TP4 Report

TRAFFIC MANAGER, FRONT DOOR AND FIREWALL

By: Nadia FRIKHA and Rania MIDAOUI, RT4-G2

Introduction:

In today's digital landscape, having a reliable and secure online presence is crucial for businesses of all sizes. To achieve this, many companies rely on cloud-based services to manage their web traffic and ensure high availability and performance for their customers.

Azure Traffic Manager, Front Door, and Firewall are three powerful cloud-based solutions offered by Microsoft Azure that can help businesses improve their online performance and security. These services enable businesses to manage their web traffic efficiently, distribute it across multiple endpoints, and filter out potential cyber threats. By leveraging these tools, businesses can enhance their online presence and provide a better experience for their customers.

Azure traffic manager :

Azure Traffic Manager enables businesses to optimize their web traffic for high availability and performance. It can distribute traffic across multiple endpoints, including Azure regions, on-premises data centers, and third-party cloud providers. It operates at the DNS level. Traffic Manager also monitors the health of each endpoint and can automatically reroute traffic if an endpoint becomes unavailable. In addition, Traffic Manager can optimize performance by routing traffic to the closest available endpoint, reducing latency and improving the user experience.

Azure front door:

Azure Front Door is a cloud-based solution that can improve web application performance, security, and scalability. It includes global load balancing capabilities to distribute traffic across multiple endpoints worldwide. Front Door is highly scalable and can handle large volumes of traffic, and includes a Web Application Firewall (WAF) to protect against common web threats. Traffic routing rules can be configured to route traffic to the best available endpoint based on health, geography, and other factors. Front Door is easy to set up and can work with a wide range of applications and services.

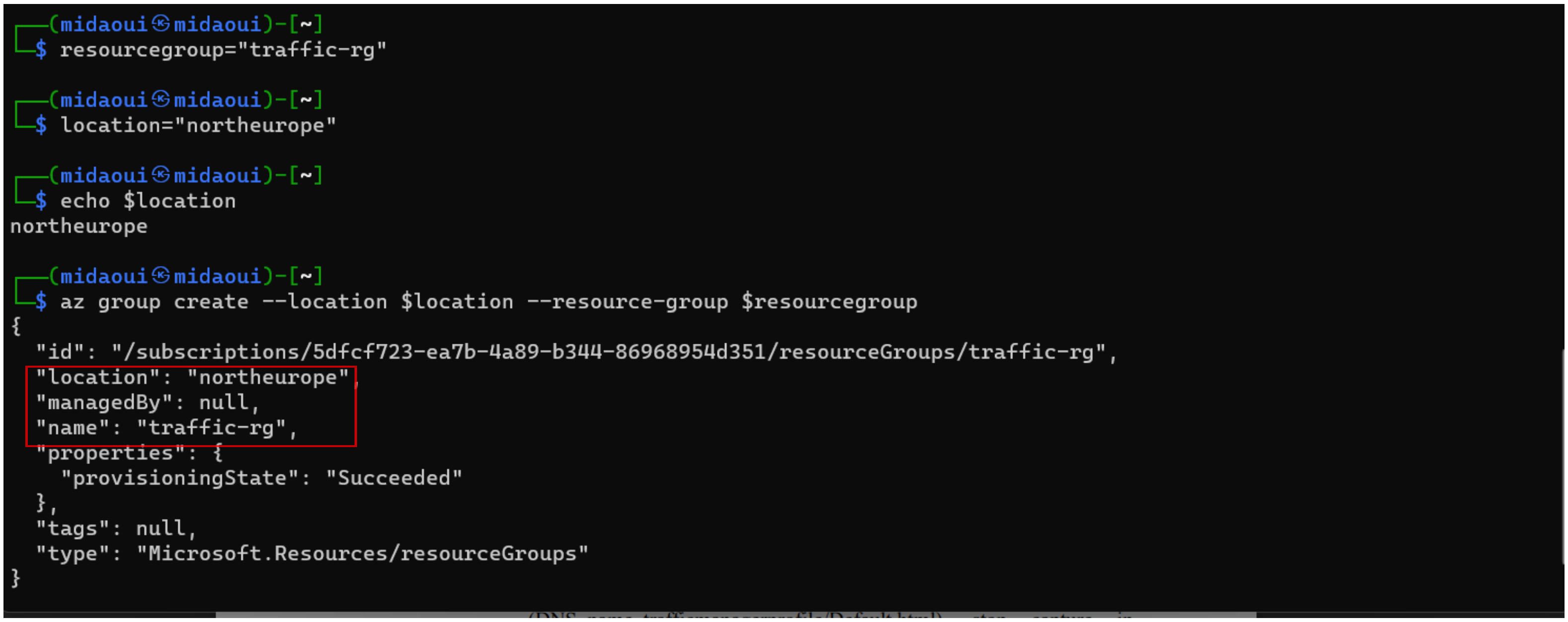
Azure firewall:

Azure Firewall is a cloud-based firewall service that provides managed, scalable, and highly available network security in the cloud. With its application and network filtering capabilities, integration with Azure Sentinel for threat intelligence, high availability and scalability, and centralized management through the Azure portal or Azure PowerShell, Azure Firewall simplifies network security for businesses migrating their applications and services to the cloud. The service offers a range of benefits, including streamlined security management, enhanced threat intelligence, and the ability to handle large volumes of traffic, making it a reliable and effective firewall solution for businesses of all sizes.

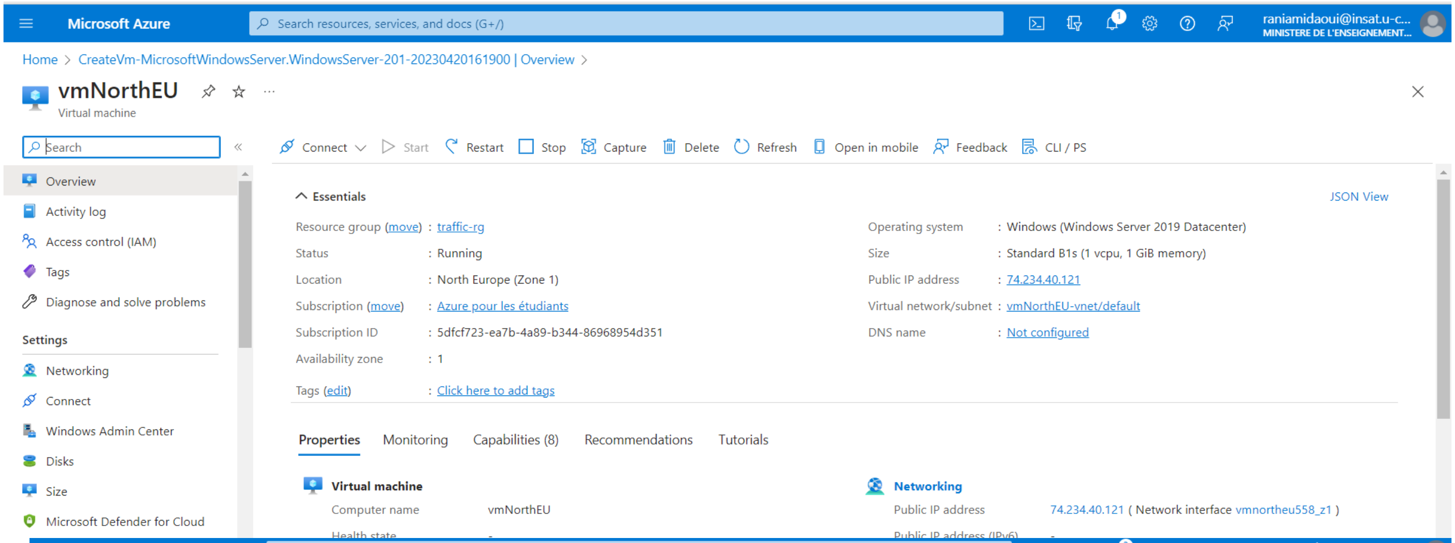
Questions:

Task 1: Azure traffic manager profile:

1-a. We create 2 virtual machines in different regions:



```
┌──(midaoui㉿midaoui)-[~]
└─$ resourcegroup="traffic-rg"

┌──(midaoui㉿midaoui)-[~]
└─$ location="northeurope"

┌──(midaoui㉿midaoui)-[~]
└─$ echo $location
northeurope

┌──(midaoui㉿midaoui)-[~]
└─$ az group create --location $location --resource-group $resourcegroup
{
  "id": "/subscriptions/5dfcf723-ea7b-4a89-b344-86968954d351/resourceGroups/traffic-rg",
  "location": "northeurope",
  "managedBy": null,
  "name": "traffic-rg",
  "properties": {
    "provisioningState": "Succeeded"
  },
  "tags": null,
  "type": "Microsoft.Resources/resourceGroups"
}
```



vmNorthEU

Virtual machine

Resource group (move) : traffic-rg

Status : Running

Location : North Europe (Zone 1)

Subscription (move) : Azure pour les étudiants

Subscription ID : 5dfcf723-ea7b-4a89-b344-86968954d351

Availability zone : 1

Tags (edit) : Click here to add tags

Operating system : Windows (Windows Server 2019 Datacenter)

Size : Standard B1s (1 vcpu, 1 GiB memory)

Public IP address : 74.234.40.121

Virtual network/subnet : vmNorthEU-vnet/default

DNS name : Not configured

Virtual machine

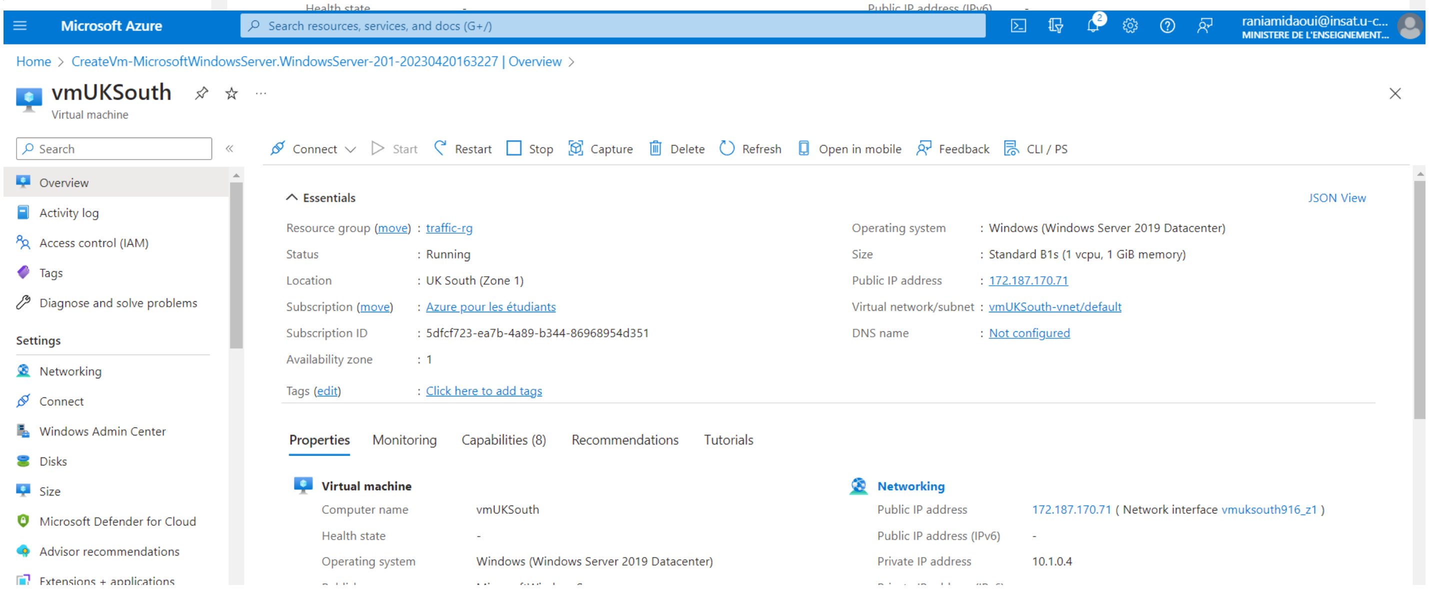
Computer name vmNorthEU

Health state -

Networking

Public IP address 74.234.40.121 (Network interface vmnortheu558_z1)

Public IP address (IPv6) -



vmUKSouth

Virtual machine

Resource group (move) : traffic-rg

Status : Running

Location : UK South (Zone 1)

Subscription (move) : Azure pour les étudiants

Subscription ID : 5dfcf723-ea7b-4a89-b344-86968954d351

Availability zone : 1

Tags (edit) : Click here to add tags

Operating system : Windows (Windows Server 2019 Datacenter)

Size : Standard B1s (1 vcpu, 1 GiB memory)

Public IP address : 172.187.170.71

Virtual network/subnet : vmUKSouth-vnet/default

DNS name : Not configured

Virtual machine

Computer name vmUKSouth

Health state -

Operating system Windows (Windows Server 2019 Datacenter)

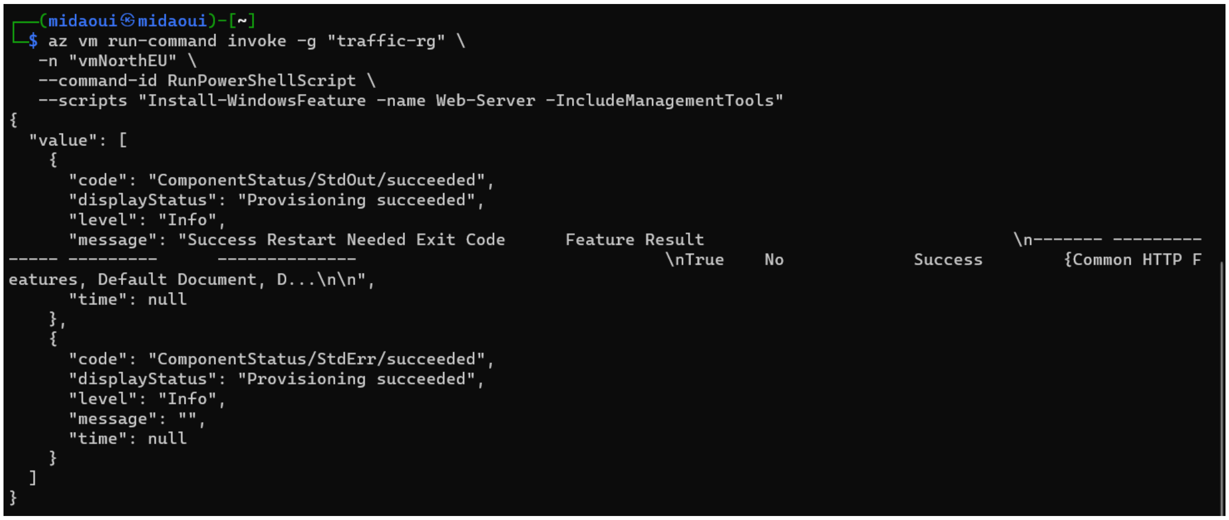
Networking

Public IP address 172.187.170.71 (Network interface vmuksouth916_z1)

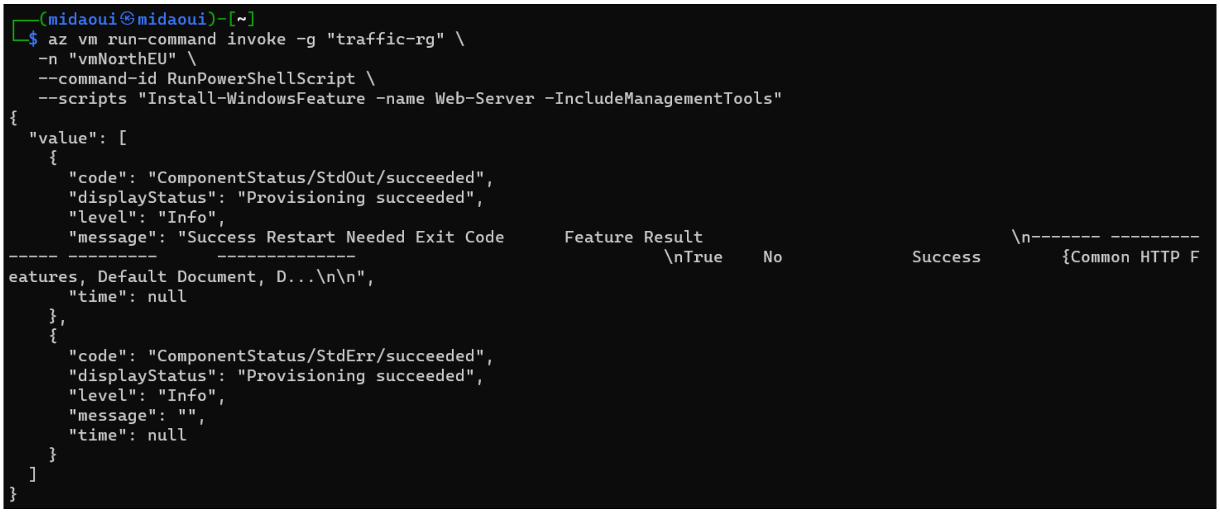
Public IP address (IPv6) -

Private IP address 10.1.0.4

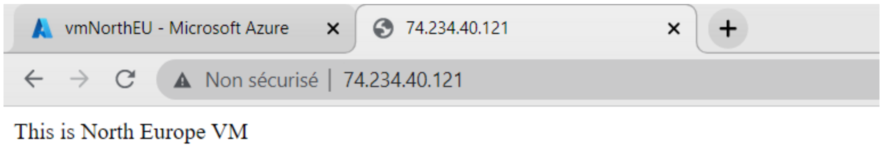
1-b. We install and configure IIS servers for each machine:



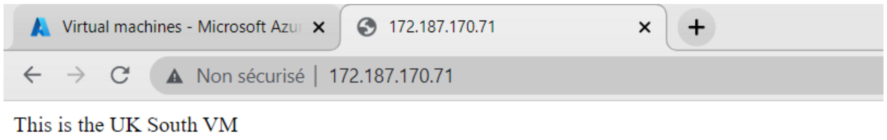
```
┌──(midaoui㉿midaoui)-[~]
└─$ az vm run-command invoke -g "traffic-rg" \
   -n "vmNorthEU" \
   --command-id RunPowerShellScript \
   --scripts "Install-WindowsFeature -name Web-Server -IncludeManagementTools"
{
  "value": [
    {
      "code": "ComponentStatus/StdOut/succeeded",
      "displayStatus": "Provisioning succeeded",
      "level": "Info",
      "message": "Success Restart Needed Exit Code      Feature Result                               \n------- ---------
----- ---------      --------------                                        \nTrue    No             Success        {Common HTTP F
eatures, Default Document, D...\n\n",
      "time": null
    },
    {
      "code": "ComponentStatus/StdErr/succeeded",
      "displayStatus": "Provisioning succeeded",
      "level": "Info",
      "message": "",
      "time": null
    }
  ]
}
```



```
┌──(midaoui㉿midaoui)-[~]
└─$ az vm run-command invoke -g "traffic-rg" \
  -n "vmNorthEU" \
  --command-id RunPowerShellScript \
  --scripts "Install-WindowsFeature -name Web-Server -IncludeManagementTools"
{
  "value": [
    {
      "code": "ComponentStatus/StdOut/succeeded",
      "displayStatus": "Provisioning succeeded",
      "level": "Info",
      "message": "Success Restart Needed Exit Code      Feature Result                          \n------- ---------
----- ---------      --------------                        \nTrue    No             Success        {Common HTTP F
eatures, Default Document, D...\n\n",
      "time": null
    },
    {
      "code": "ComponentStatus/StdErr/succeeded",
      "displayStatus": "Provisioning succeeded",
      "level": "Info",
      "message": "",
      "time": null
    }
  ]
}
```

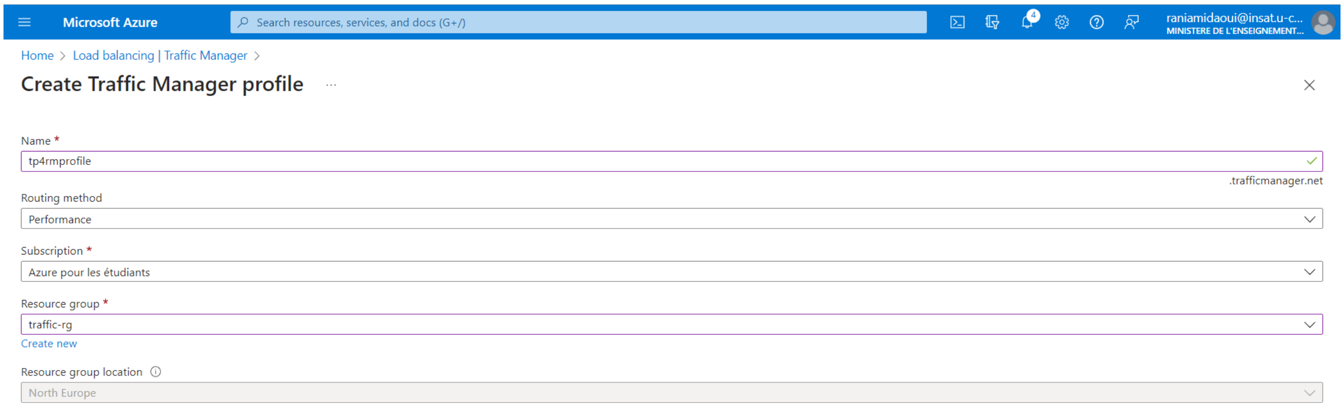


This is North Europe VM


Virtual machines - Microsoft Azu
172.187.170.71
Non sécurisé | 172.187.170.71

This is the UK South VM

1-c. We create the traffic manager profile:


Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Load balancing | Traffic Manager >

Create Traffic Manager profile

Name *
tp4rmprofile
.trafficmanager.net

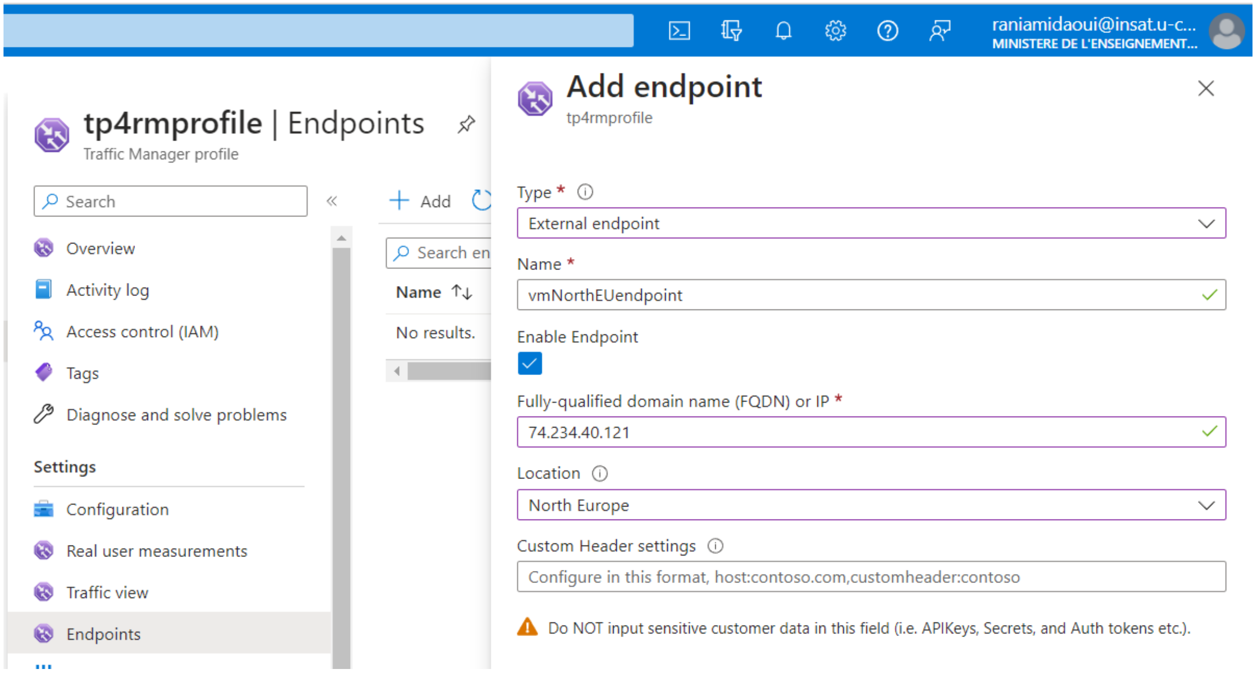
Routing method
Performance

Subscription *
Azure pour les étudiants

Resource group *
traffic-rg
Create new

Resource group location
North Europe

1-d. We add the virtual machines as External endpoints:



Add endpoint
tp4rmprofile

Type * : External endpoint

Name * : vmNorthEUendpoint

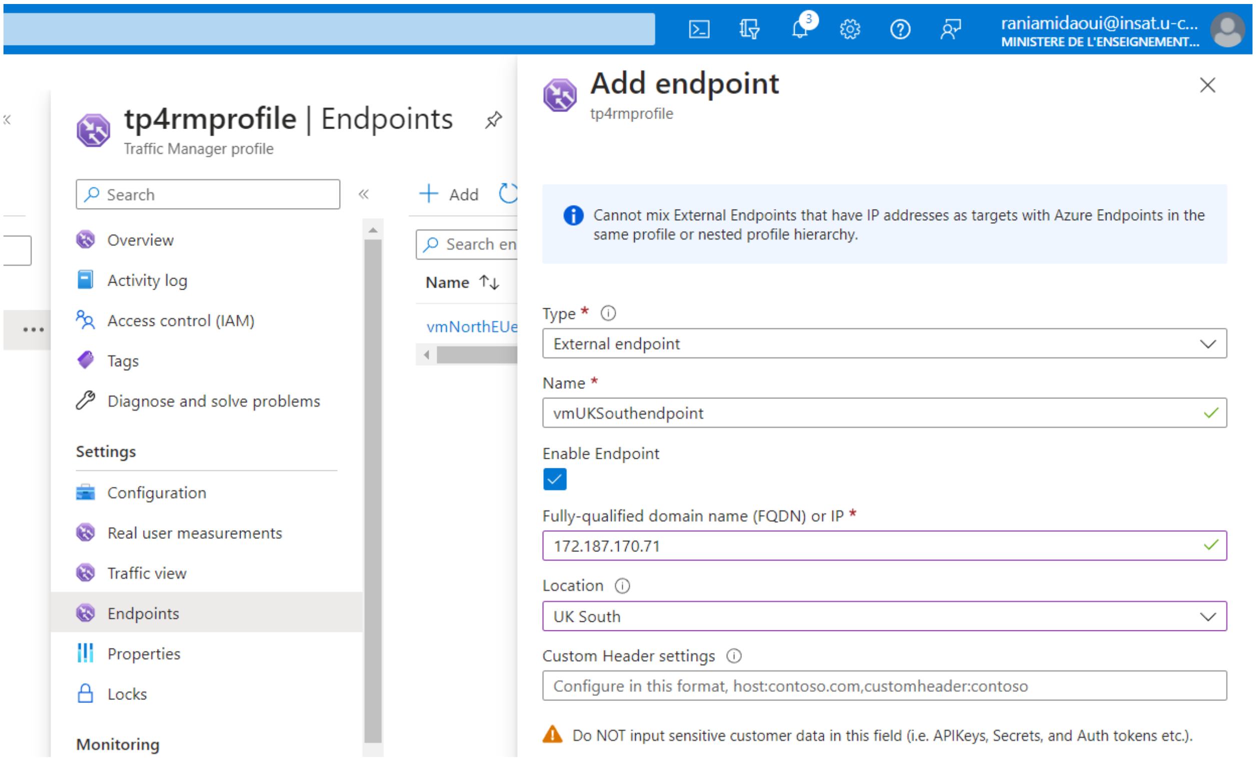
Enable Endpoint: ☑

Fully-qualified domain name (FQDN) or IP * : 74.234.40.121

Location: North Europe

Custom Header settings: Configure in this format, host:contoso.com,customheader:contoso

⚠ Do NOT input sensitive customer data in this field (i.e. APIKeys, Secrets, and Auth tokens etc.).



Add endpoint
tp4rmprofile

ⓘ Cannot mix External Endpoints that have IP addresses as targets with Azure Endpoints in the same profile or nested profile hierarchy.

Type * : External endpoint

Name * : vmUKSouthendpoint

Enable Endpoint: ☑

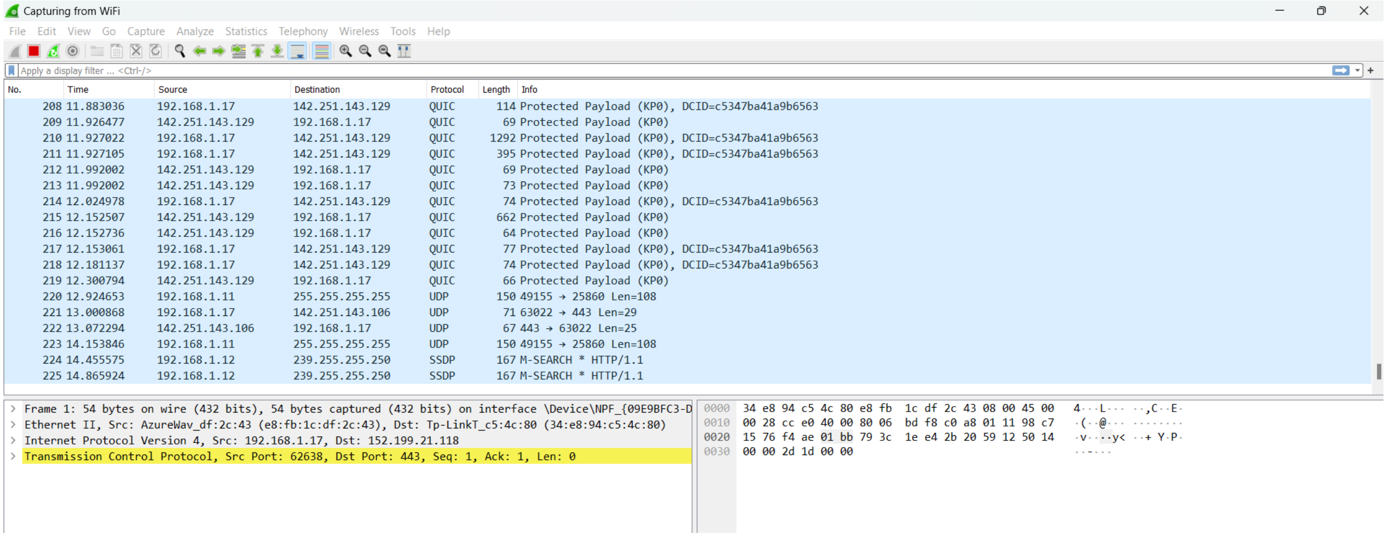
Fully-qualified domain name (FQDN) or IP * : 172.187.170.71

Location: UK South

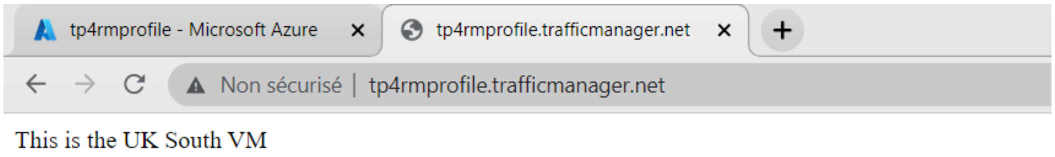
Custom Header settings: Configure in this format, host:contoso.com,customheader:contoso

⚠ Do NOT input sensitive customer data in this field (i.e. APIKeys, Secrets, and Auth tokens etc.).

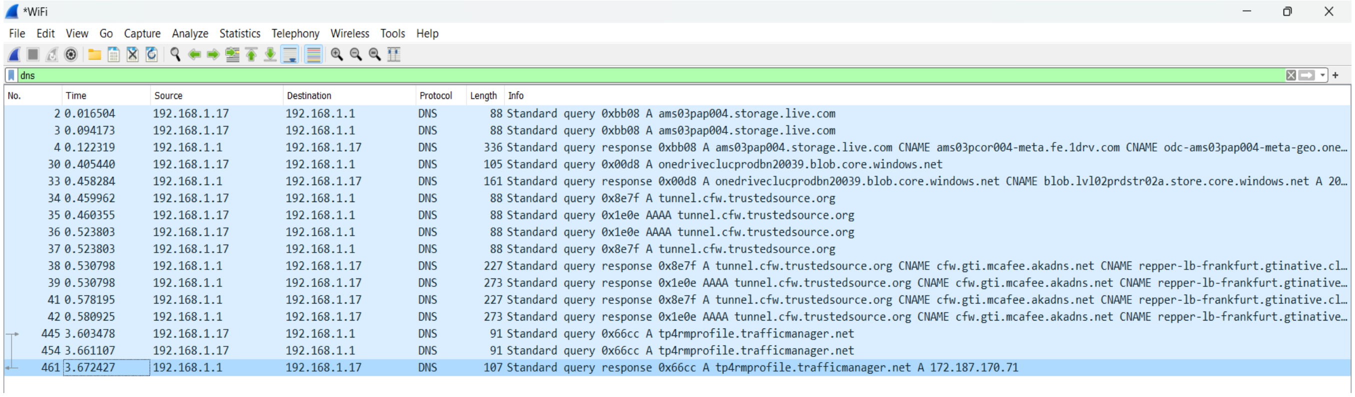
1-e. We make a request onto the traffic manager profile and analyze the results:


Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source           Destination      Protocol Length Info
  208 11.883036  192.168.1.17     142.251.143.129  QUIC      114 Protected Payload (KP0), DCID=c5347ba41a9b6563
  209 11.926477  142.251.143.129  192.168.1.17     QUIC       69 Protected Payload (KP0)
  210 11.927022  192.168.1.17     142.251.143.129  QUIC     1292 Protected Payload (KP0), DCID=c5347ba41a9b6563
  211 11.927105  192.168.1.17     142.251.143.129  QUIC      395 Protected Payload (KP0), DCID=c5347ba41a9b6563
  212 11.992002  142.251.143.129  192.168.1.17     QUIC       69 Protected Payload (KP0)
  213 11.992002  142.251.143.129  192.168.1.17     QUIC       73 Protected Payload (KP0)
  214 12.024978  192.168.1.17     142.251.143.129  QUIC       74 Protected Payload (KP0), DCID=c5347ba41a9b6563
  215 12.152507  142.251.143.129  192.168.1.17     QUIC      662 Protected Payload (KP0)
  216 12.152736  142.251.143.129  192.168.1.17     QUIC       64 Protected Payload (KP0)
  217 12.153061  192.168.1.17     142.251.143.129  QUIC       77 Protected Payload (KP0), DCID=c5347ba41a9b6563
  218 12.181137  192.168.1.17     142.251.143.129  QUIC       74 Protected Payload (KP0), DCID=c5347ba41a9b6563
  219 12.300794  142.251.143.129  192.168.1.17     QUIC       66 Protected Payload (KP0)
  220 12.924653  192.168.1.11     255.255.255.255  UDP       150 49155 → 25860 Len=108
  221 13.000868  192.168.1.17     142.251.143.106  UDP        71 63022 → 443 Len=29
  222 13.072294  142.251.143.106  192.168.1.17     UDP        67 443 → 63022 Len=25
  223 14.153846  192.168.1.11     255.255.255.255  UDP       150 49155 → 25860 Len=108
  224 14.455575  192.168.1.12     239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1
  225 14.865924  192.168.1.12     239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{09E9BFC3-D
> Ethernet II, Src: AzureWav_df:2c:43 (e8:fb:1c:df:2c:43), Dst: Tp-LinkT_c5:4c:80 (34:e8:94:c5:4c:80)
> Internet Protocol Version 4, Src: 192.168.1.17, Dst: 152.199.21.118
> Transmission Control Protocol, Src Port: 62638, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000  34 e8 94 c5 4c 80 e8 fb  1c df 2c 43 08 00 45 00   4···L··· ··,C··E·
0010  00 28 cc e0 40 00 80 06  bd f8 c0 a8 01 11 98 c7   ·(··@··· ········
0020  15 76 f4 ae 01 bb 79 3c  1e e4 2b 20 59 12 50 14   ·v····y< ··+ Y·P·
0030  00 00 2d 1d 00 00                                  ··-···
```

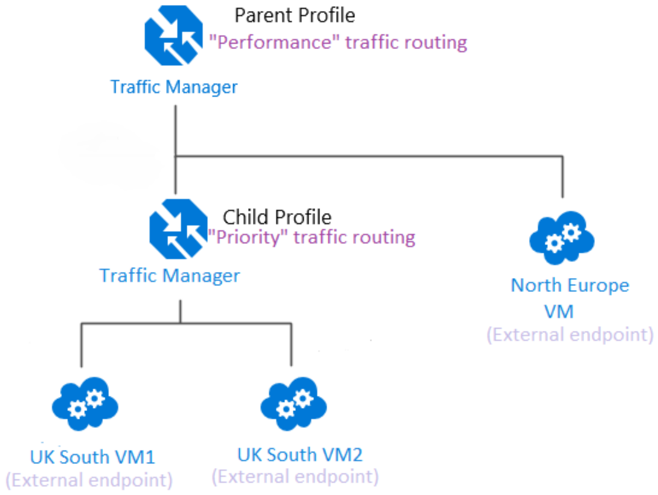

tp4rmprofile - Microsoft Azure
tp4rmprofile.trafficmanager.net
Non sécurisé | tp4rmprofile.trafficmanager.net

This is the UK South VM


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

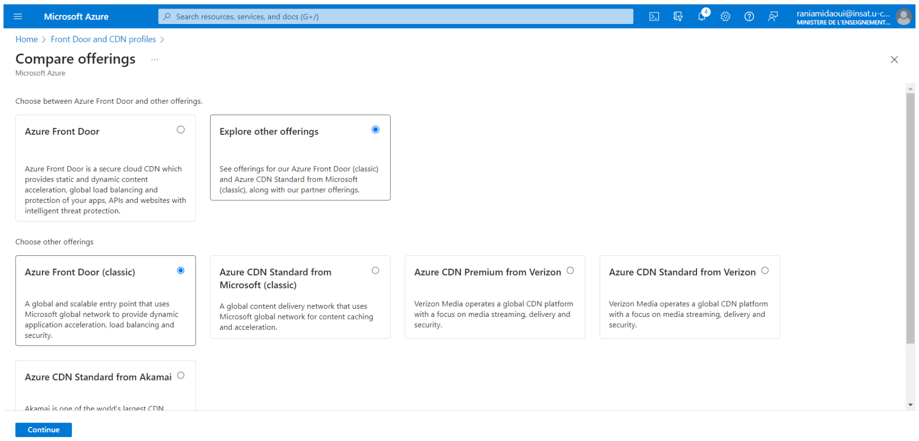
```
dns

No.   Time      Source        Destination   Protocol Length Info
    2 0.016504  192.168.1.17  192.168.1.1   DNS       88 Standard query 0xbb08 A ams03pap004.storage.live.com
    3 0.094173  192.168.1.17  192.168.1.1   DNS       88 Standard query 0xbb08 A ams03pap004.storage.live.com
    4 0.122319  192.168.1.1   192.168.1.17  DNS      336 Standard query response 0xbb08 A ams03pap004.storage.live.com CNAME ams03pcor004-meta.fe.1drv.com CNAME odc-ams03pap004-meta-geo.one…
   30 0.405440  192.168.1.17  192.168.1.1   DNS      105 Standard query 0x00d8 A onedriveclucprodbn20039.blob.core.windows.net
   33 0.458284  192.168.1.1   192.168.1.17  DNS      161 Standard query response 0x00d8 A onedriveclucprodbn20039.blob.core.windows.net CNAME blob.lvl02prdstr02a.store.core.windows.net A 20…
   34 0.459962  192.168.1.17  192.168.1.1   DNS       88 Standard query 0x8e7f A tunnel.cfw.trustedsource.org
   35 0.460355  192.168.1.17  192.168.1.1   DNS       88 Standard query 0x1e0e AAAA tunnel.cfw.trustedsource.org
   36 0.523803  192.168.1.17  192.168.1.1   DNS       88 Standard query 0x1e0e AAAA tunnel.cfw.trustedsource.org
   37 0.523803  192.168.1.17  192.168.1.1   DNS       88 Standard query 0x8e7f A tunnel.cfw.trustedsource.org
   38 0.530798  192.168.1.1   192.168.1.17  DNS      227 Standard query response 0x8e7f A tunnel.cfw.trustedsource.org CNAME cfw.gti.mcafee.akadns.net CNAME repper-lb-frankfurt.gtinative.cl…
   39 0.530798  192.168.1.1   192.168.1.17  DNS      273 Standard query response 0x1e0e AAAA tunnel.cfw.trustedsource.org CNAME cfw.gti.mcafee.akadns.net CNAME repper-lb-frankfurt.gtinative…
   41 0.578195  192.168.1.1   192.168.1.17  DNS      227 Standard query response 0x8e7f A tunnel.cfw.trustedsource.org CNAME cfw.gti.mcafee.akadns.net CNAME repper-lb-frankfurt.gtinative.cl…
   42 0.580925  192.168.1.1   192.168.1.17  DNS      273 Standard query response 0x1e0e AAAA tunnel.cfw.trustedsource.org CNAME cfw.gti.mcafee.akadns.net CNAME repper-lb-frankfurt.gtinative…
  445 3.603478  192.168.1.17  192.168.1.1   DNS       91 Standard query 0x66cc A tp4rmprofile.trafficmanager.net
  454 3.661107  192.168.1.17  192.168.1.1   DNS       91 Standard query 0x66cc A tp4rmprofile.trafficmanager.net
  461 3.672427  192.168.1.1   192.168.1.17  DNS      107 Standard query response 0x66cc A tp4rmprofile.trafficmanager.net A 172.187.170.71
```

2- Proposed architecture diagram:



Task 2: Azure Front door:

1-


Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Front Door and CDN profiles >

Compare offerings

Microsoft Azure

Choose between Azure Front Door and other offerings.

○ Azure Front Door

Azure Front Door is a secure cloud CDN which provides static and dynamic content acceleration, global load balancing and protection of your apps, APIs and websites with intelligent threat protection.

● Explore other offerings

See offerings for our Azure Front Door (classic) and Azure CDN Standard from Microsoft (classic), along with our partner offerings.

Choose other offerings

● Azure Front Door (classic)

A global and scalable entry point that uses Microsoft global network to provide dynamic application acceleration, load balancing and security.

○ Azure CDN Standard from Microsoft (classic)

A global content delivery network that uses Microsoft global network for content caching and acceleration.

○ Azure CDN Premium from Verizon

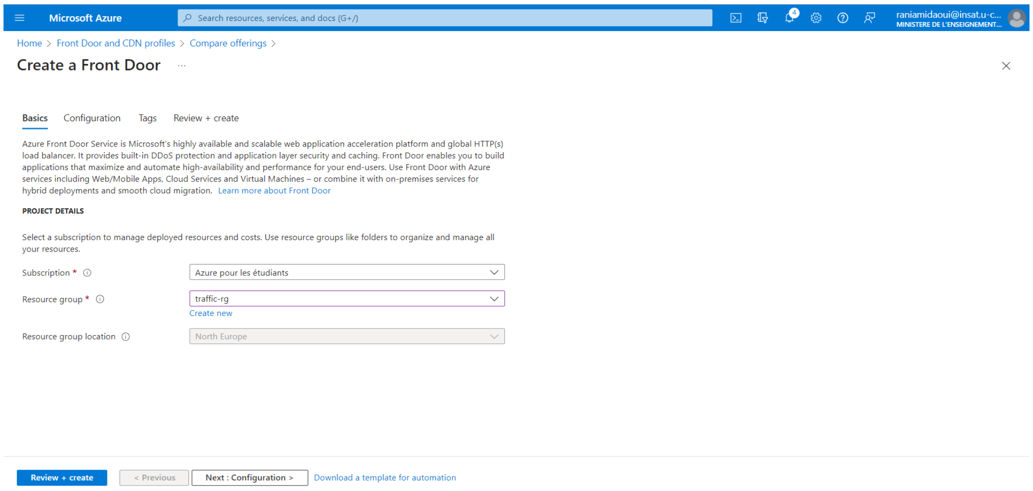
Verizon Media operates a global CDN platform with a focus on media streaming, delivery and security.

○ Azure CDN Standard from Verizon

Verizon Media operates a global CDN platform with a focus on media streaming, delivery and security.

○ Azure CDN Standard from Akamai

Akamai is one of the world's largest CDN


Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Front Door and CDN profiles > Compare offerings >

Create a 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

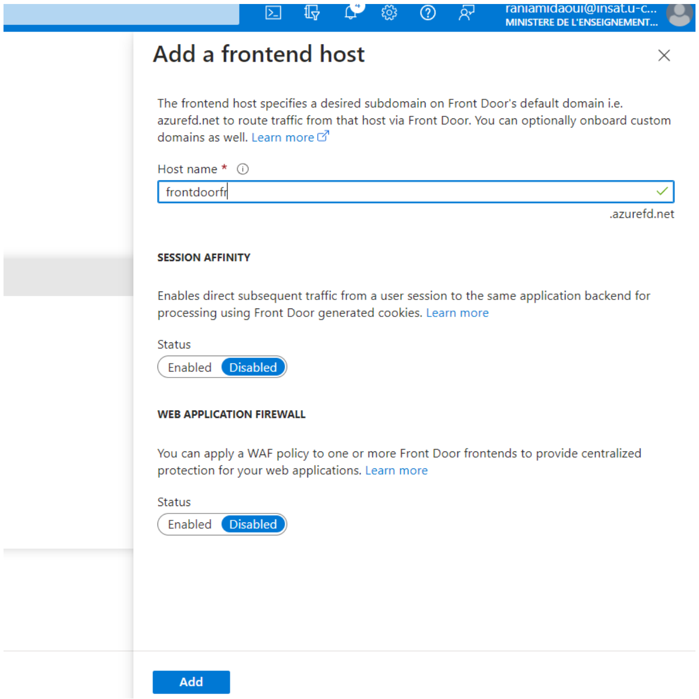
Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure pour les étudiants

Resource group * : traffic-rg

Create new

Resource group location : North Europe



raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...

Add a frontend host

The frontend host specifies a desired subdomain on Front Door's default domain i.e. azurefd.net to route traffic from that host via Front Door. You can optionally onboard custom domains as well. Learn more

Host name * : frontdoorfr .azurefd.net

SESSION AFFINITY

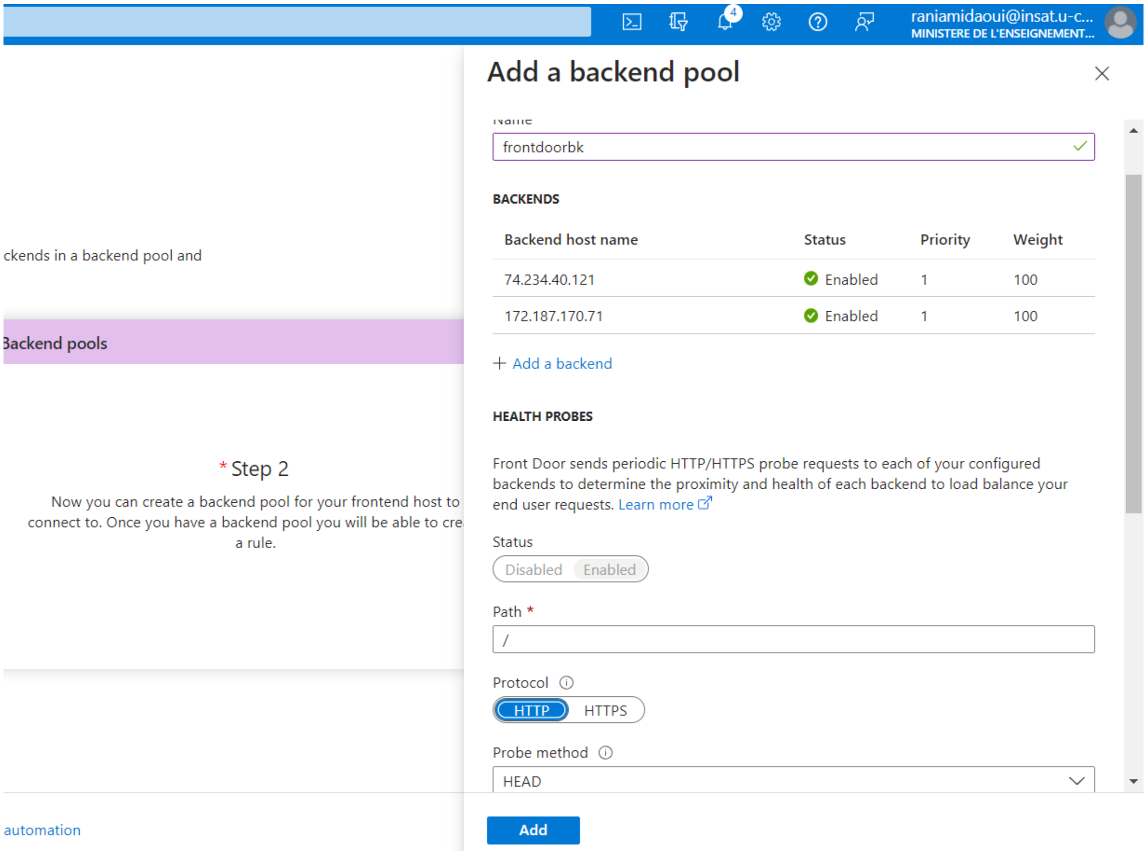
Enables direct subsequent traffic from a user session to the same application backend for processing using Front Door generated cookies. Learn more

Status: Enabled [✓ Disabled]

WEB APPLICATION FIREWALL

You can apply a WAF policy to one or more Front Door frontends to provide centralized protection for your web applications. Learn more

Status: Enabled [✓ Disabled]



raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...

ckends in a backend pool and

Backend pools

* Step 2

Now you can create a backend pool for your frontend host to connect to. Once you have a backend pool you will be able to cre a rule.

automation

Add a backend pool

Name: frontdoorbk

BACKENDS

Backend host name	Status	Priority	Weight
74.234.40.121	✓ Enabled	1	100
172.187.170.71	✓ Enabled	1	100

HEALTH PROBES

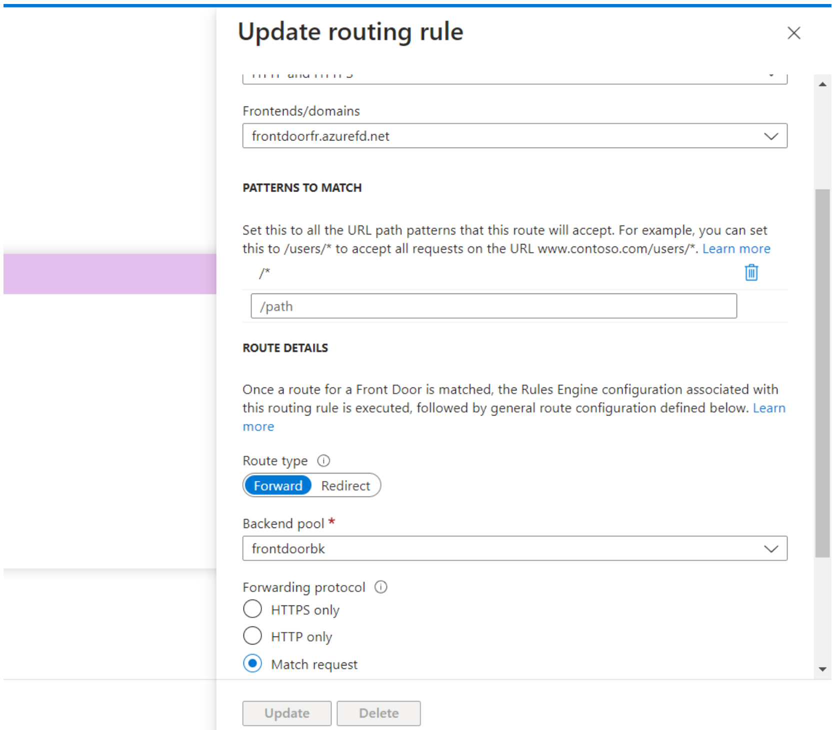
Front Door sends periodic HTTP/HTTPS probe requests to each of your configured backends to determine the proximity and health of each backend to load balance your end user requests. Learn more

Status: Disabled [✓ Enabled]

Path * : /

Protocol: [✓ HTTP] HTTPS

Probe method: HEAD



Update routing rule

Frontends/domains: frontdoorfr.azurefd.net

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

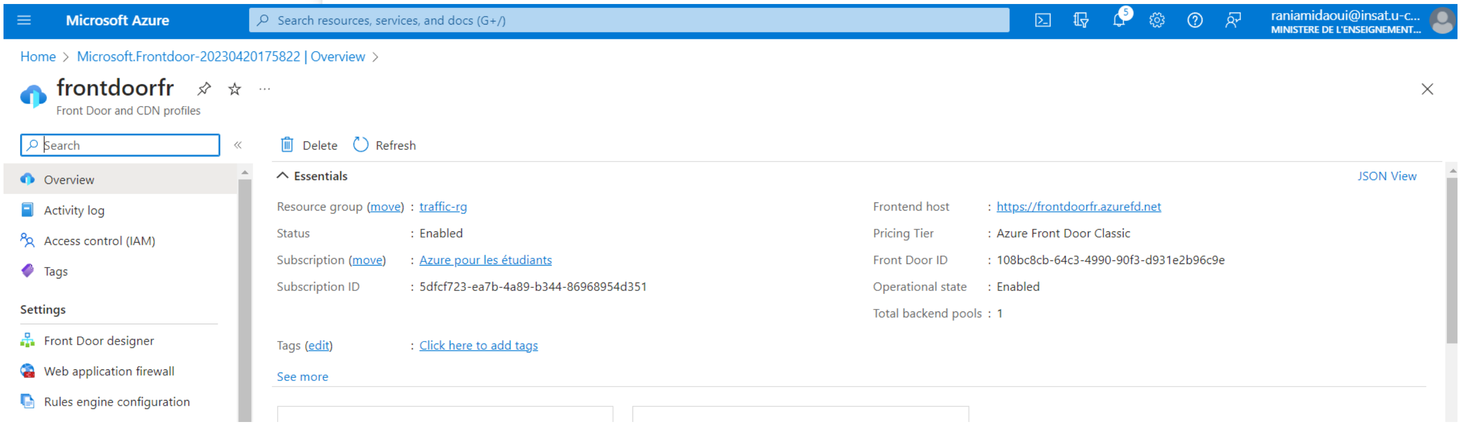
ROUTE DETAILS

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

Backend pool *: frontdoorbk

Forwarding protocol:
○ HTTPS only
○ HTTP only
● Match request



Home > Microsoft.Frontdoor-20230420175822 | Overview >

frontdoorfr

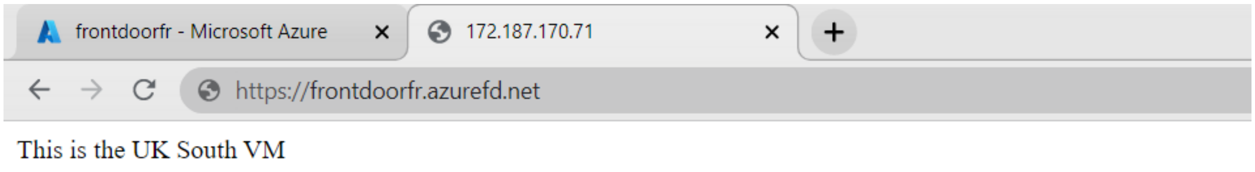
Front Door and CDN profiles

Essentials

Resource group (move) : traffic-rg
Status : Enabled
Subscription (move) : Azure pour les étudiants
Subscription ID : 5dfcf723-ea7b-4a89-b344-86968954d351
Tags (edit) : Click here to add tags

Frontend host : https://frontdoorfr.azurefd.net
Pricing Tier : Azure Front Door Classic
Front Door ID : 108bc8cb-64c3-4990-90f3-d931e2b96c9e
Operational state : Enabled
Total backend pools : 1

2- We copy the URL link of the fronted host and paste it in a new browser tab:

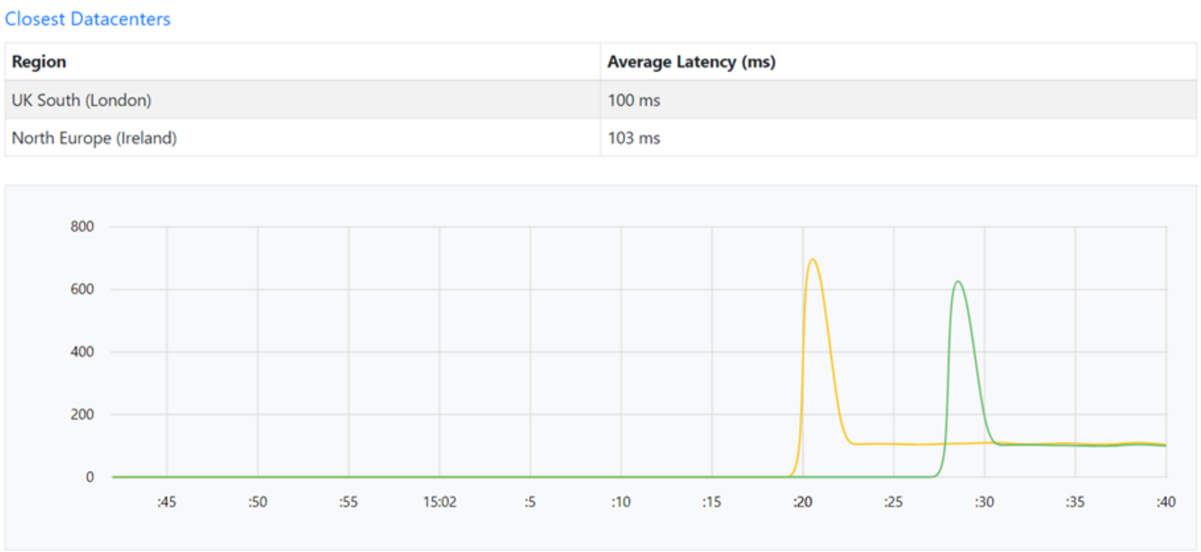


https://frontdoorfr.azurefd.net

This is the UK South VM

Why was the UK south VM selected ?

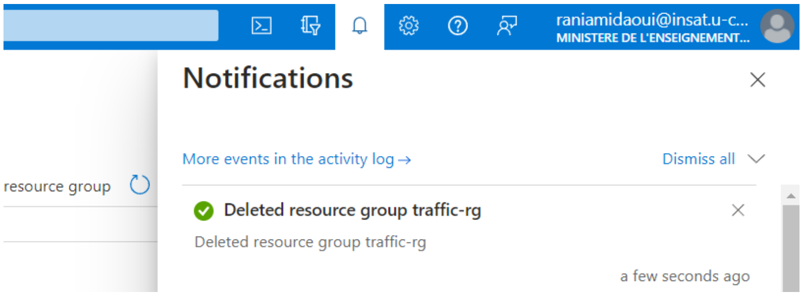
When we accessed the URL of the Azure Front Door, Azure Front Door used the IP address of the device we used to determine our location. Based on this location, Azure Front Door used the Geographic routing method, which is the default routing method, to determine which endpoint is closest to us. Since we are located in Tunis, which is closer to the UK South location than the North Europe location, Azure Front Door directed us to the endpoint in the UK South.



Closest Datacenters

Region	Average Latency (ms)
UK South (London)	100 ms
North Europe (Ireland)	103 ms

3- We delete the resource group:



Notifications

More events in the activity log →

Dismiss all

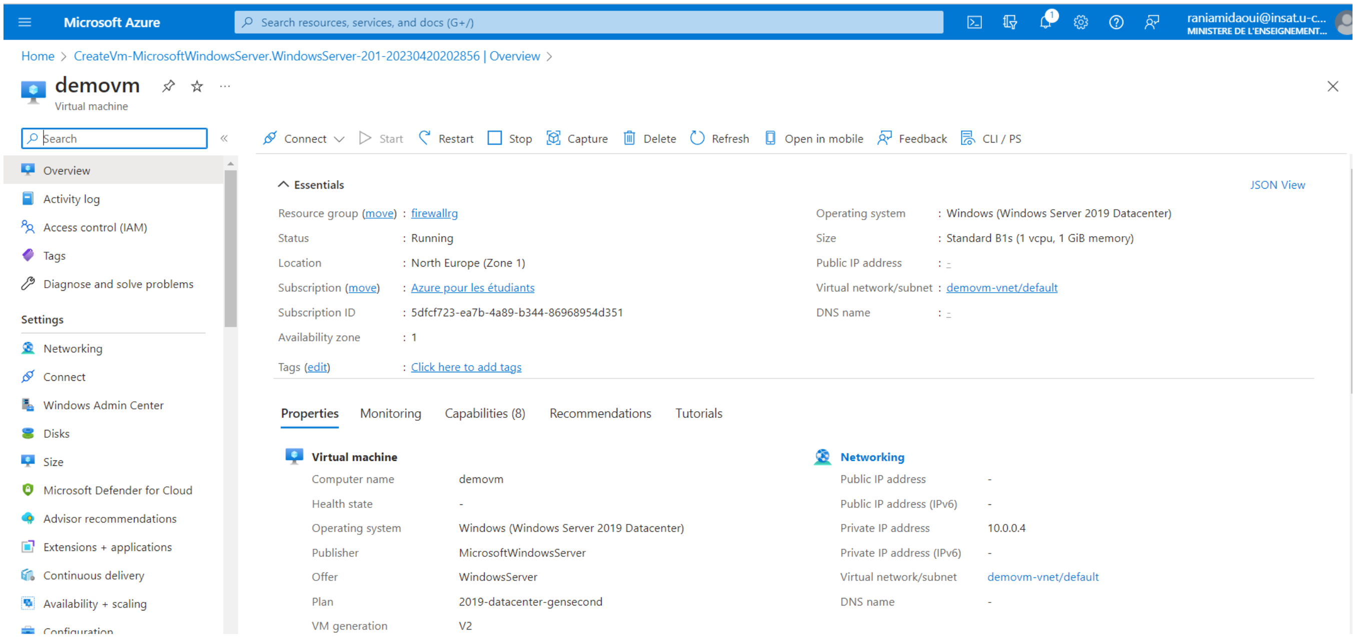
Deleted resource group traffic-rg

Deleted resource group traffic-rg

a few seconds ago

Task 3: Azure firewall:

1- We create a virtual machine:



Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...

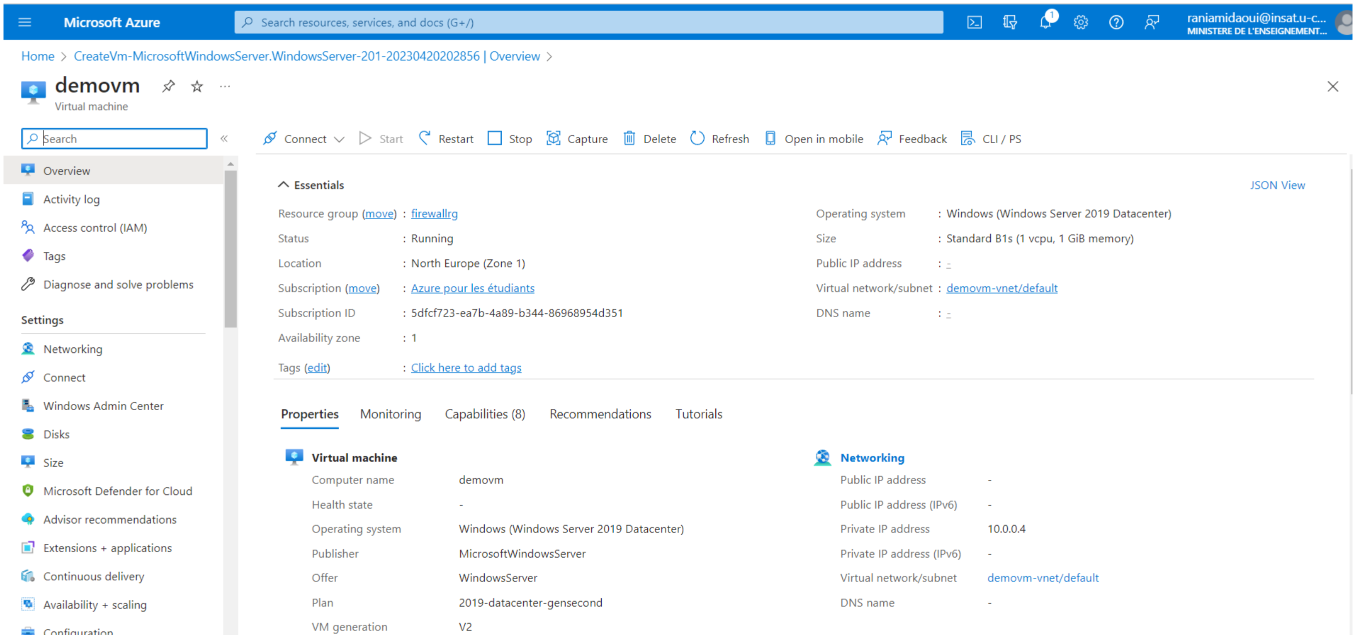
Home > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230420202856 | Overview >

demovm
Virtual machine

Essentials

Resource group (move)	: firewallrg	Operating system	: Windows (Windows Server 2019 Datacenter)
Status	: Running	Size	: Standard B1s (1 vcpu, 1 GiB memory)
Location	: North Europe (Zone 1)	Public IP address	: -
Subscription (move)	: Azure pour les étudiants	Virtual network/subnet	: demovm-vnet/default
Subscription ID	: 5dfcf723-ea7b-4a89-b344-86968954d351	DNS name	: -
Availability zone	: 1		
Tags (edit)	: Click here to add tags		

Virtual machine		Networking	
Computer name	demovm	Public IP address	-
Health state	-	Public IP address (IPv6)	-
Operating system	Windows (Windows Server 2019 Datacenter)	Private IP address	10.0.0.4
Publisher	MicrosoftWindowsServer	Private IP address (IPv6)	-
Offer	WindowsServer	Virtual network/subnet	demovm-vnet/default
Plan	2019-datacenter-gensecond	DNS name	-
VM generation	V2		



Home > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230420202856 | Overview >

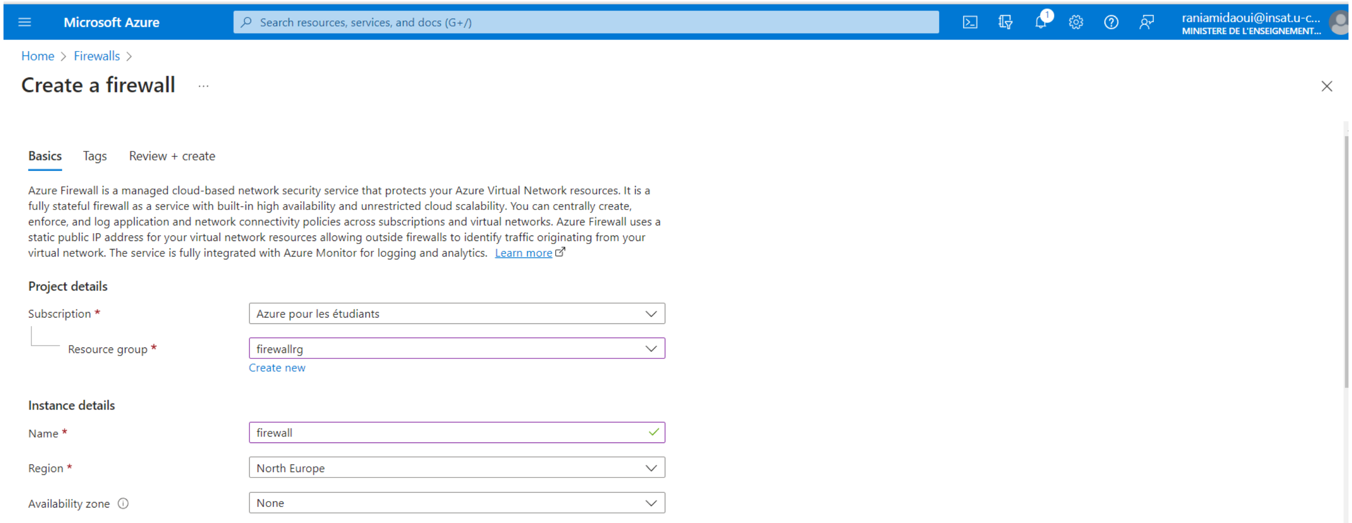
demovm
Virtual machine

Essentials

Resource group (move)	: firewallrg	Operating system	: Windows (Windows Server 2019 Datacenter)
Status	: Running	Size	: Standard B1s (1 vcpu, 1 GiB memory)
Location	: North Europe (Zone 1)	Public IP address	: -
Subscription (move)	: Azure pour les étudiants	Virtual network/subnet	: demovm-vnet/default
Subscription ID	: 5dfcf723-ea7b-4a89-b344-86968954d351	DNS name	: -
Availability zone	: 1		
Tags (edit)	: Click here to add tags		

Virtual machine		Networking	
Computer name	demovm	Public IP address	-
Health state	-	Public IP address (IPv6)	-
Operating system	Windows (Windows Server 2019 Datacenter)	Private IP address	10.0.0.4
Publisher	MicrosoftWindowsServer	Private IP address (IPv6)	-
Offer	WindowsServer	Virtual network/subnet	demovm-vnet/default
Plan	2019-datacenter-gensecond	DNS name	-
VM generation	V2		

2- We create a firewall:



Microsoft Azure | Search resources, services, and docs (G+/) | raniamidaoui@insat.u-c... MINISTERE DE L'ENSEIGNEMENT...

Home > Firewalls >

Create a firewall

Basics | Tags | Review + create

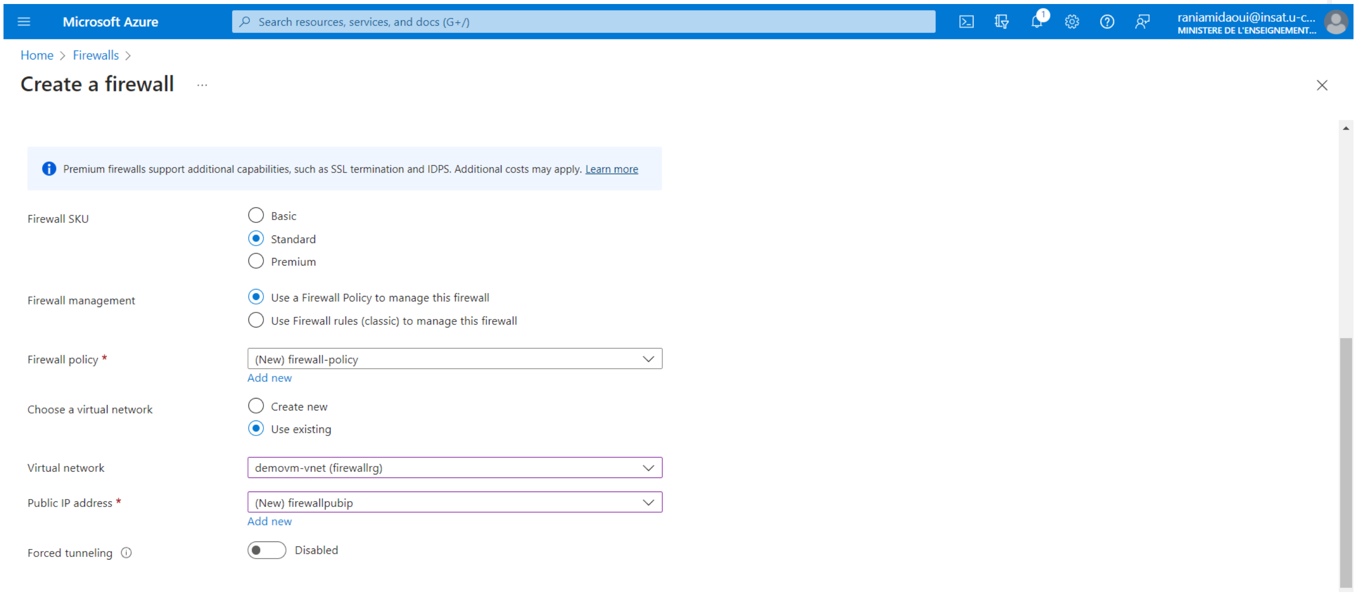
Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity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

Project details

Subscription *	Azure pour les étudiants
Resource group *	firewallrg Create new

Instance details

Name *	firewall
Region *	North Europe
Availability zone	None



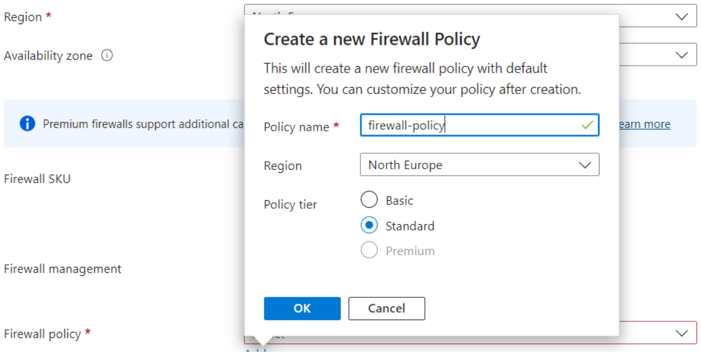
Microsoft Azure | Search resources, services, and docs (G+/) | raniamidaoui@insat.u-c... MINISTERE DE L'ENSEIGNEMENT...

Home > Firewalls >

Create a firewall

Premium firewalls support additional capabilities, such as SSL termination and IDPS. Additional costs may apply. Learn more

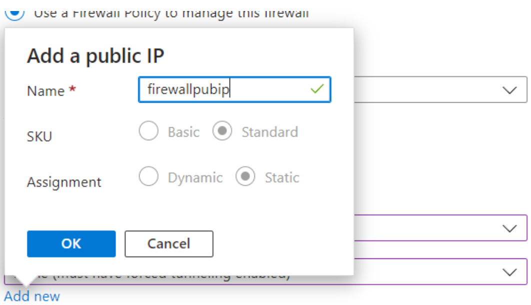
Firewall SKU	○ Basic ● Standard ○ Premium
Firewall management	● Use a Firewall Policy to manage this firewall ○ Use Firewall rules (classic) to manage this firewall
Firewall policy *	(New) firewall-policy Add new
Choose a virtual network	○ Create new ● Use existing
Virtual network	demovm-vnet (firewallrg)
Public IP address *	(New) firewallpubip Add new
Forced tunneling	Disabled



Create a new Firewall Policy

This will create a new firewall policy with default settings. You can customize your policy after creation.

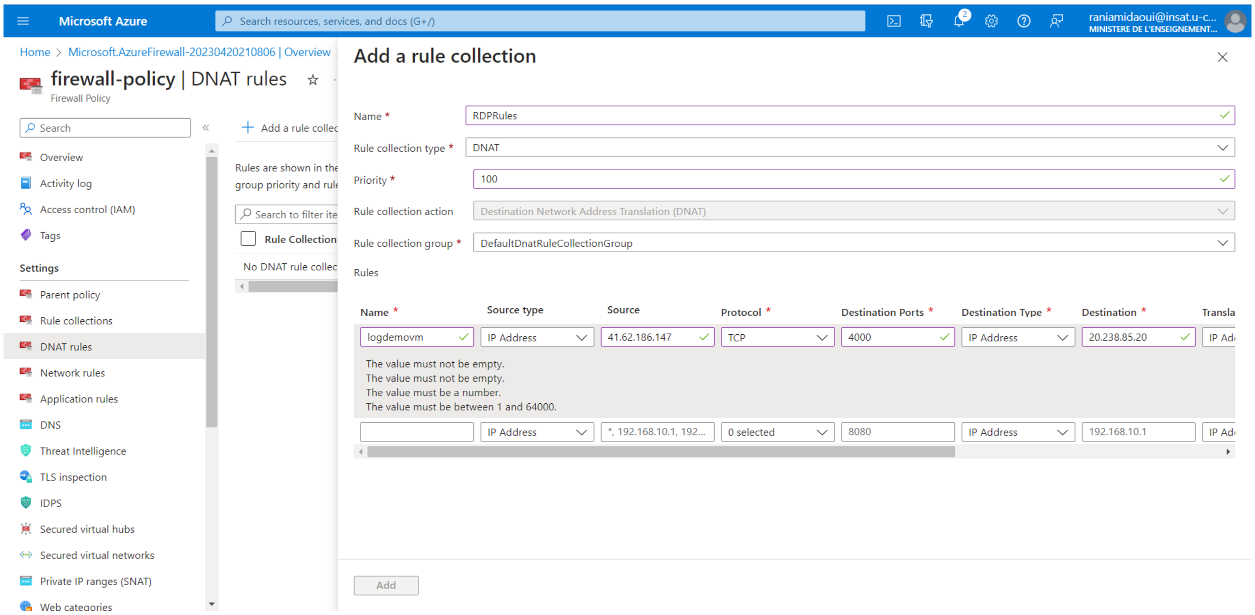
Policy name *	firewall-policy
Region	North Europe
Policy tier	○ Basic ● Standard ○ Premium



Add a public IP

Name *	firewallpubip
SKU	○ Basic ● Standard
Assignment	○ Dynamic ● Static

3- We add a DNAT rule:



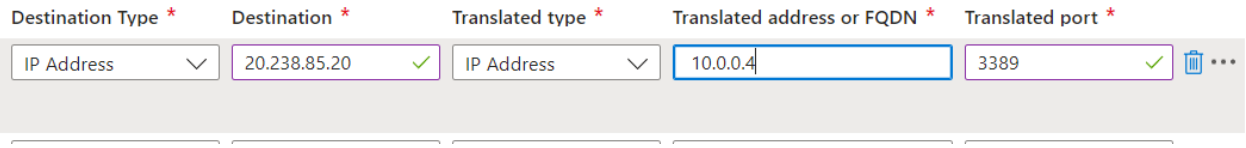
Add a rule collection

Name *	RDPRules
Rule collection type *	DNAT
Priority *	100
Rule collection action	Destination Network Address Translation (DNAT)
Rule collection group *	DefaultDnatRuleCollectionGroup

Rules

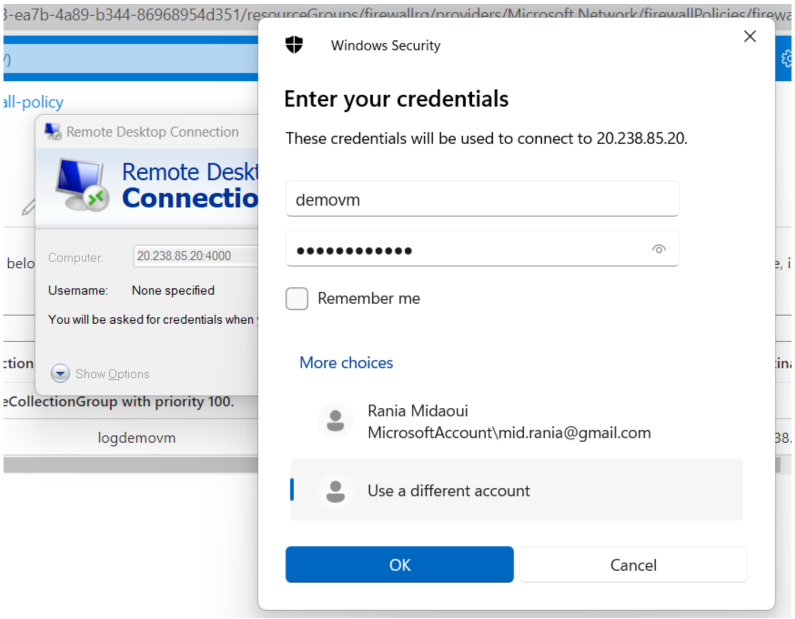
Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *	Transla
logdemovm	IP Address	41.62.186.147	TCP	4000	IP Address	20.238.85.20	IP Ad
	IP Address	*, 192.168.10.1, 192...	0 selected	8080	IP Address	192.168.10.1	IP Ad

The value must not be empty.
The value must not be empty.
The value must be a number.
The value must be between 1 and 64000.



Destination Type *	Destination *	Translated type *	Translated address or FQDN *	Translated port *
IP Address	20.238.85.20	IP Address	10.0.0.4	3389

4- We access the vm via RDP, using the port we defined:


3-ea7b-4a89-b344-86968954d351/resourceGroups/firewallrg/providers/Microsoft.Network/firewallPolicies/firewa
all-policy
Remote Desktop Connection
Remote Deskt
Connectio
belo
ction
eCollectionGroup with priority 100.
logdemovm
Show Options

Computer: 20.238.85.20:4000

Username: None specified

You will be asked for credentials when

Windows Security

Enter your credentials

These credentials will be used to connect to 20.238.85.20.

demovm

•••••••••••••

□ Remember me

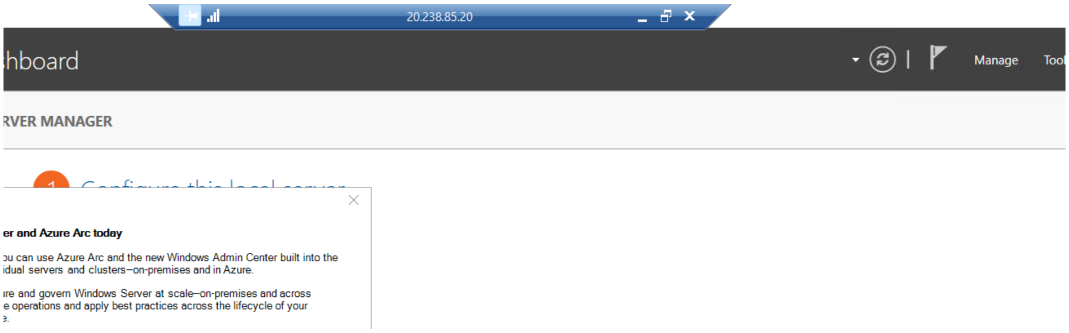
More choices

Rania Midaoui
MicrosoftAccount\mid.rania@gmail.com

Use a different account

OK | Cancel

And we're connected!!

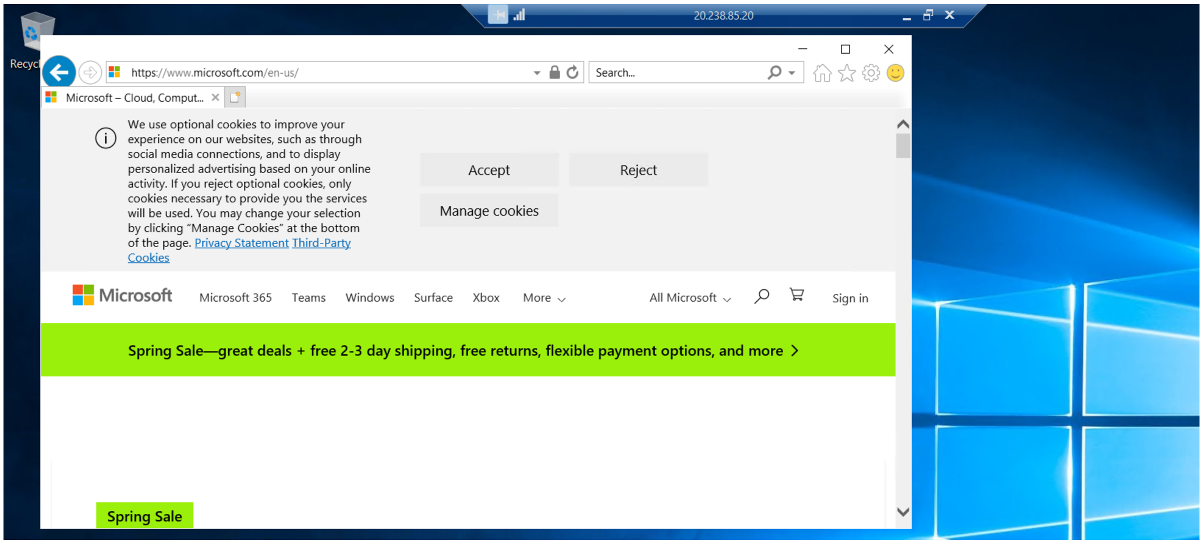


er and Azure Arc today

ou can use Azure Arc and the new Windows Admin Center built into the idual servers and clusters—on-premises and in Azure.

ıre and govern Windows Server at scale–on-premises and across e operations and apply best practices across the lifecycle of your e.

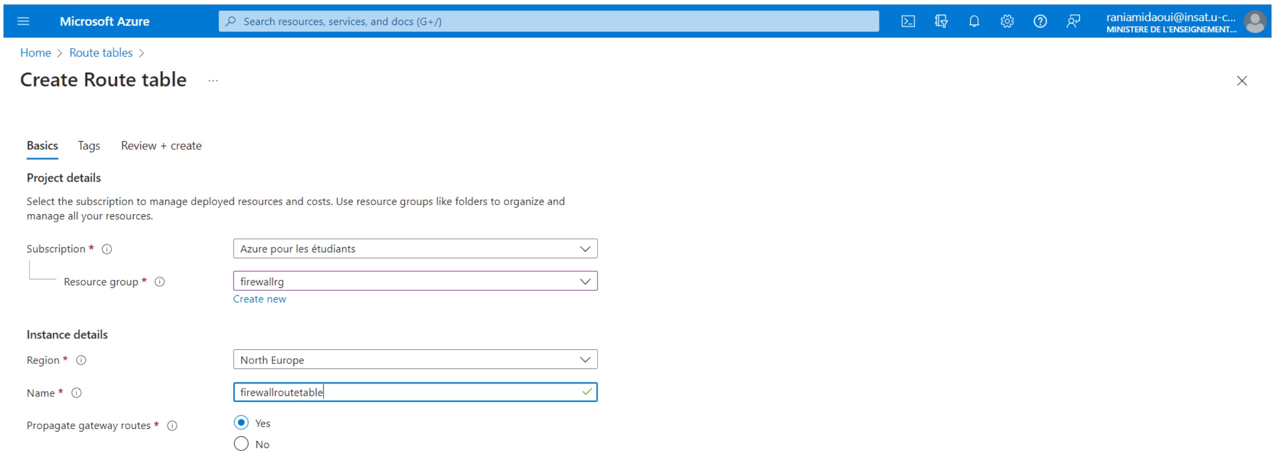
5- We are able to reach www.microsoft.com from the VM:



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. Privacy Statement Third-Party Cookies

Spring Sale—great deals + free 2-3 day shipping, free returns, flexible payment options, and more >

6-


Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Route tables >
Basics
Tags
Review + create
Create new

Create Route table

Project details

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

Subscription *: Azure pour les étudiants

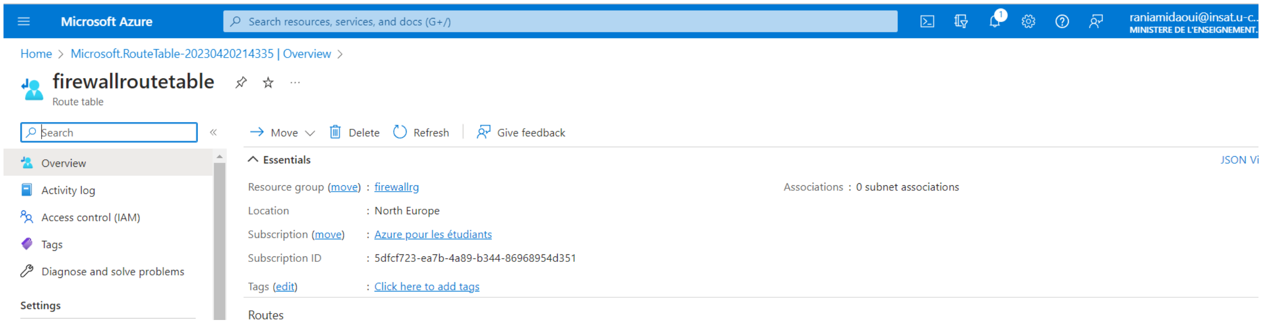
Resource group *: firewallrg

Instance details

Region *: North Europe

Name *: firewallroutetable

Propagate gateway routes *: ● Yes ○ No


Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Microsoft.RouteTable-20230420214335 | Overview >
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Move
Delete
Refresh
Give feedback
JSON Vi

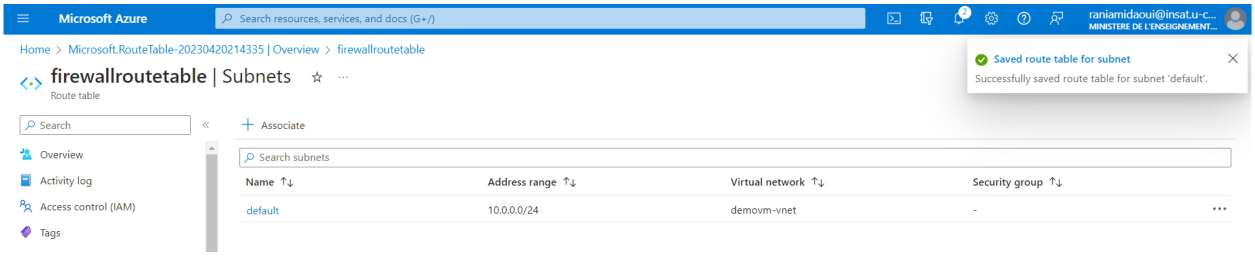
firewallroutetable
Route table

Essentials

Resource group (move) : firewallrg
Location : North Europe
Subscription (move) : Azure pour les étudiants
Subscription ID : 5dfcf723-ea7b-4a89-b344-86968954d351
Tags (edit) : Click here to add tags
Associations : 0 subnet associations

Routes

7- We associate the default subnet:

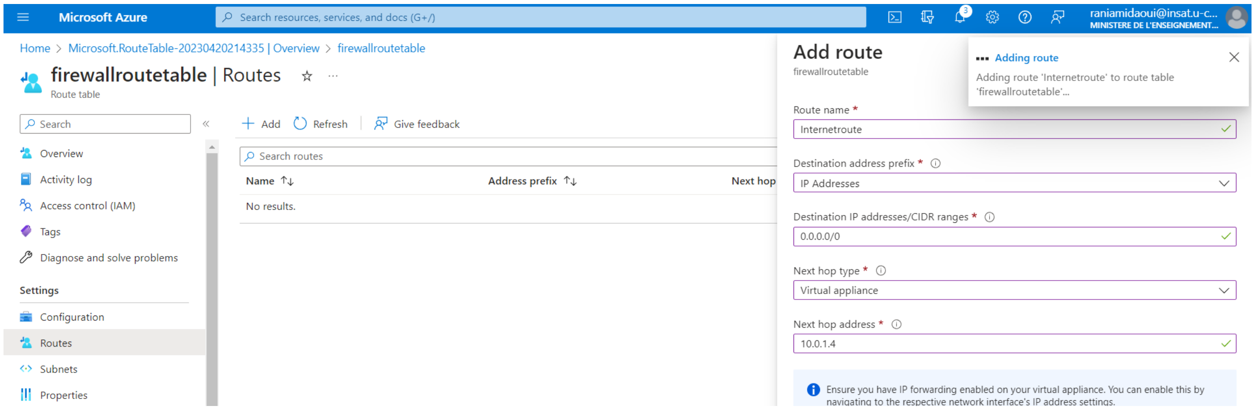

Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Microsoft.RouteTable-20230420214335 | Overview > firewallroutetable
Search
Overview
Activity log
Access control (IAM)
Tags
Associate
Search subnets

firewallroutetable | Subnets
Route table

Saved route table for subnet
Successfully saved route table for subnet 'default'.

Name	Address range	Virtual network	Security group
default	10.0.0.0/24	demovm-vnet	-

then, we add a route:


Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Microsoft.RouteTable-20230420214335 | Overview > firewallroutetable
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Routes
Subnets
Properties
Add
Refresh
Give feedback
Search routes

firewallroutetable | Routes
Route table

Name	Address prefix	Next hop
No results.		

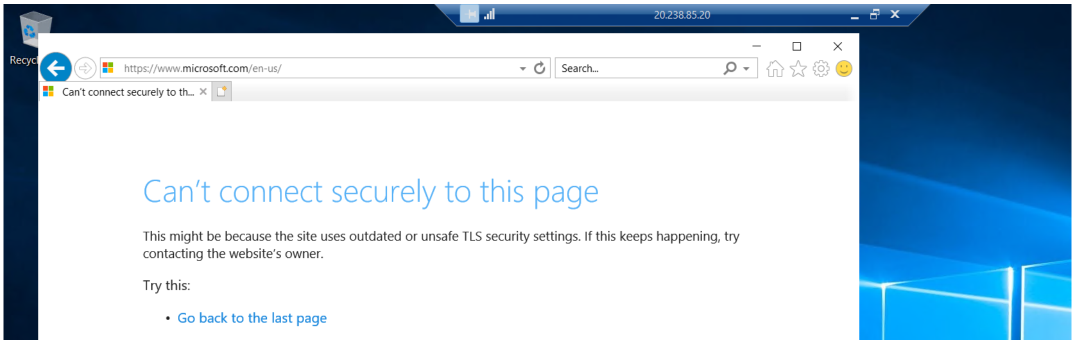
Add route
firewallroutetable

Adding route
Adding route 'Internetroute' to route table 'firewallroutetable'...

Route name * : Internetroute
Destination address prefix * : IP Addresses
Destination IP addresses/CIDR ranges * : 0.0.0.0/0
Next hop type * : Virtual appliance
Next hop address * : 10.0.1.4

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.

8- Now, if we try to access the microsoft page from the VM, the action will be denied:


20.238.85.20
Recyc
https://www.microsoft.com/en-us/
Search...
Can't connect securely to th...

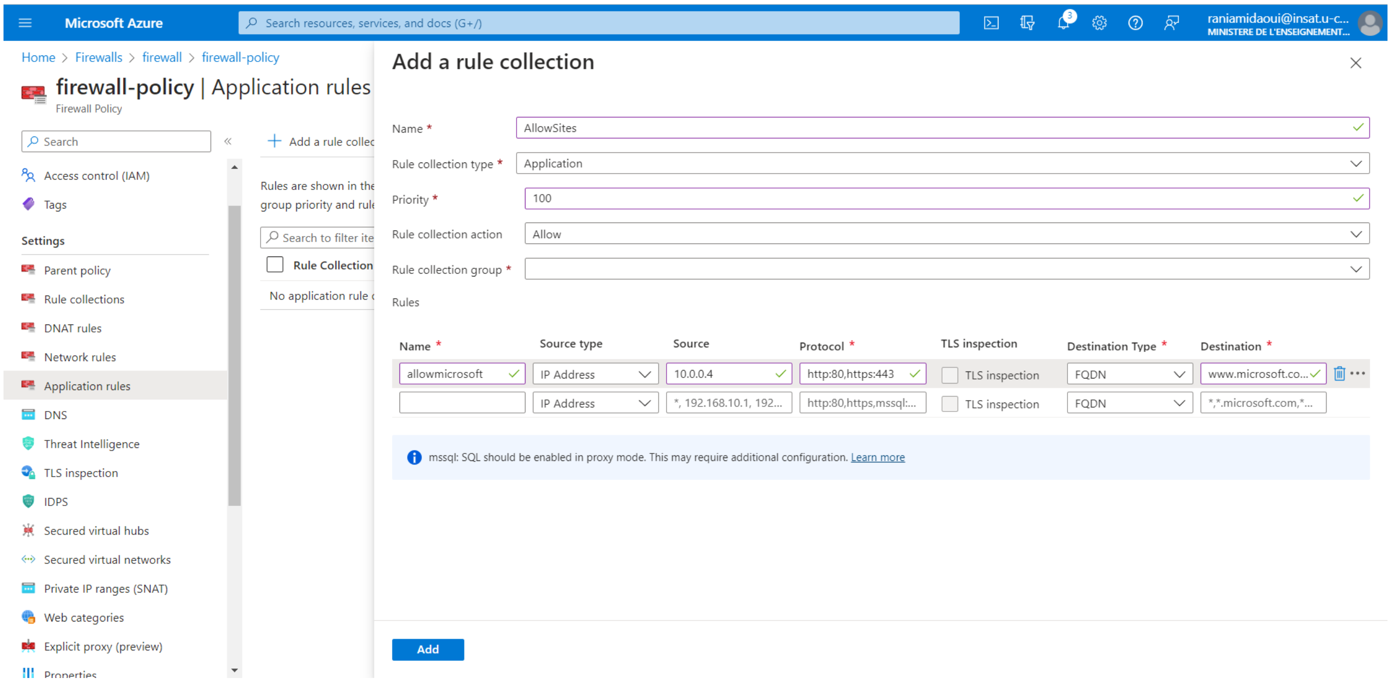
Can't connect securely to this page

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

9- We create an application rule to allow traffic onto the website:



Add a rule collection

Name * AllowSites

Rule collection type * Application

Priority * 100

Rule collection action Allow

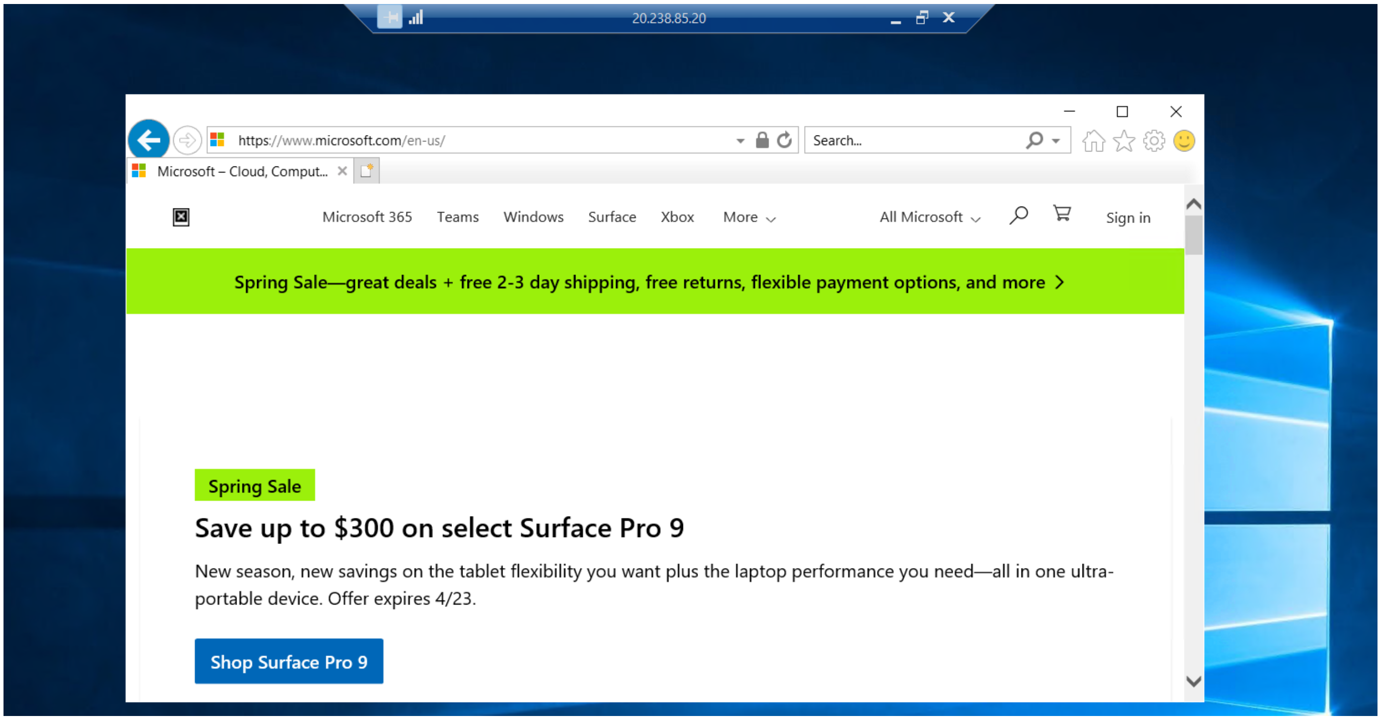
Rule collection group *

Rules

Name *	Source type	Source	Protocol *	TLS inspection	Destination Type *	Destination *
allowmicrosoft	IP Address	10.0.0.4	http:80,https:443	□ TLS inspection	FQDN	www.microsoft.co...
	IP Address	*, 192.168.10.1, 192...	http:80,https,mssql:...	□ TLS inspection	FQDN	*,*.microsoft.com,*...

mssql: SQL should be enabled in proxy mode. This may require additional configuration. Learn more

10- We are now able to reach the website from the VM!



https://www.microsoft.com/en-us/

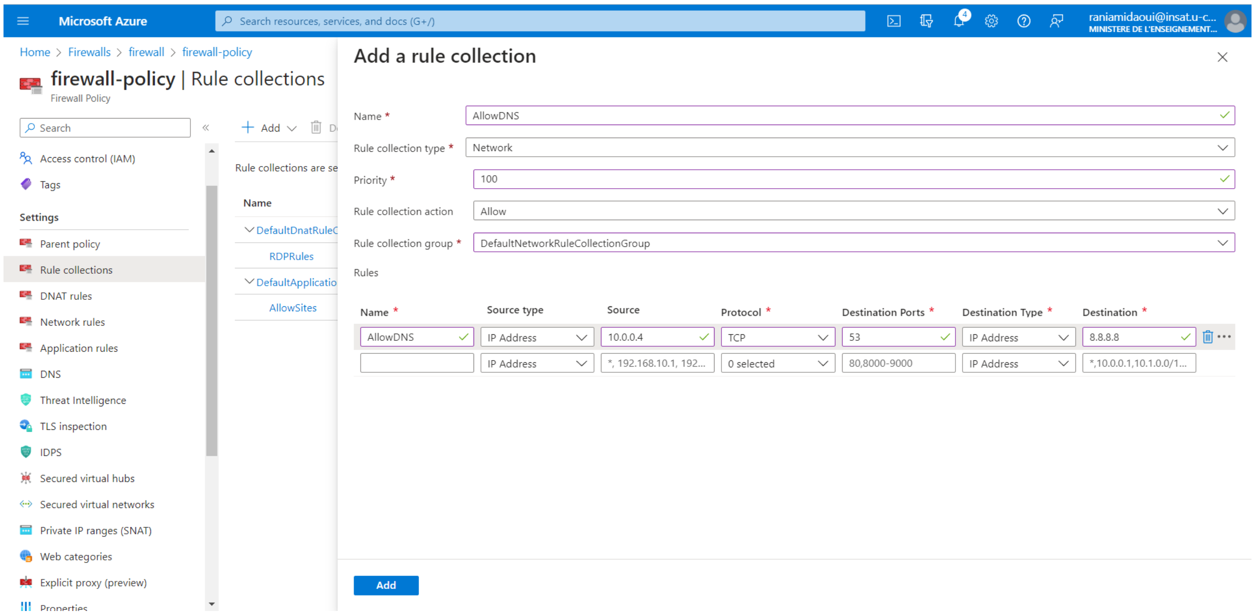
Spring Sale—great deals + free 2-3 day shipping, free returns, flexible payment options, and more >

Spring Sale

Save up to $300 on select Surface Pro 9

New season, new savings on the tablet flexibility you want plus the laptop performance you need—all in one ultra-portable device. Offer expires 4/23.

11- We add a network rule to allow collection to allow “demovm” to access the DNS server 8.8.8.8:



Add a rule collection

Name * AllowDNS

Rule collection type * Network

Priority * 100

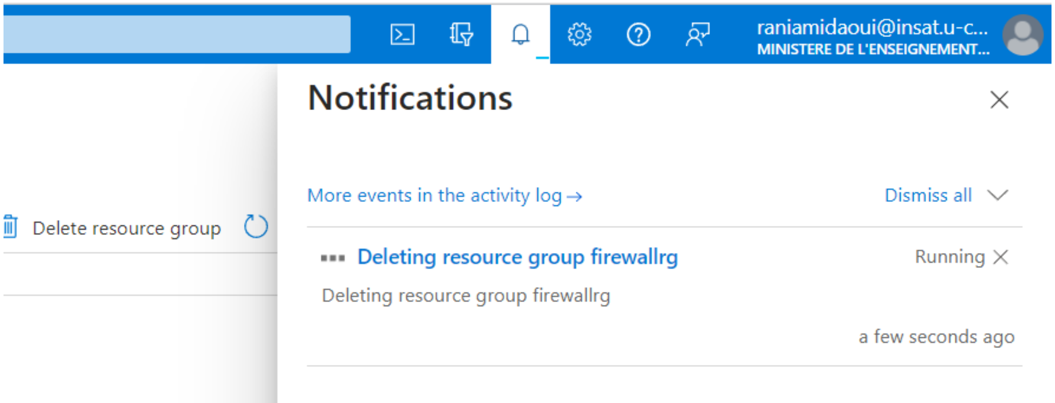
Rule collection action Allow

Rule collection group * DefaultNetworkRuleCollectionGroup

Rules

Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *
AllowDNS	IP Address	10.0.0.4	TCP	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...

12- We delete the resource group:



Notifications

More events in the activity log →   Dismiss all

Deleting resource group firewallrg   Running

Deleting resource group firewallrg

a few seconds ago

Conclusion:

This TP on Azure Traffic Manager, Front Door, and Firewall demonstrates the significant benefits these services can provide for businesses. Azure Traffic Manager improves availability and reliability by distributing traffic across multiple endpoints, while Azure Front Door optimizes routing and improves performance for global application delivery. Azure Firewall simplifies network security management for businesses migrating to the cloud. These cloud-based solutions offer powerful network security and performance optimization, and are worth considering for businesses looking to enhance their network infrastructure.