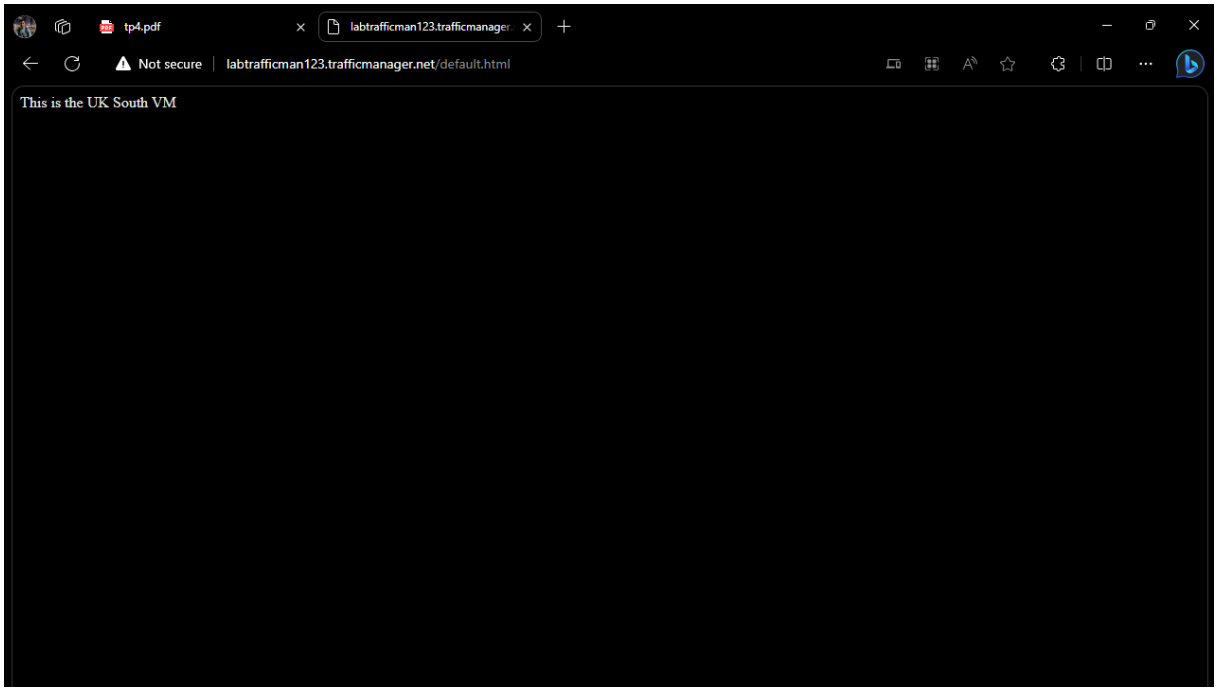


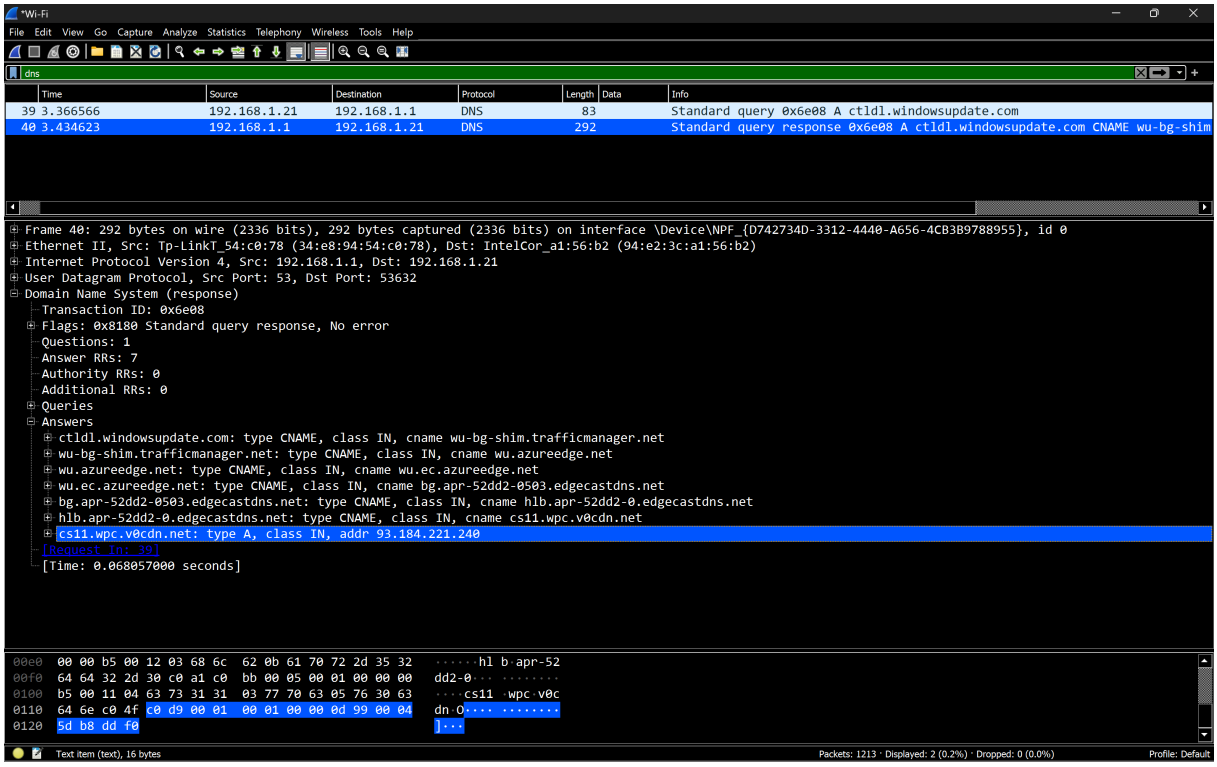
2.1.1.4 Add VMs as external endpoints

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.



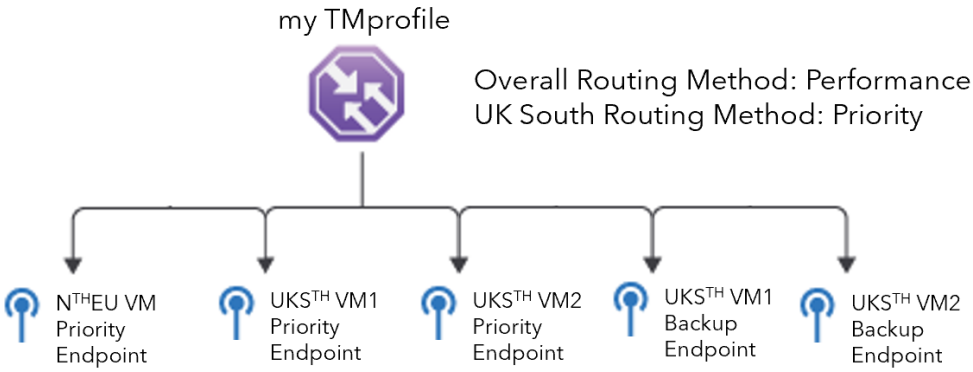
2.1.1.5 Requesting the Traffic Manager profile





2.1.2 Subtask 2.

Proposed Architecture with respect to the provided scenario:



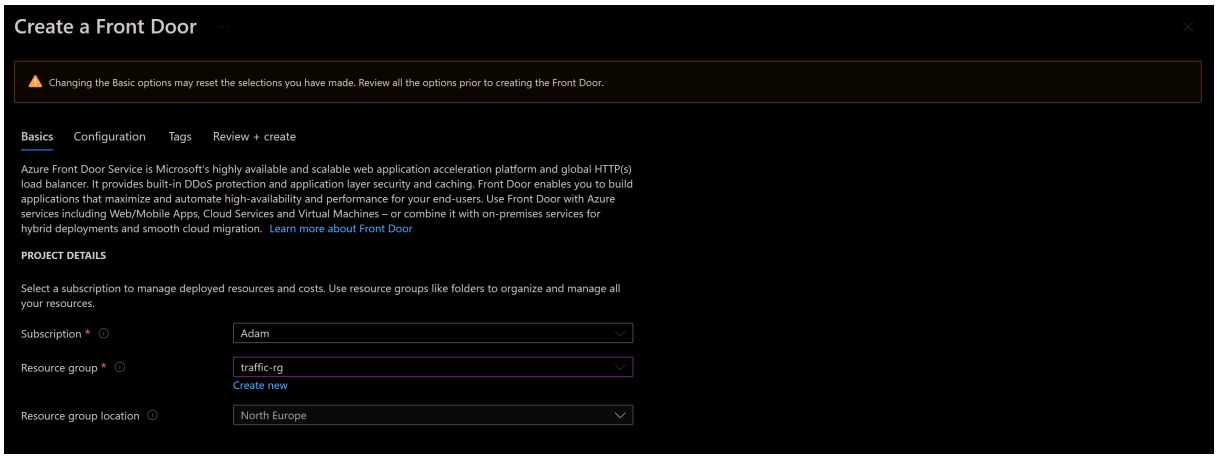
2.1.3 Subtask 3.

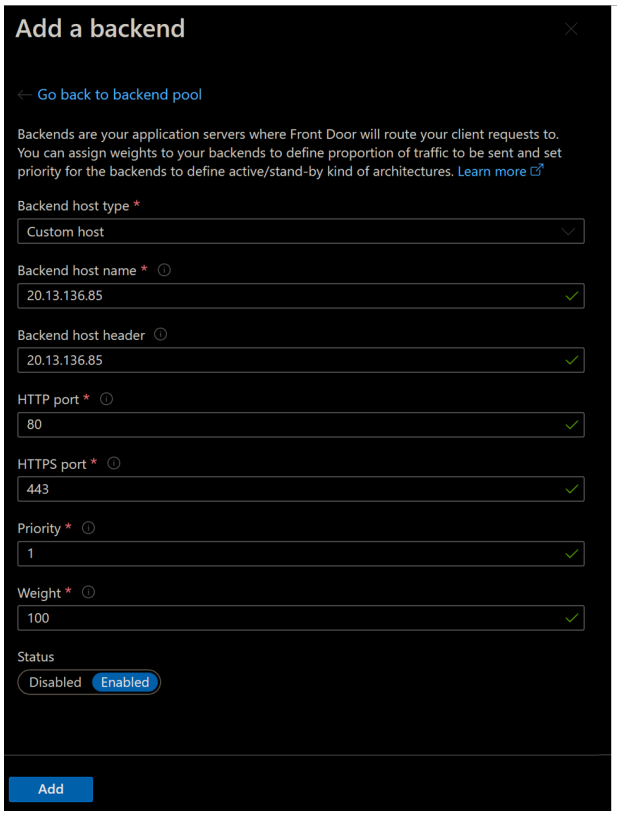
Noted.

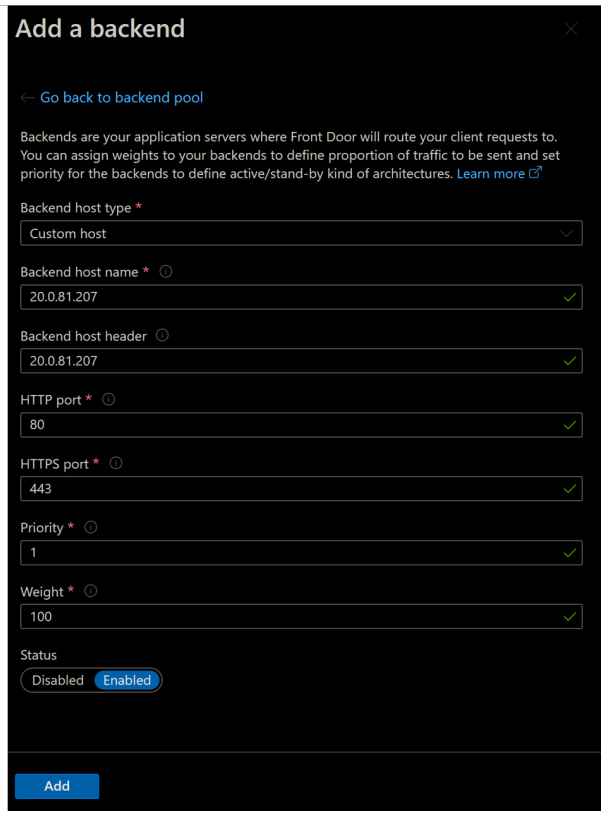
2.2 Task 2 · Azure Front Door

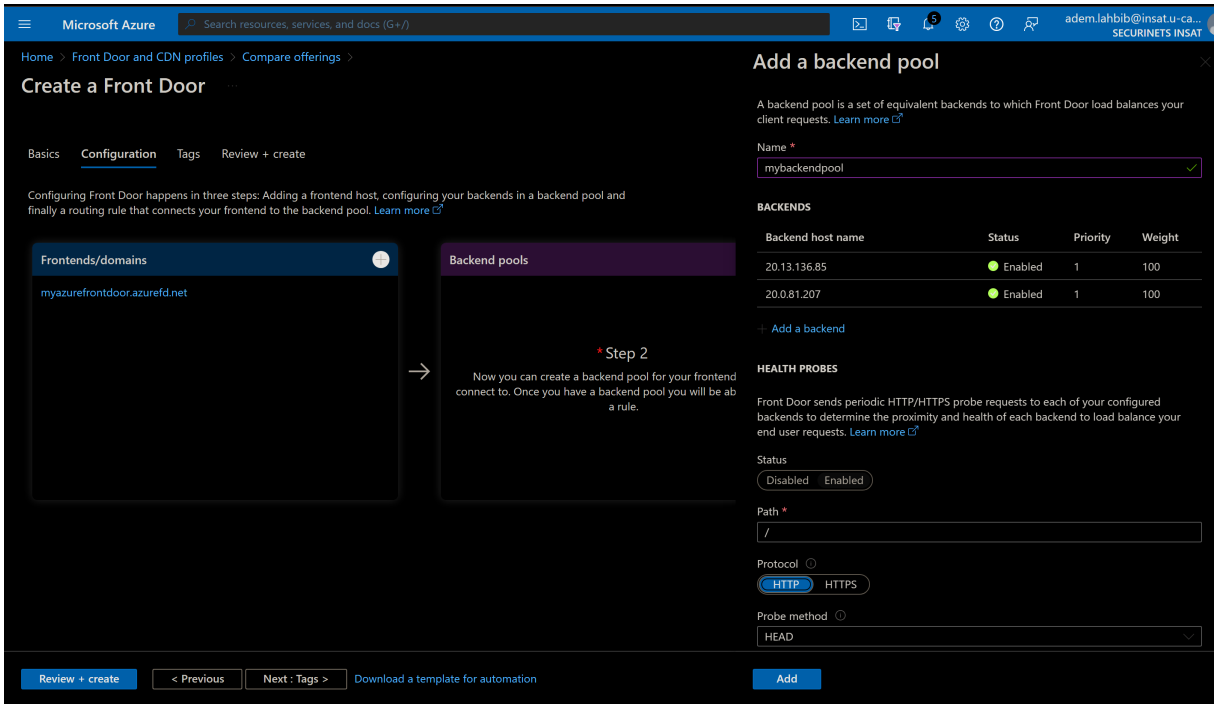
Azure Front Door is a global service that improves the performance and security of your applications. Front Door routes traffic to the optimal backend based on health, performance, and routing rules. Front Door also provides advanced security capabilities, including WAF, DDoS protection, and custom HTTPS.

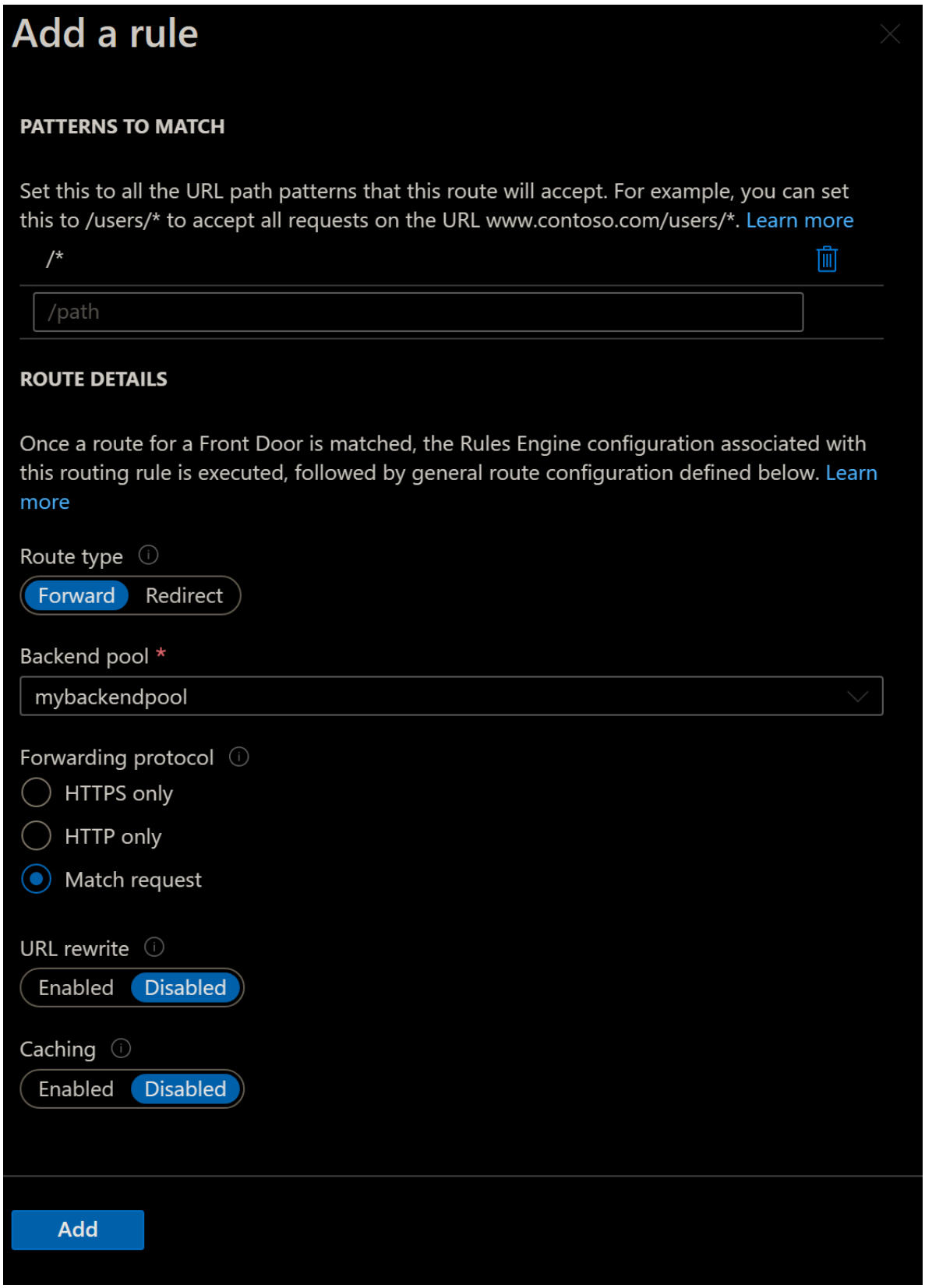
2.2.1 Azure Front Door Classic Offering Set-up



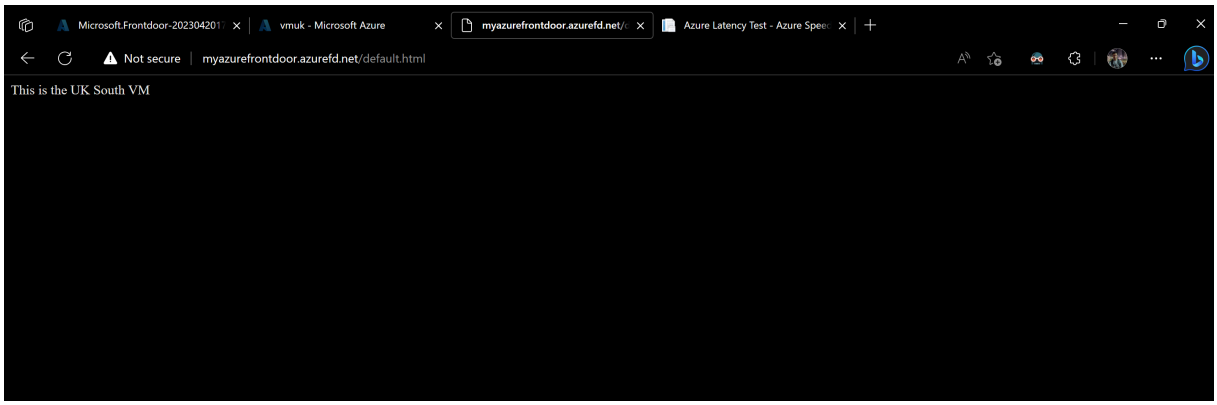





Microsoft Azure
Search resources, services, and docs (G+/)
adem.lahbib@insat.u-ca...
SECURINETS INSAT
Home > Front Door and CDN profiles > Compare offerings >
Create a Front Door
Basics
Configuration
Tags
Review + create
Configuring Front Door happens in three steps: Adding a frontend host, configuring your backends in a backend pool and finally a routing rule that connects your frontend to the backend pool. Learn more
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 ab a rule.
Review + create
< Previous
Next : Tags >
Download a template for automation
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
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

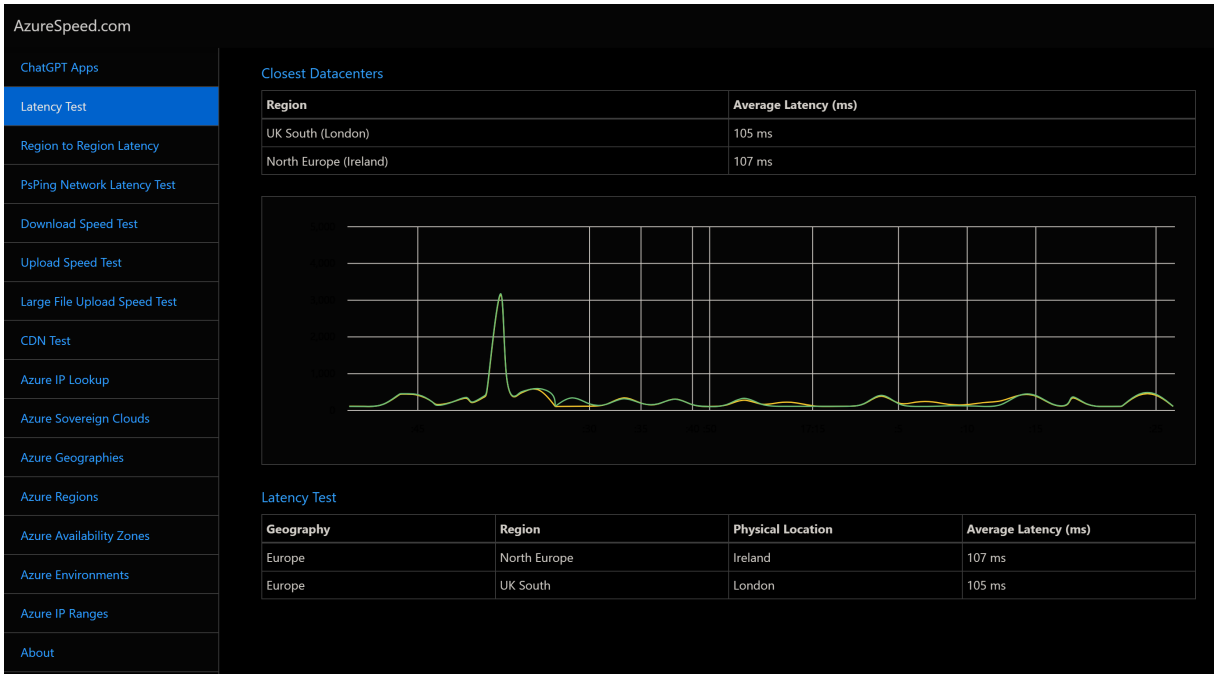


- Interpretations:

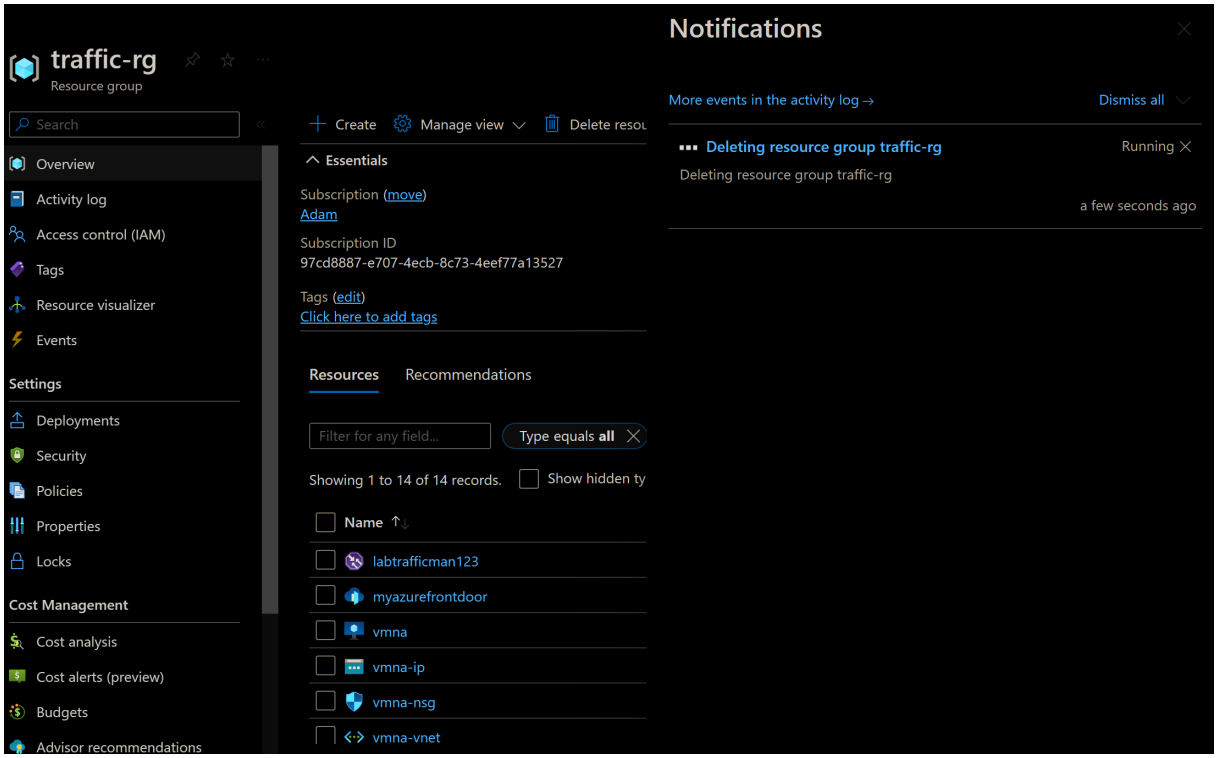
You can see here, as indicated in the lab sheet, I've got UK South (London) instead of North Europe (Ireland) and one reason for that is based on proximity to the VMs. I am based in North Tunisia and the VMs are in both in North Europe, However with a slightly lower latency for London over Ireland.

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:



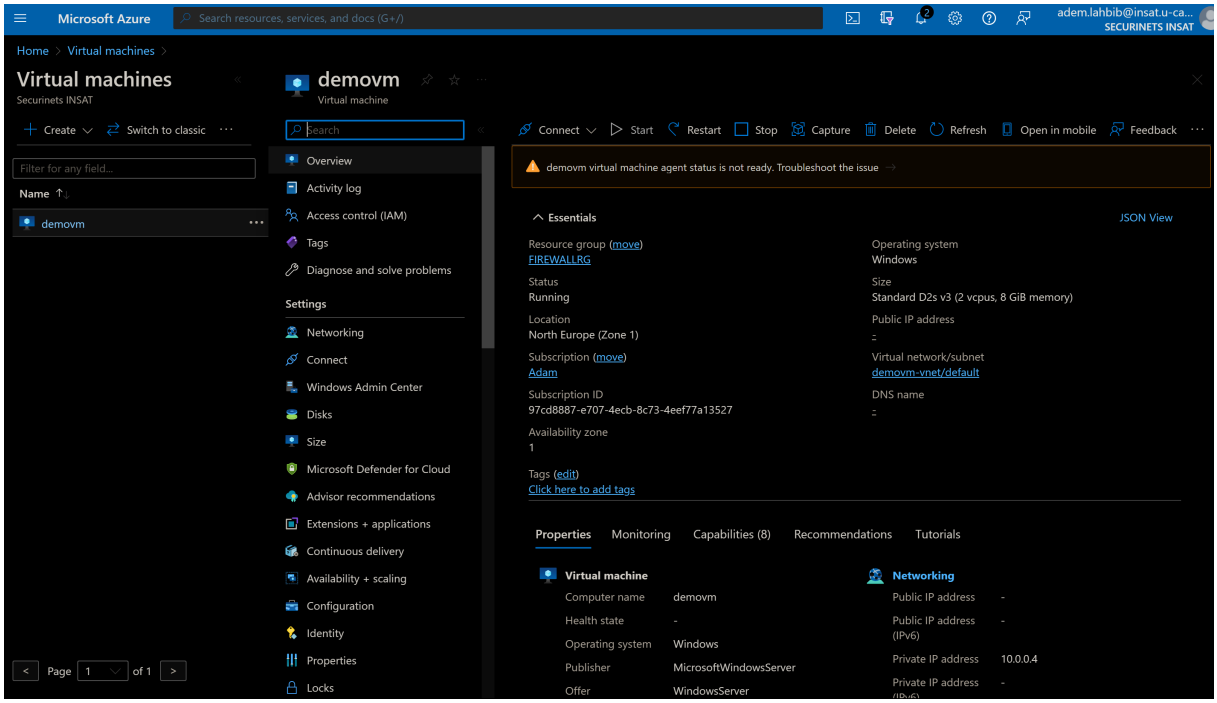
2.2.3 Delete Resource Group

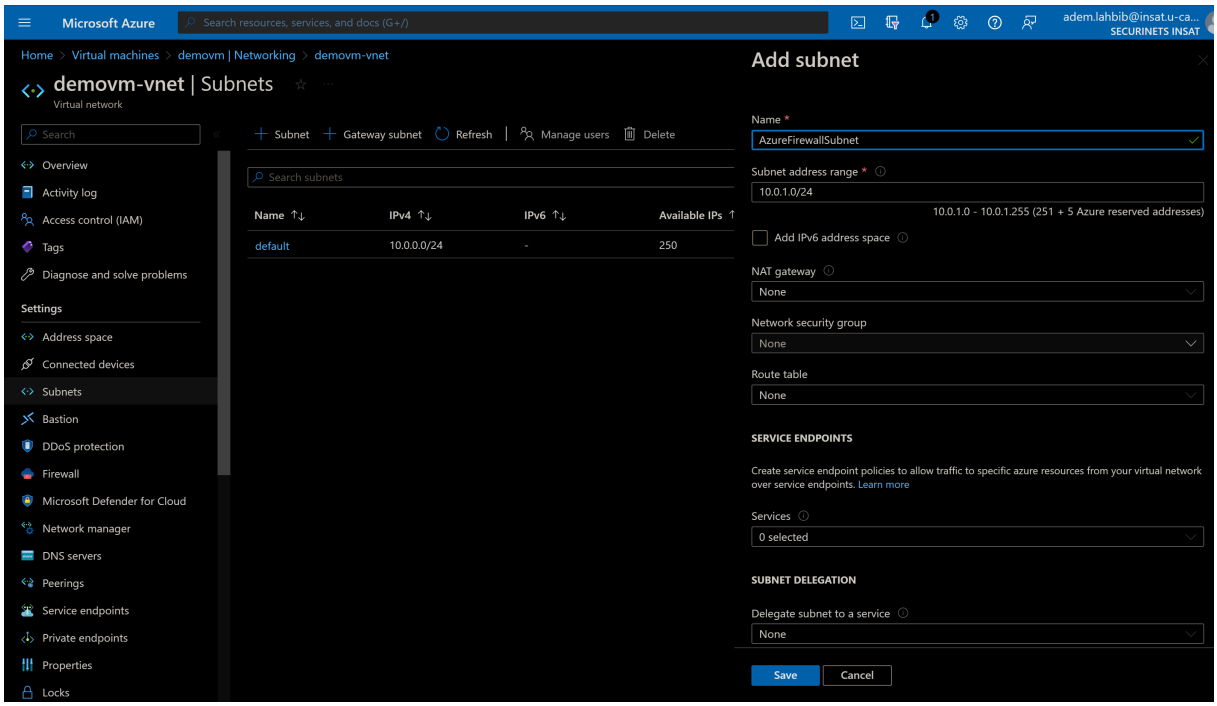


2.3 Task 3 · Azure Firewall

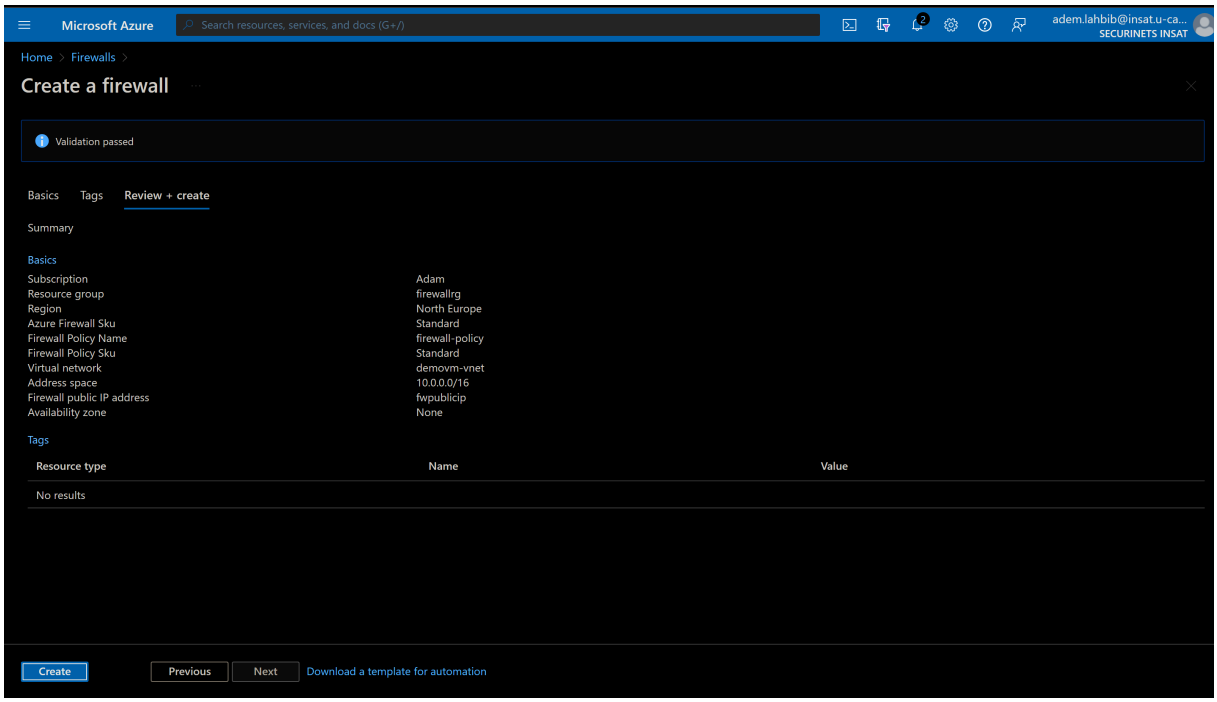
Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. Azure Firewall provides stateful network traffic filtering to protect your Azure virtual network resources from common network threats. Azure Firewall is a fully stateful firewall as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

2.3.1 Deploy a VM



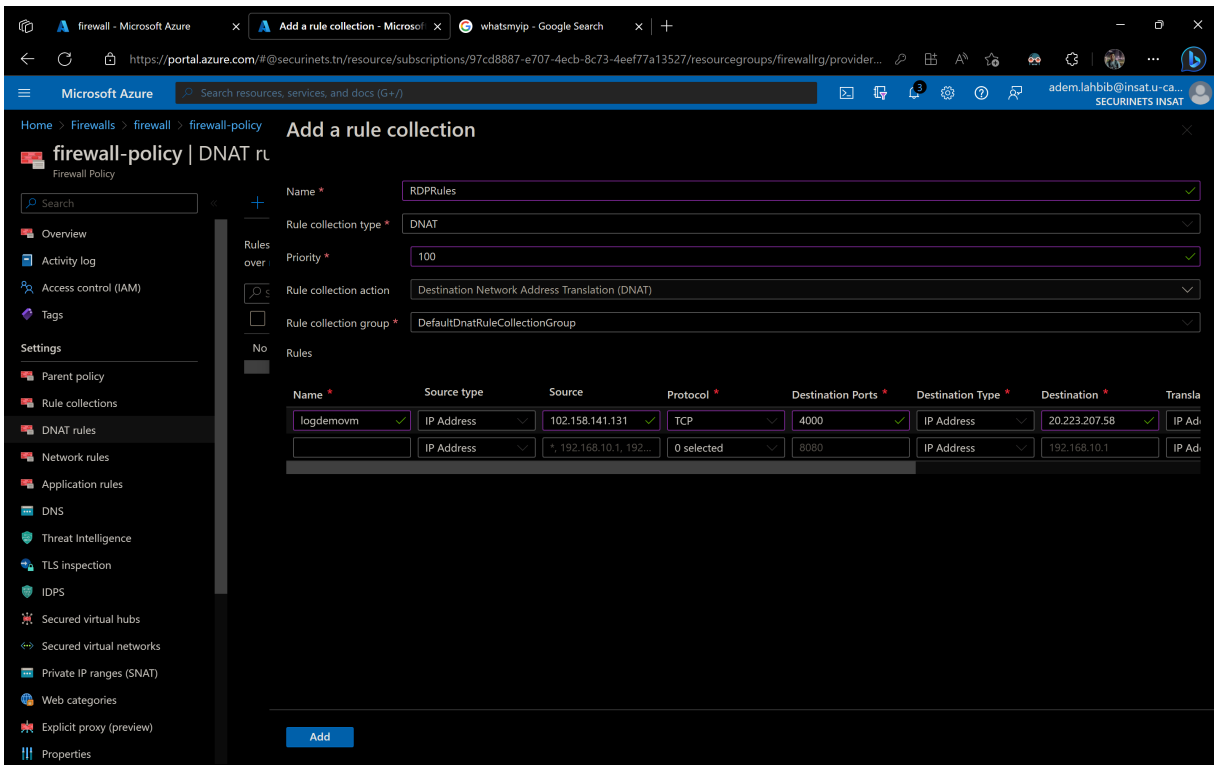


2.3.2 Create a Firewall

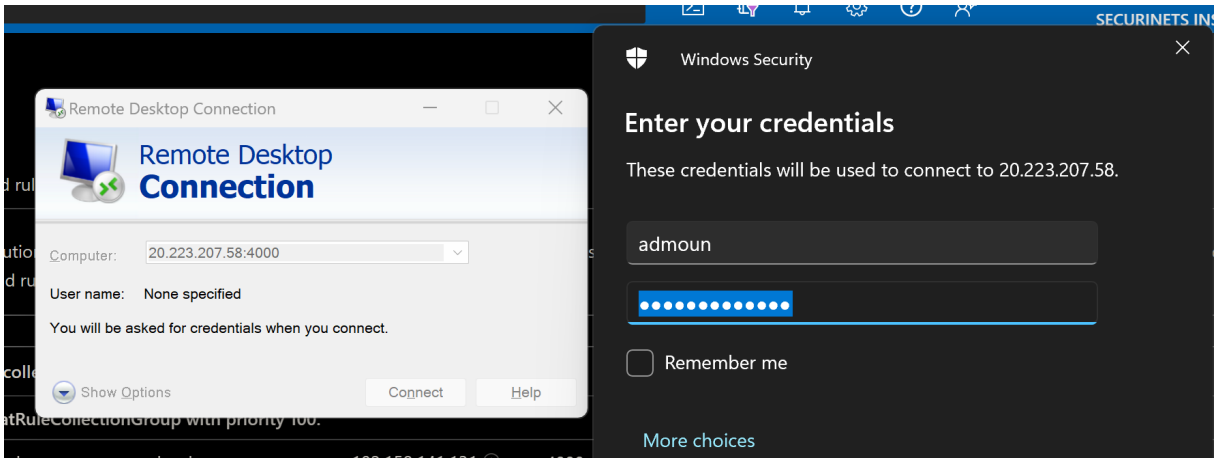


2.3.3 Add DNAT Rules

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.

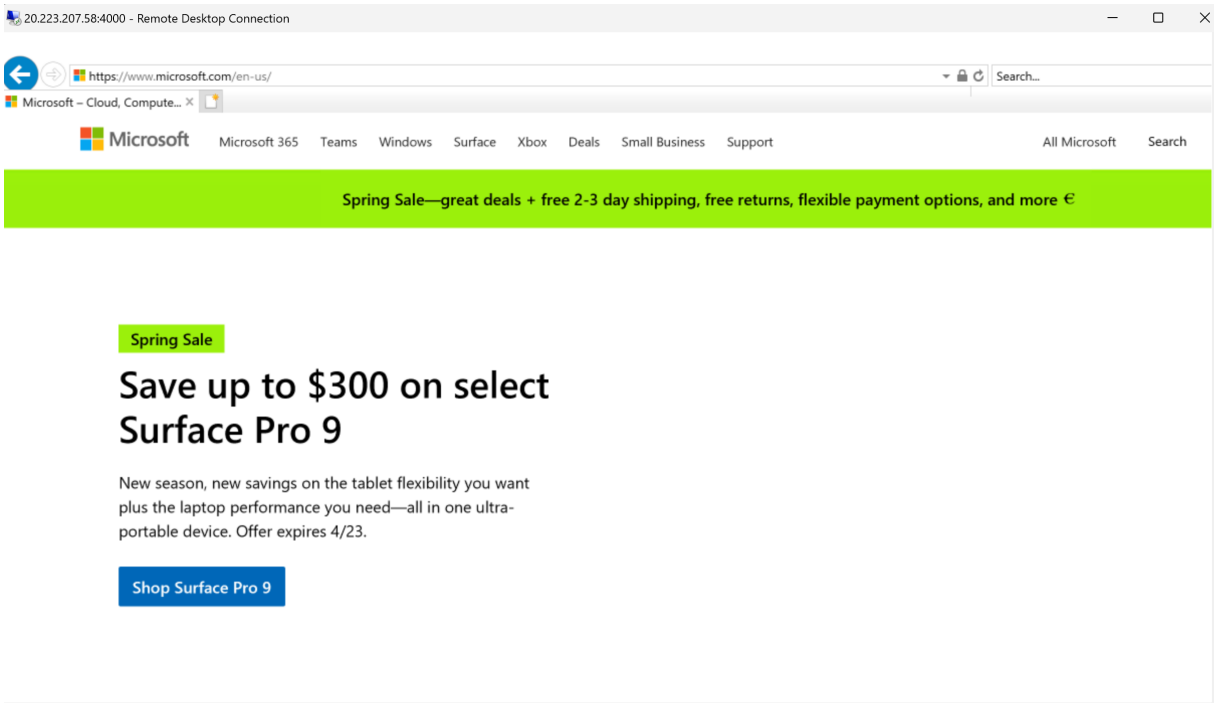


2.3.4 Testing DNAT Translation



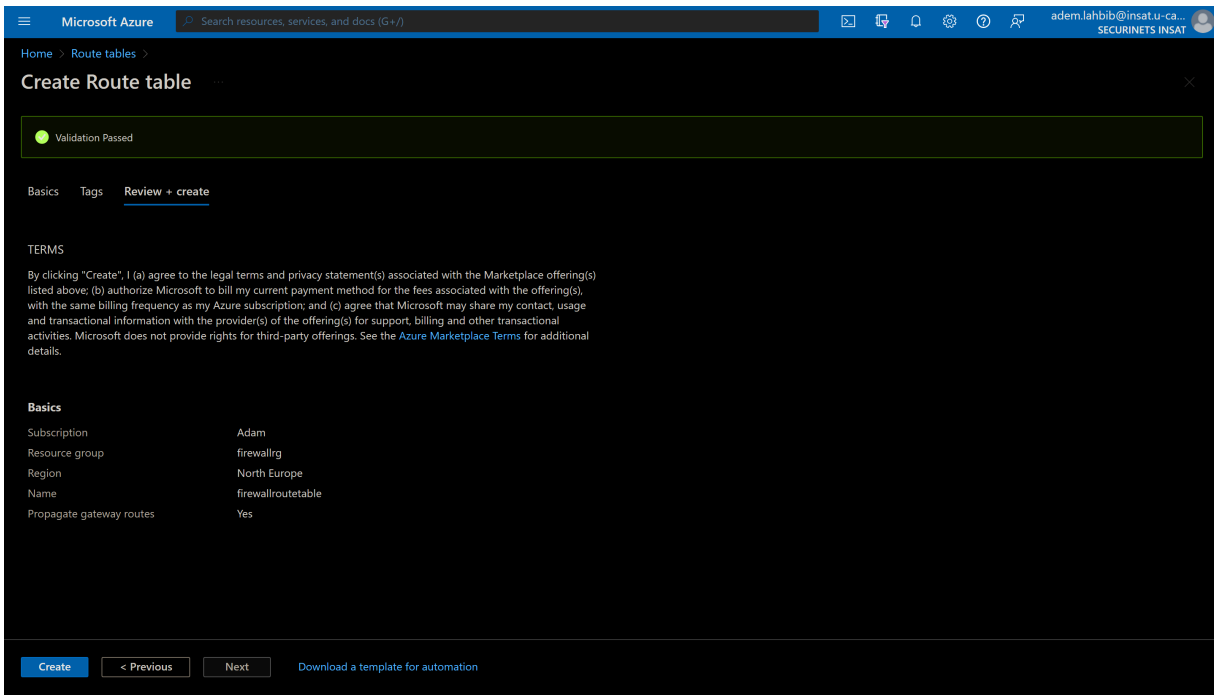
Okay, that worked! Great!

2.3.5 Access Microsoft dot com

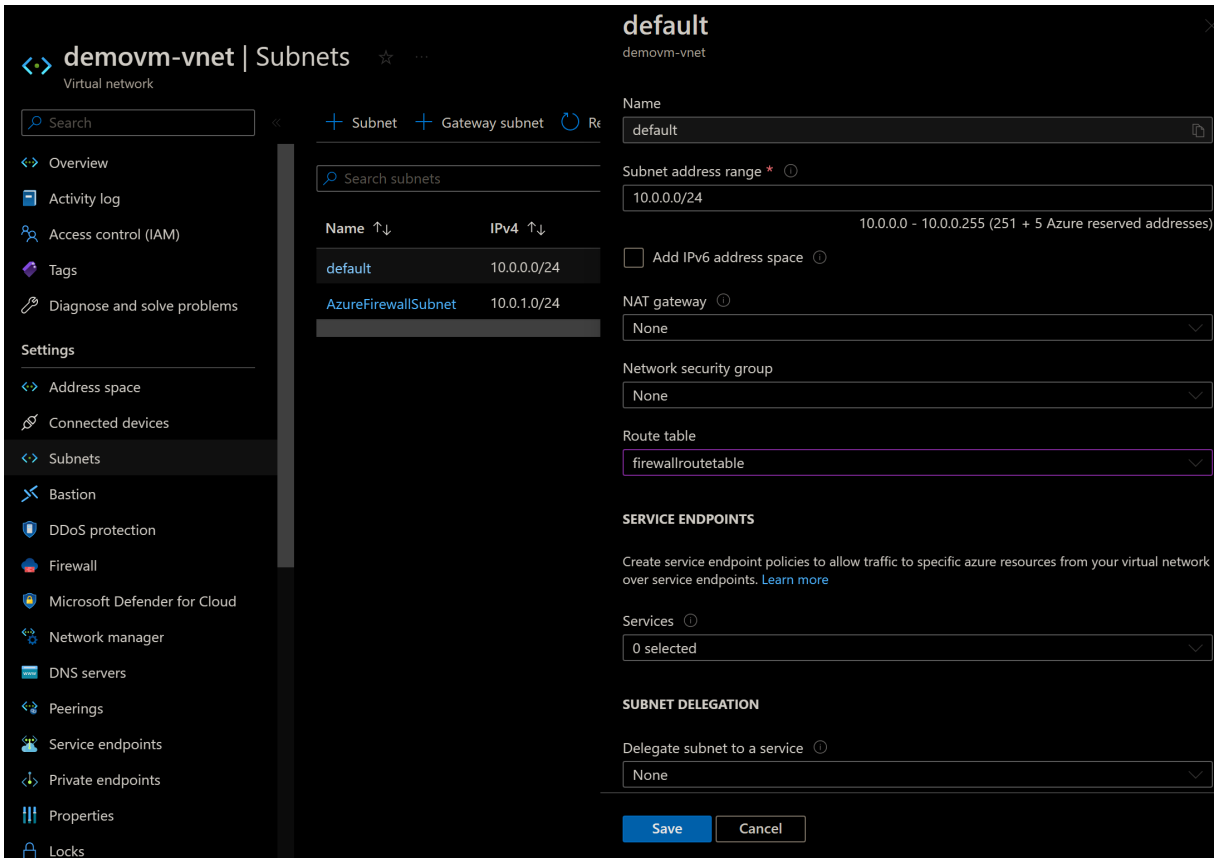


2.3.6 Create new route table

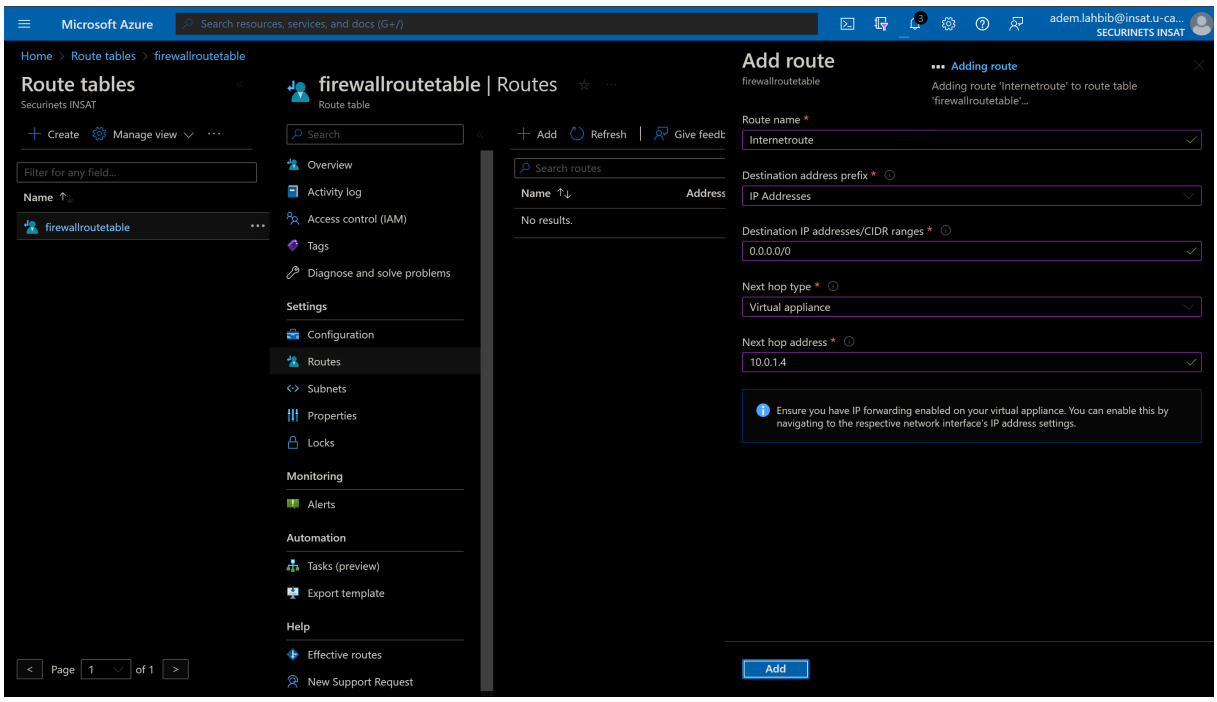
A route table contains a set of rules, called routes, that are used to determine where network traffic from your virtual network or subnet will be directed. You can associate a route table with one or more subnets, and thus control the routing for traffic destined for the subnet's network address space.


Microsoft Azure
Search resources, services, and docs (G+/)
adem.lahbib@insat.u-ca...
SECURINETS INSAT
Home > Route tables >
Create Route table
Validation Passed
Basics
Tags
Review + 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



- 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.

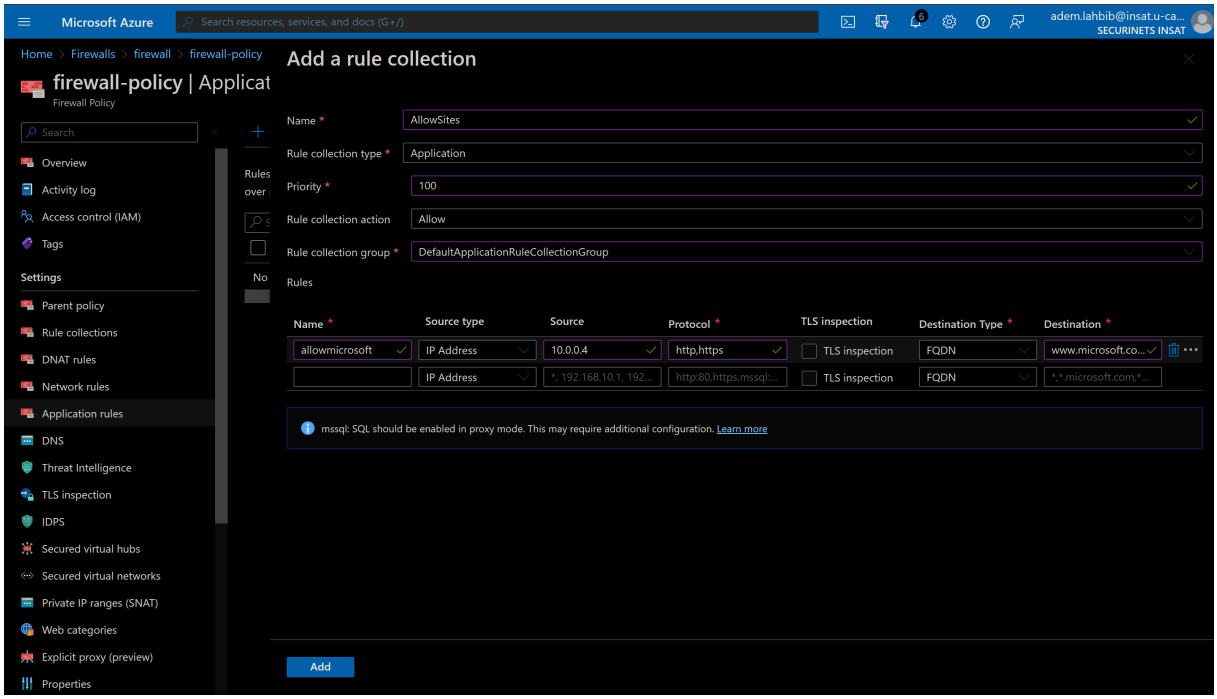
Try this:

- Go back to the last page

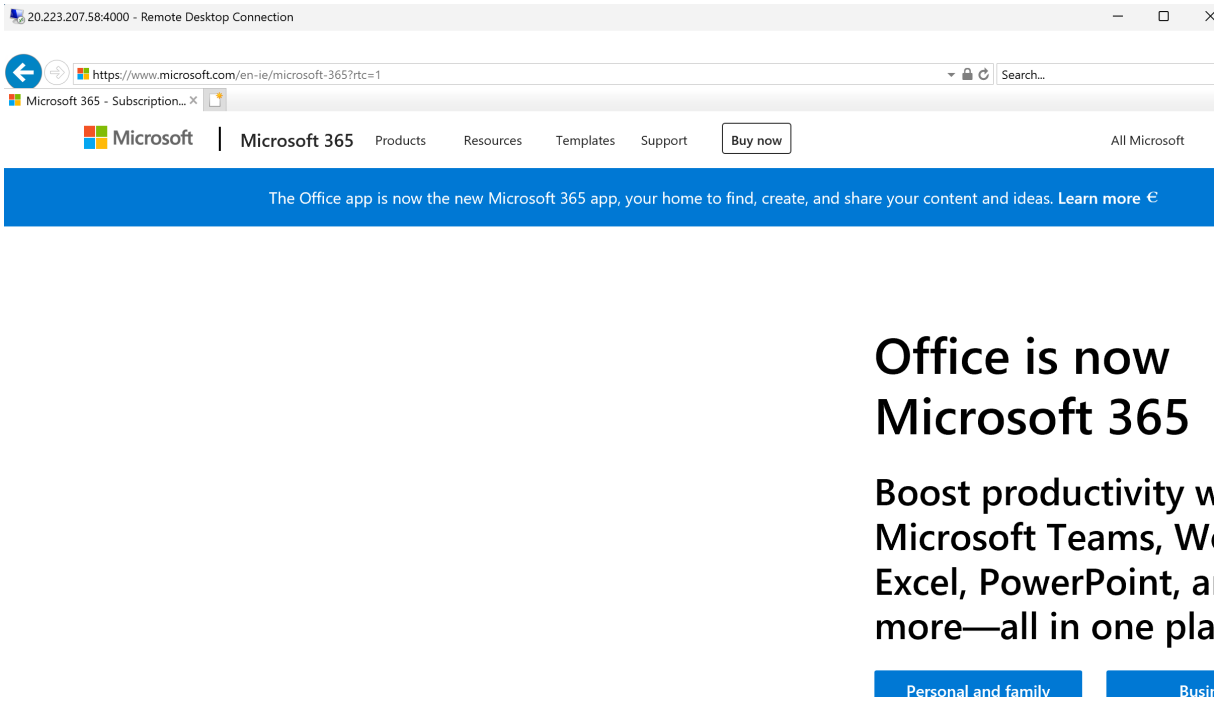
Denied!

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.



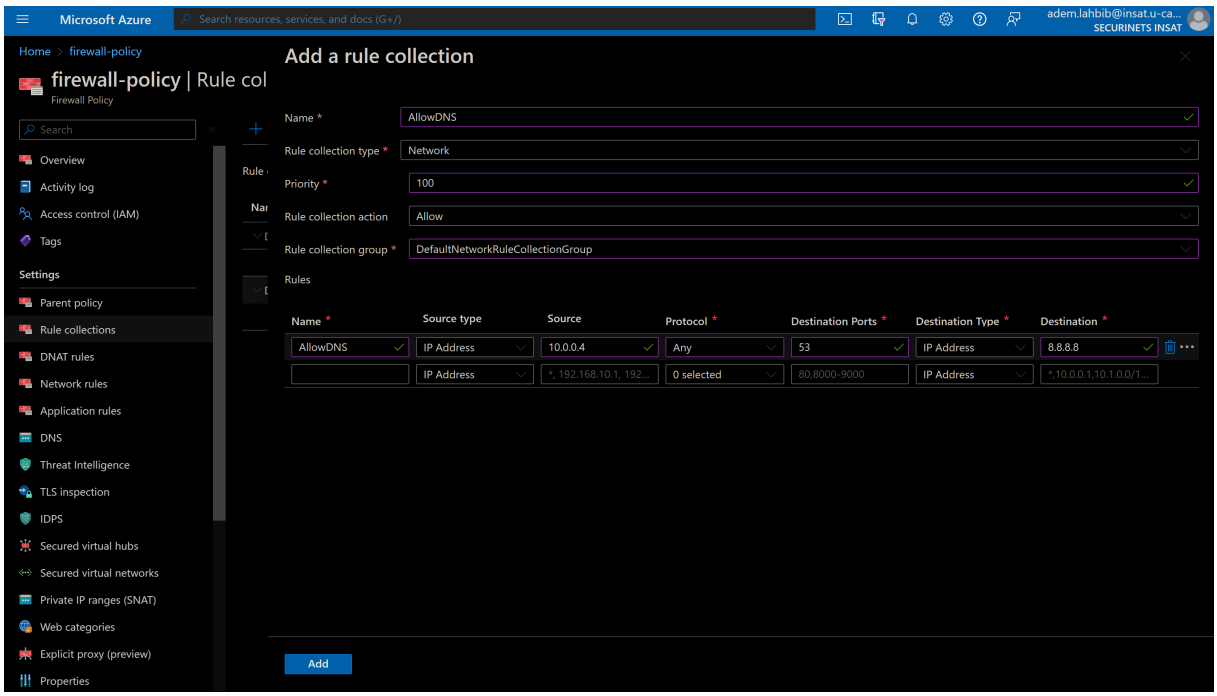
2.3.10 Try Microsoft dot com again?



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.



2.3.12 Delete resource group