Securing Hybrid Cloud in Azure

Student Lab Guide

version 1

FORTINET®

Training Institute

Fortinet Training Institute - Library

https://www.fortinet.com

Fortinet Product Document

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

20 January 2026

Table of Contents

Lab Access Using the Azure Portal

Lab Environment

This lab is configured to allow each student to have their own training lab environment using pre-created Azure resource groups all in one shared Azure Subscription.

Azure Portal Lab Access

First, you must log in to the Azure Portal. Then, you will gain access to the lab environment.

To access the Azure Portal sign-in page

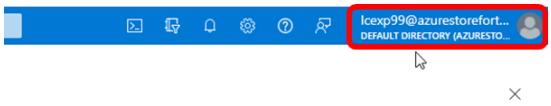
1. Open a browser, and then access the following URL:

   ```
   https://portal.azure.com
   ```

2. Use the credentials shared with you by your instructors. If you didn't find it, try looking at your junk mail too. Look for an email with a subject of: MIS - Xperts Summit - Public Cloud Track - AZURE LAB Credentials

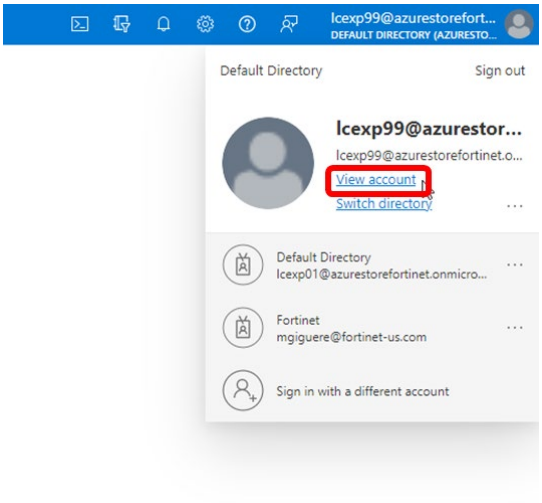
Username:	<user@domain received by email>
Password:	<password provided by email>

3. Click **Log in**.
4. Click on your own account name in the upper right corner

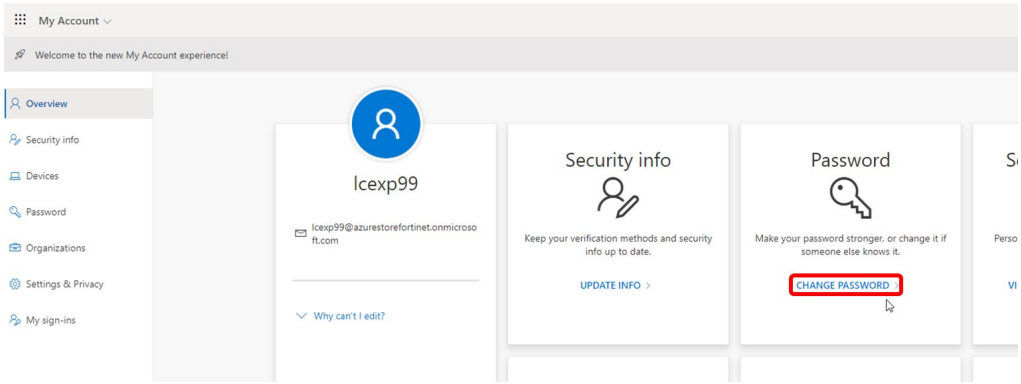


5. Click on **View Account** (which will automatically open a new tab)

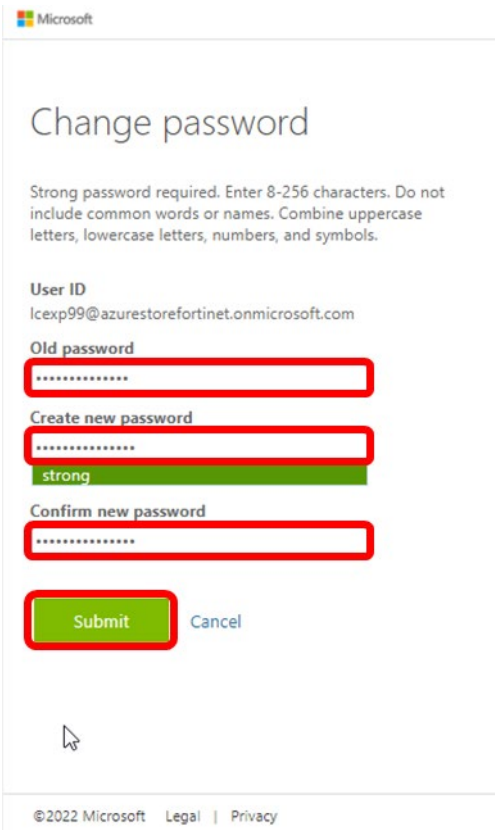
- Lab Access Using the Azure Portal



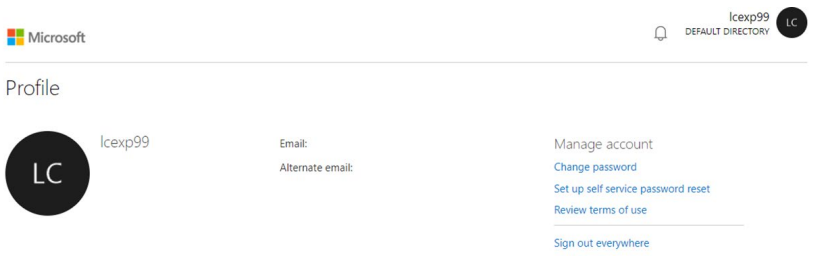
6. Click Change Password



7. Enter the necessary information to change your password then click **Submit**

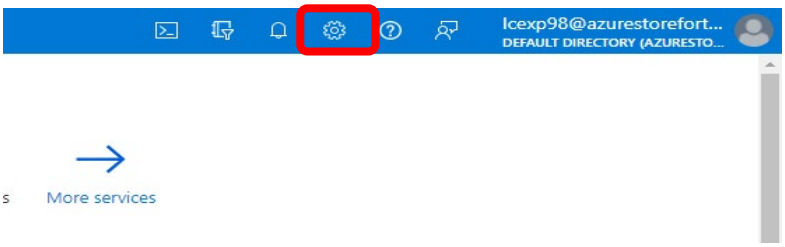


8. Upon seeing the following screen, this tab can be closed as the password was changed successfully.

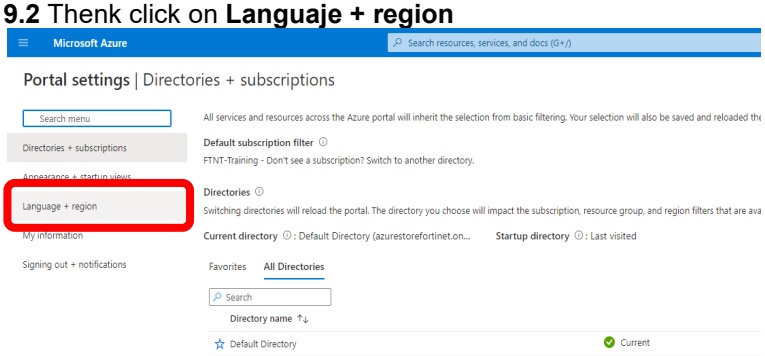


9. If you want to change your Azure dashboard language you can follow the next steps:

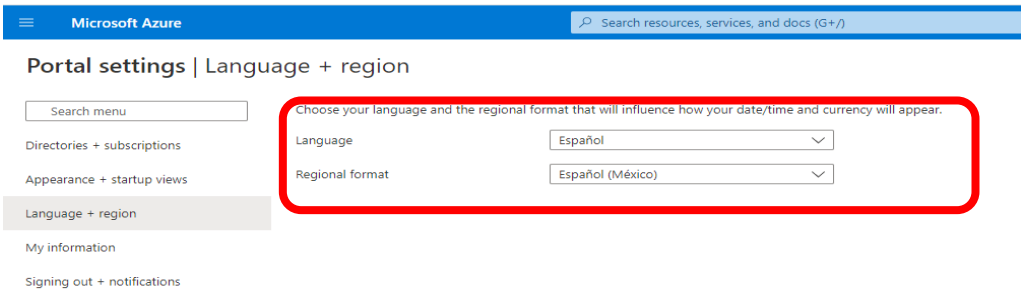
9.1 Once you are logged into your Azure account click on **gear icon** in the upper right corner



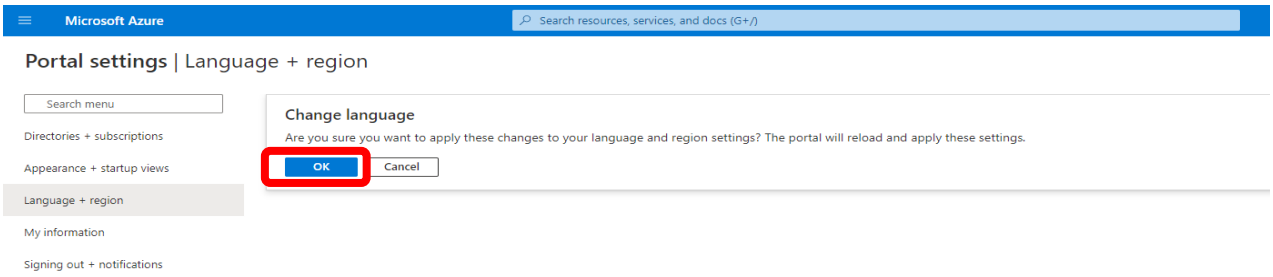
9.2 Thenk click on **Languaje + region**



9.3 Then you can choose the language and regional format of your preference. In this case “Español” to change the Dashboard language to Spanish.

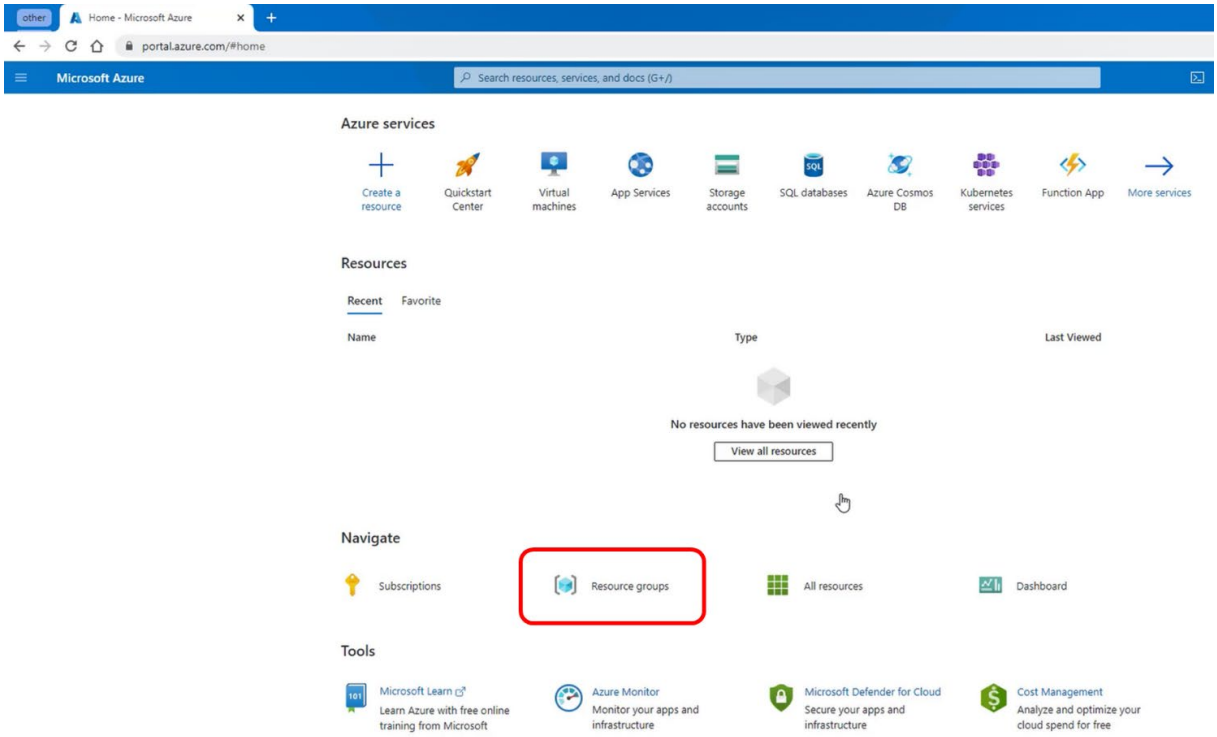


9.4 Click on **Apply.** A message will come up to ask if you are sure to change the language. Click on **OK** and that will save the change you made.

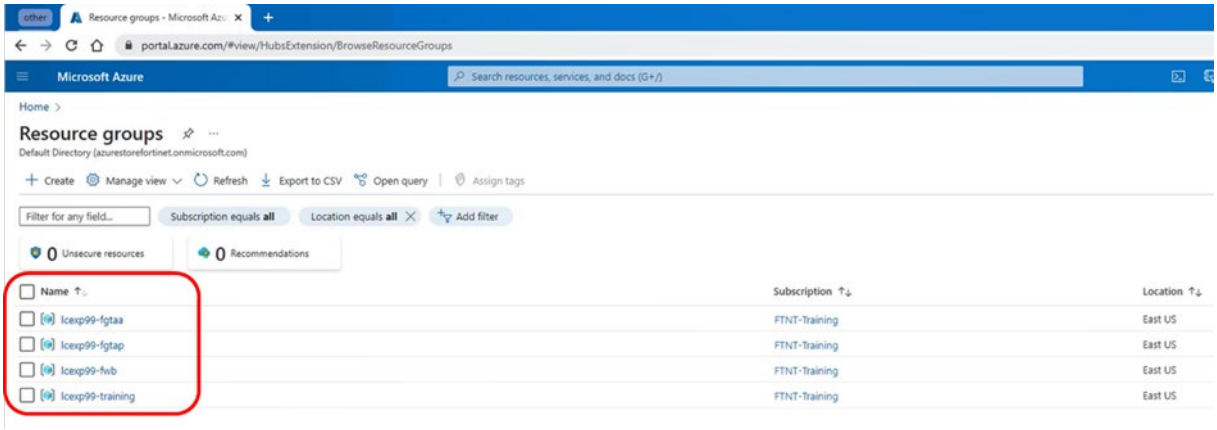


10. Of note, in the Azure account, which is a new Azure subscription, only four resource groups will be already there pre-created. All four will be used in this lab. No new ones can be created as resource groups are used as the basis of the individualization of the security in the lab environment

11. Click on Resource Groups in the main page.



12. Confirm the four resource groups are shown (with a different student number).



LAB 1— Securing Hybrid Cloud in Azure

The customer Global Gas company is moving to Azure as a lift and shift. This is due to their main datacenter and all its equipment is well passed its end of support by the various manufacturers.

The CIO is concerned about problems with the quality of communications and interruptions of the datacenter.

The new CISO needs to improve the level of compliance and auditing in the multi-cloud environment

In preparation for moving the various workload, the IT network security department is setting up a secure landing zone based on Azure Enterprise Scale using Fortinet.

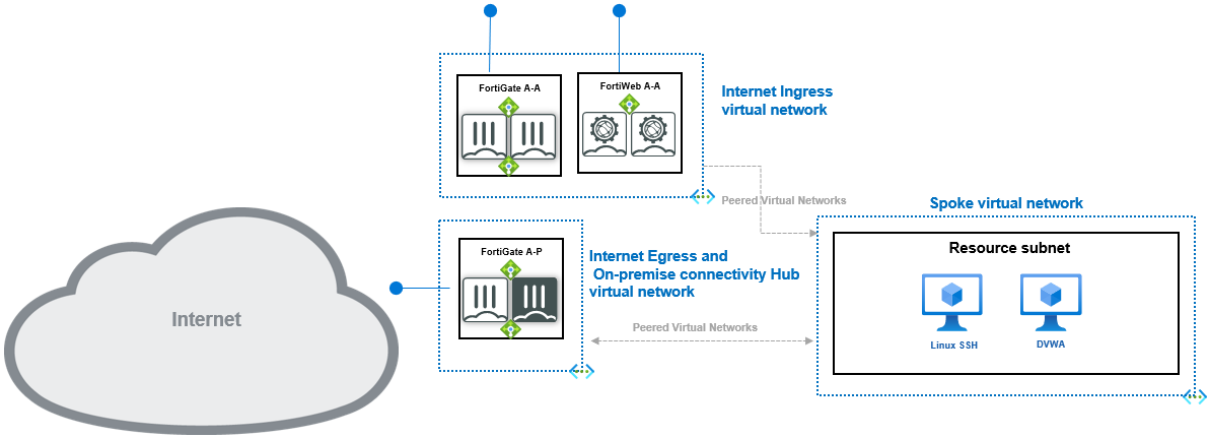
You are part of this team and will be the main person deploying and configuring in Azure the various network and security components.

Objectives

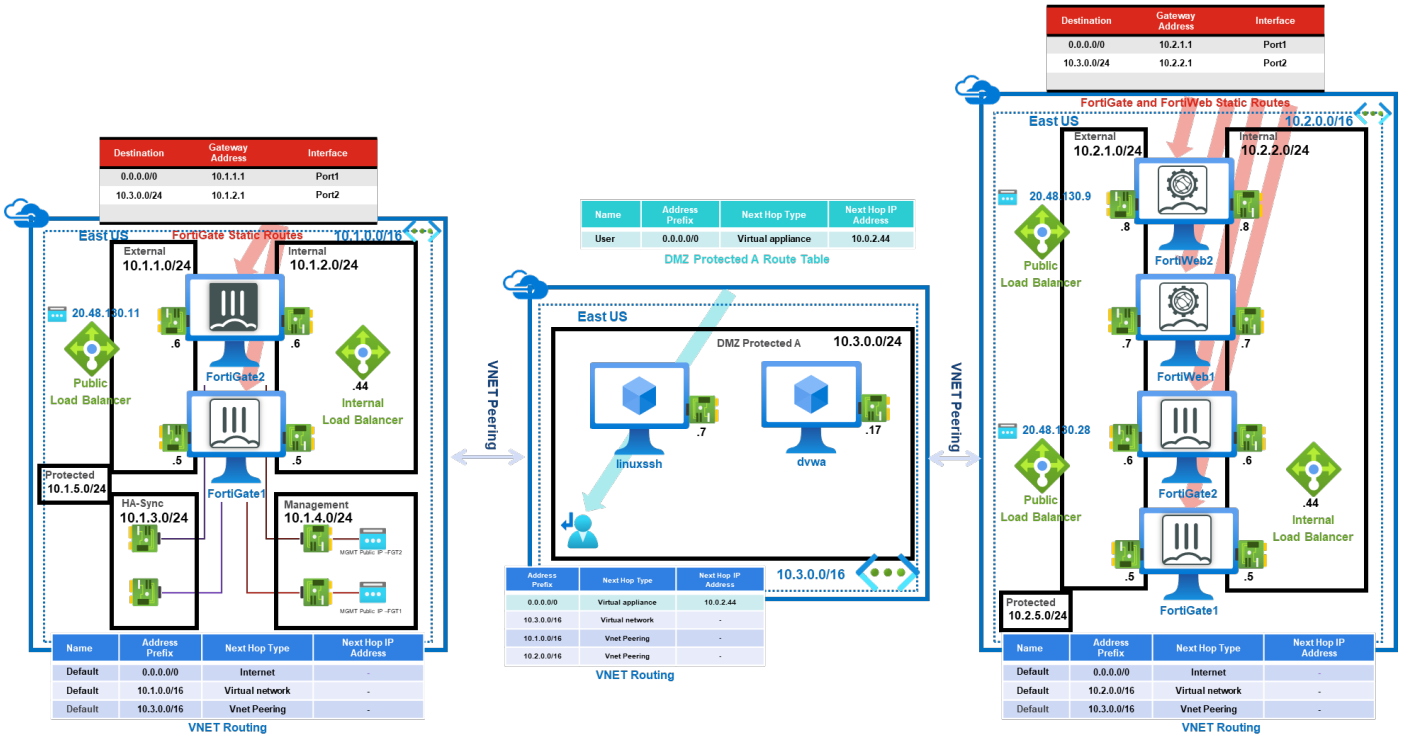
- Configure Azure resources
- Familiarize with Fortinet architecture in Azure
- Gain an understanding of networking and security in Azure leveraging Fortinet

Lab Diagrams

Network Topology



Detailed Architecture

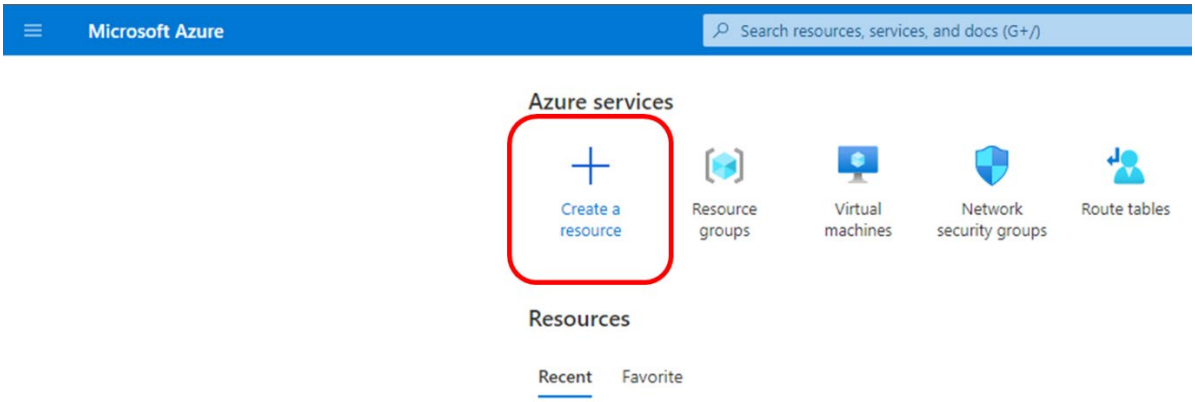


Task 1 - Creating a Virtual Network in Azure

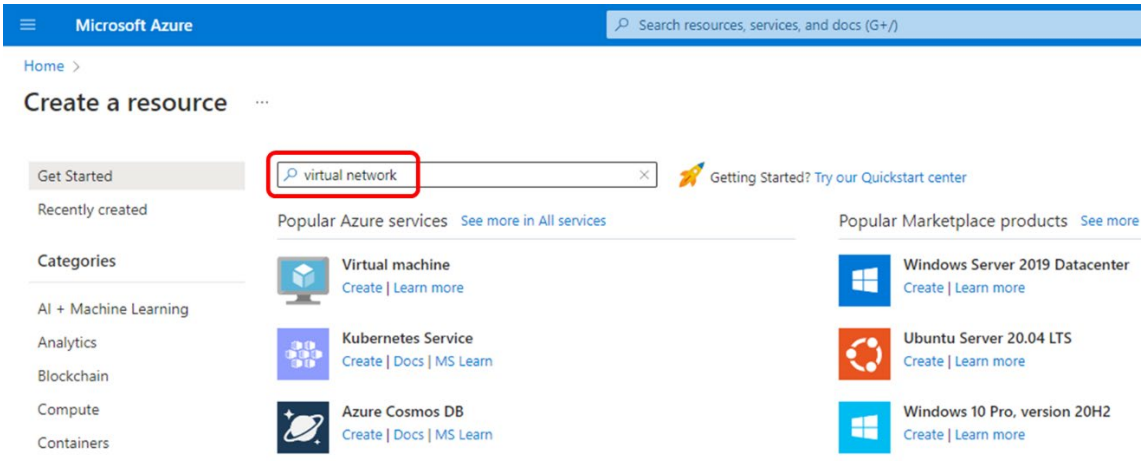
Our first step is going to be creation of a new VNET (Virtual Network) in the training Resource Group for the workload VNET.

Creation steps

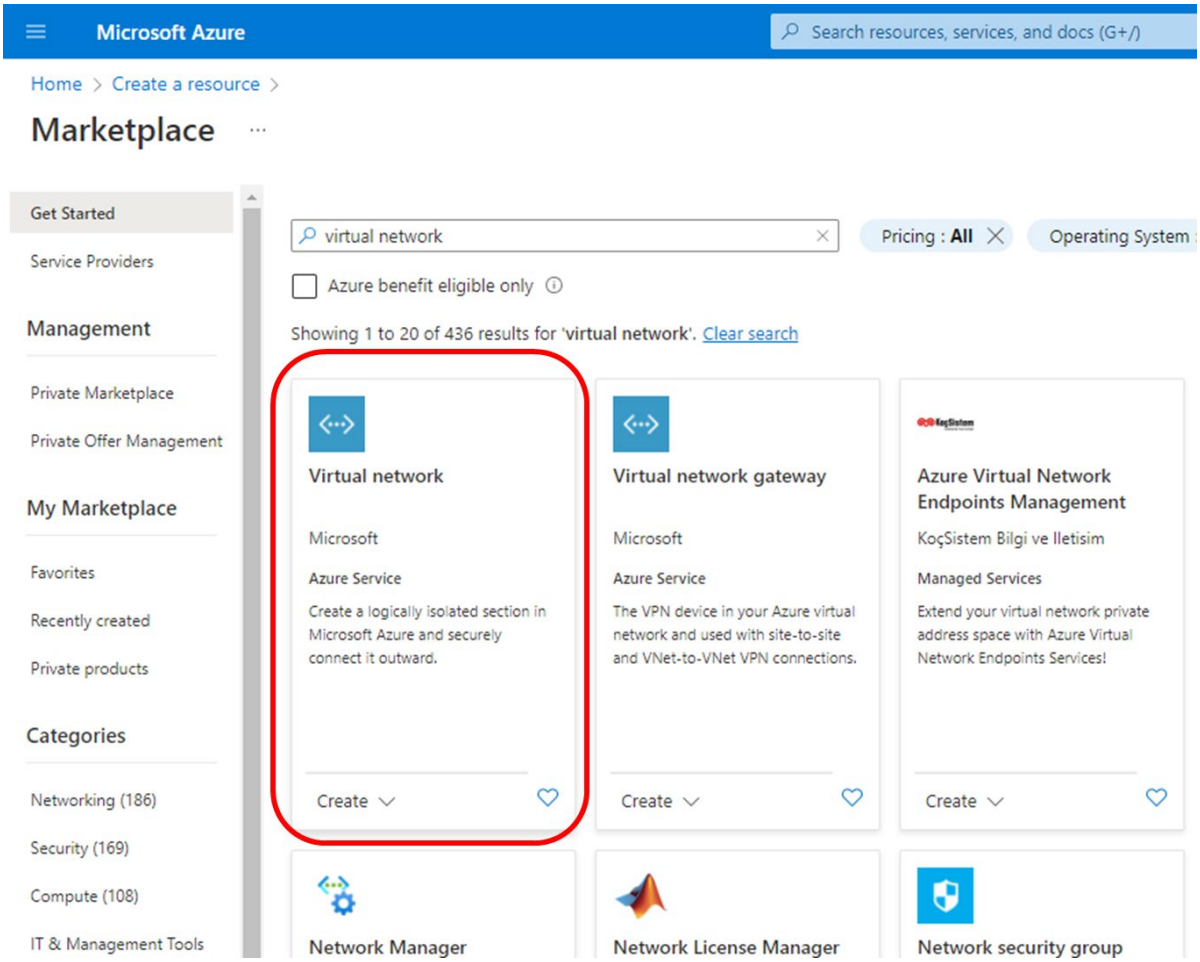
1. From the Azure Portal, click on **Create a resource**



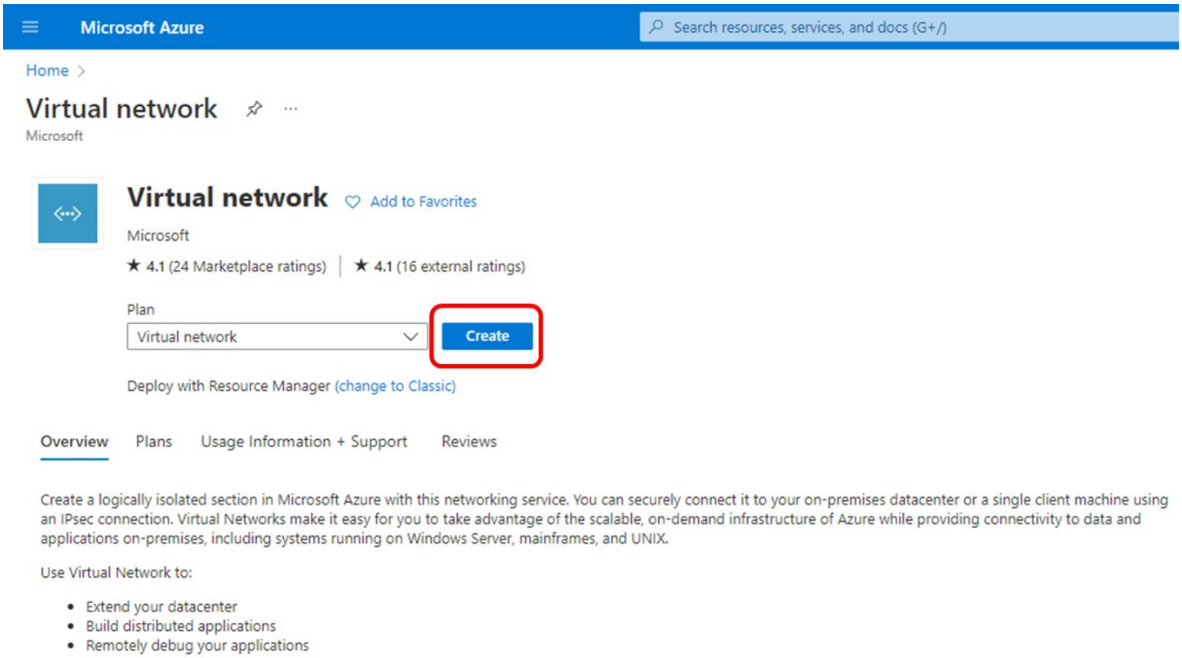
2. A new page will be displayed. Search for **Virtual Network** in the search bar and hit enter.



3. Click on **Virtual Network Azure service**

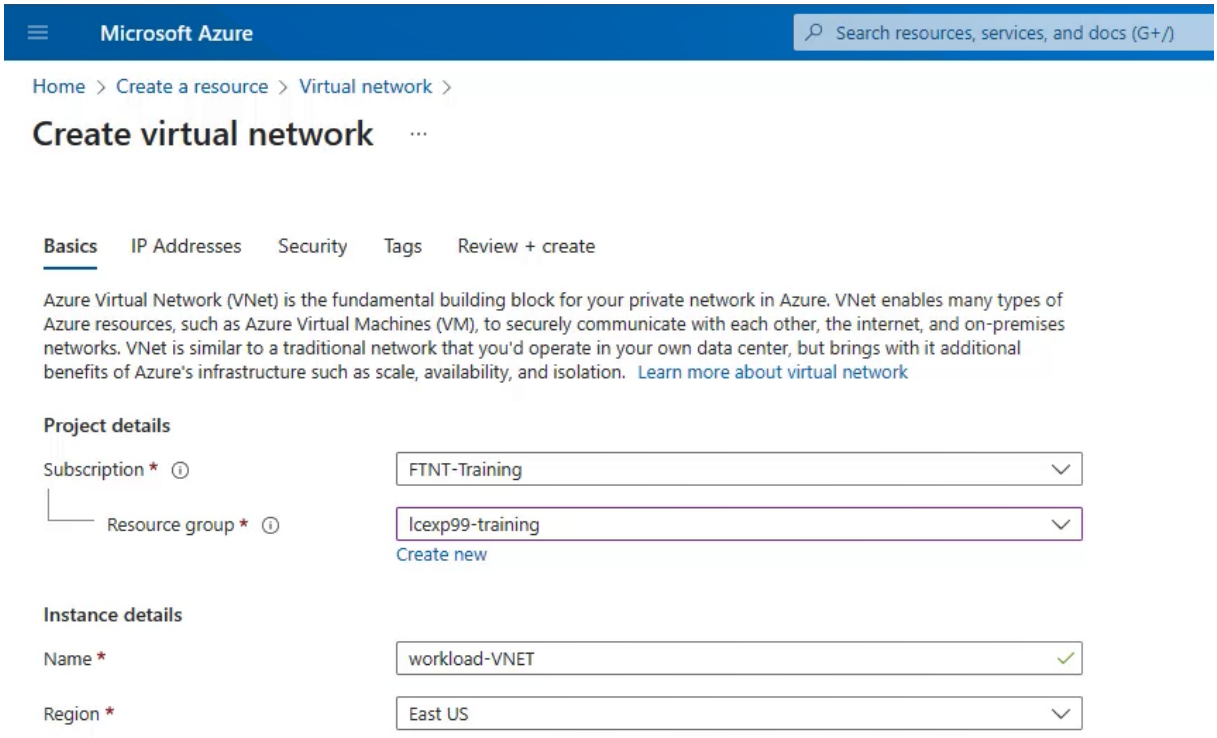


4. In the new pane, click **Create**

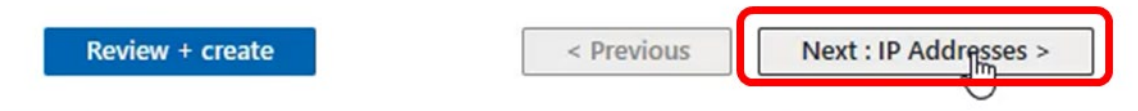


5. The VNET wizard will be opened. Fill in using the table below

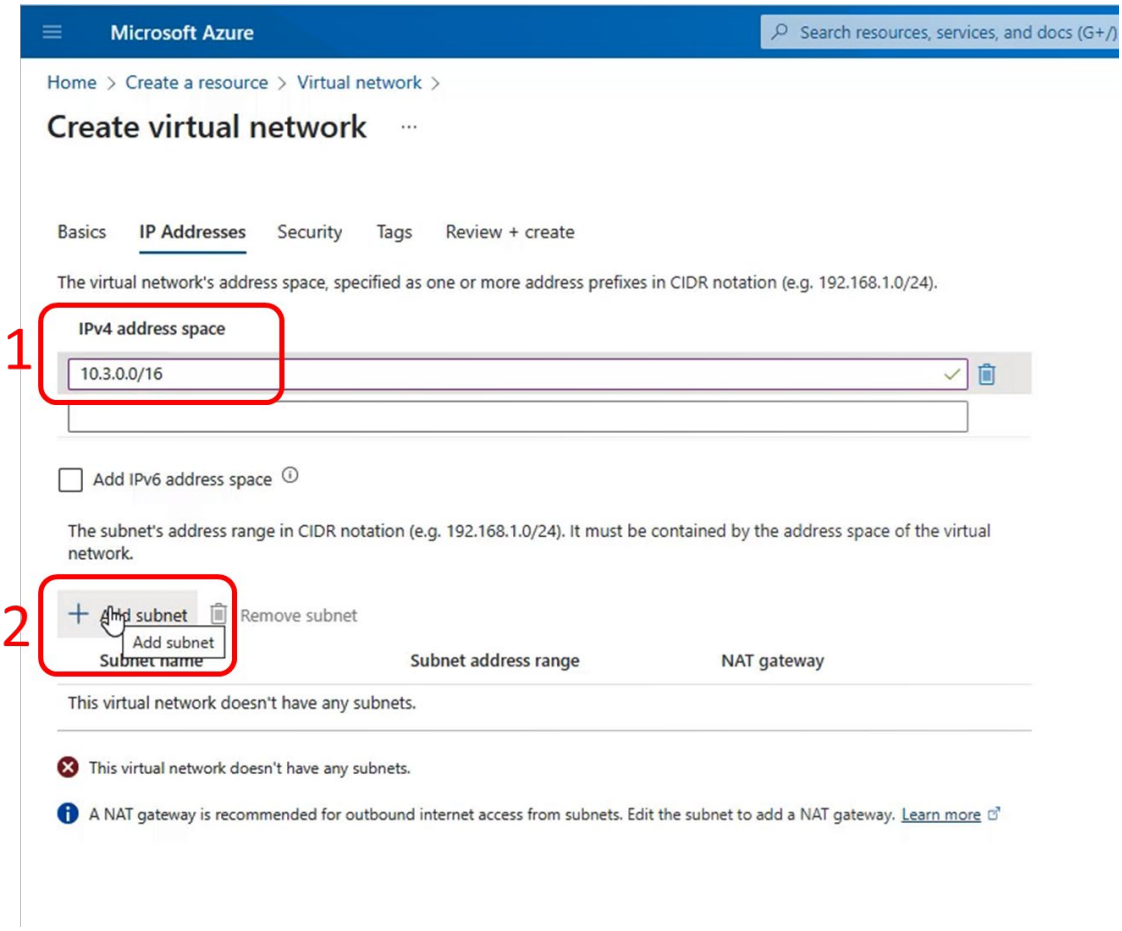
Subscription	FTNT-Training
Resource group	lcexp***<your student number>***-training
Instance Name	workload-VNET
Region	East US



6. Click on **Next: IP Addresses** or on the **IP Addresses** pane

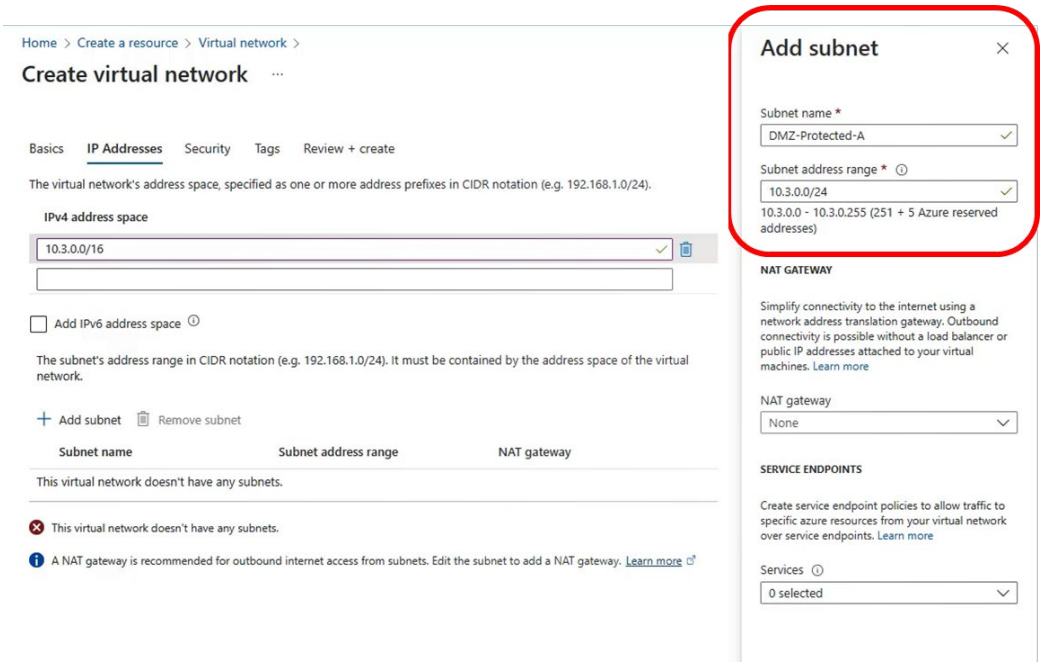


7. Add **10.3.0.0/16** into IPv4 address space and then click on “Add subnet”. The existing vNet information must be deleted.



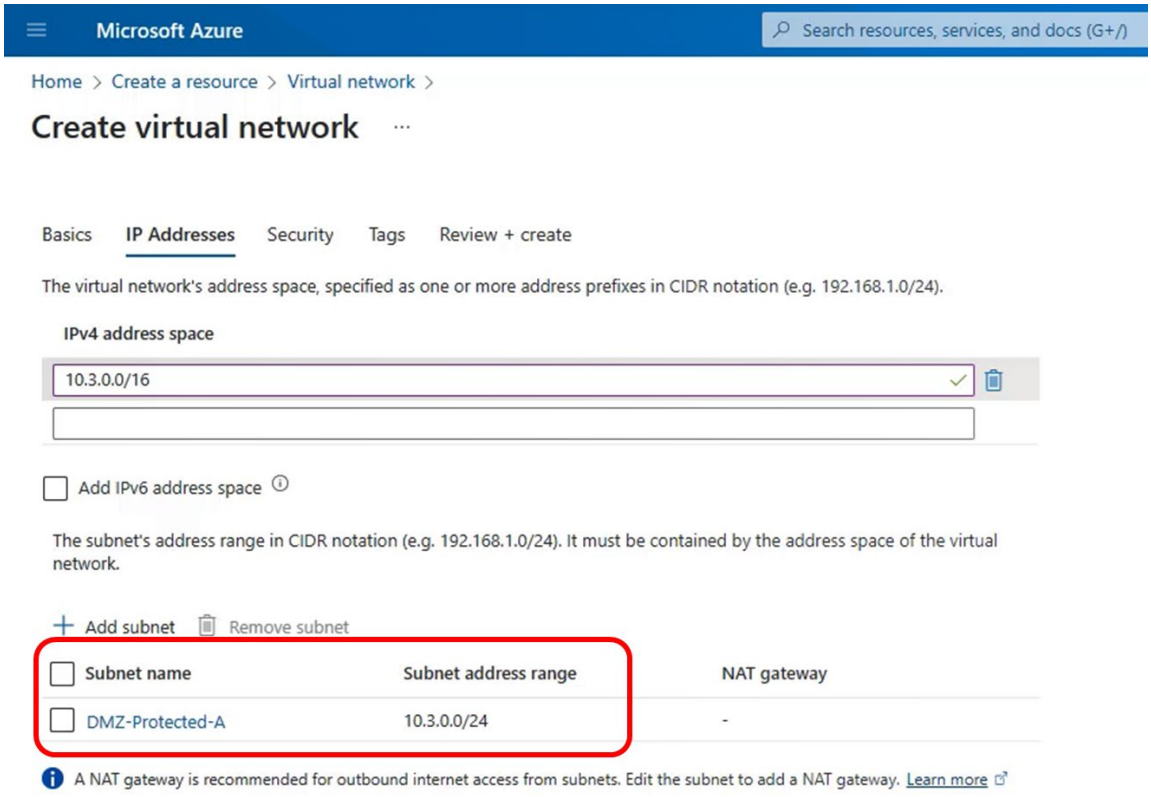
8. A new pane will open on the right side of the screen. Add a DMZ Network by adding

Subnet name	DMZ-Protected-A
Subnet address range	10.3.0.0/24

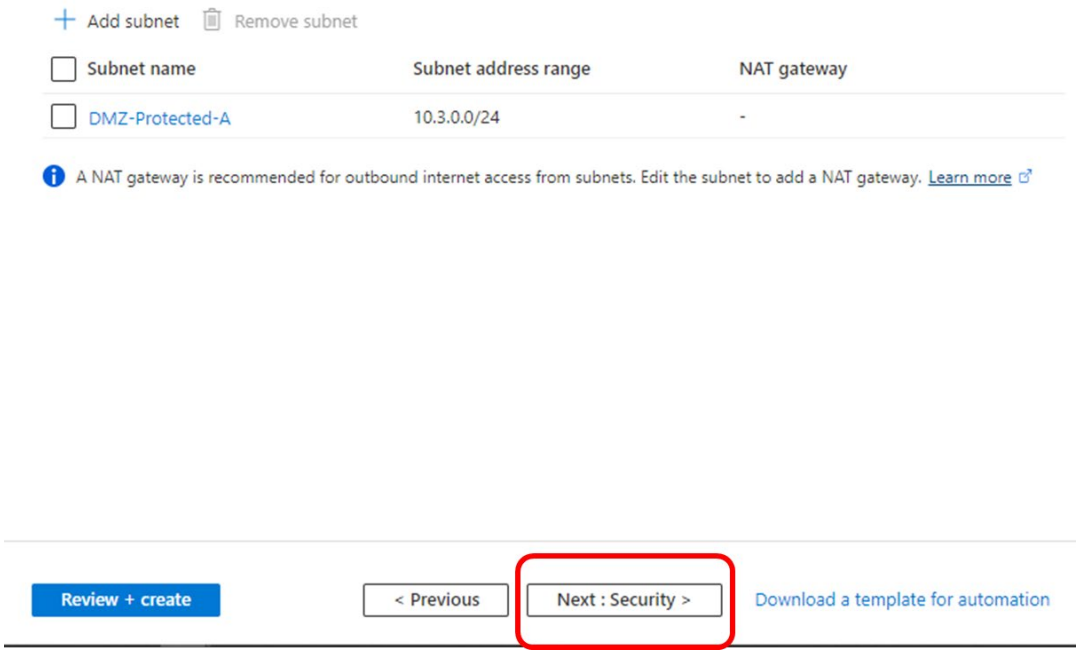


9. Click on **Add**

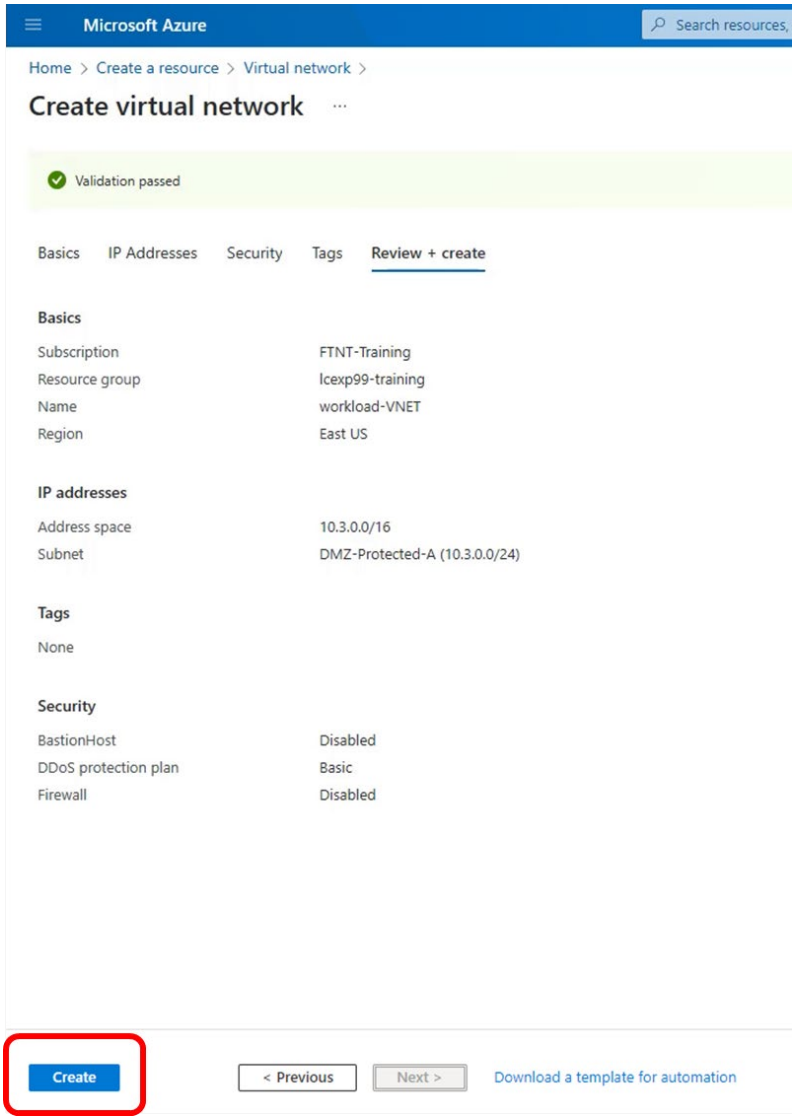
10. The DMZ subnet will then appear in the VNET configuration



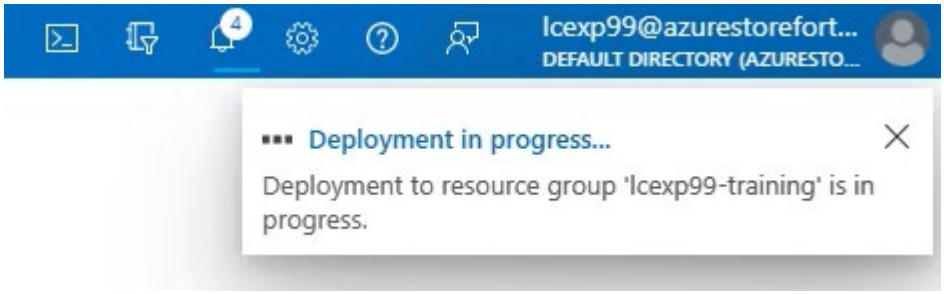
11. Click **Next: Security** or click on the Security pane, nothing will be changed there



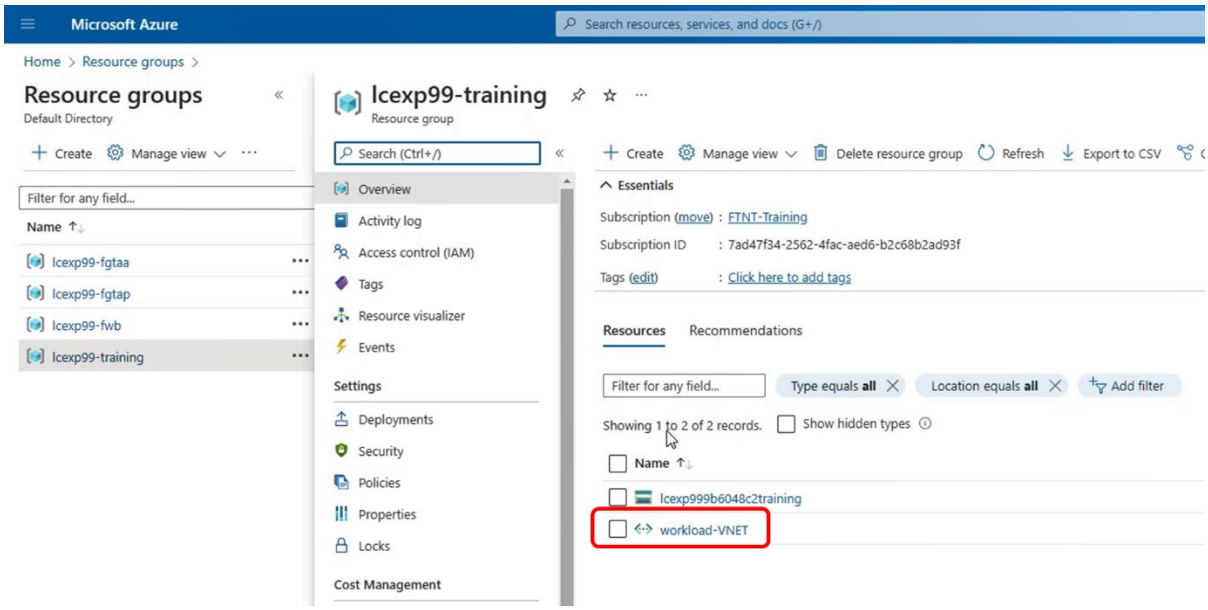
12. Then click on **Next: Tags** or click on the **Tags** pane, there is nothing to change there either
13. Verify that everything is set accordingly and click **Create**



14. The deployment of the VNET will start



15. Upon completion of the deployment, go to the list of Resource Groups, select the training Resource Group where after a few minutes the newly created VNET will appear (might require web browser refresh).



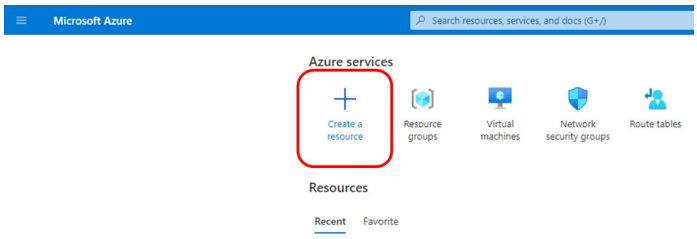
16. The Workload VNET was successfully created

Task 2 - Deploy linuxssh virtual machine

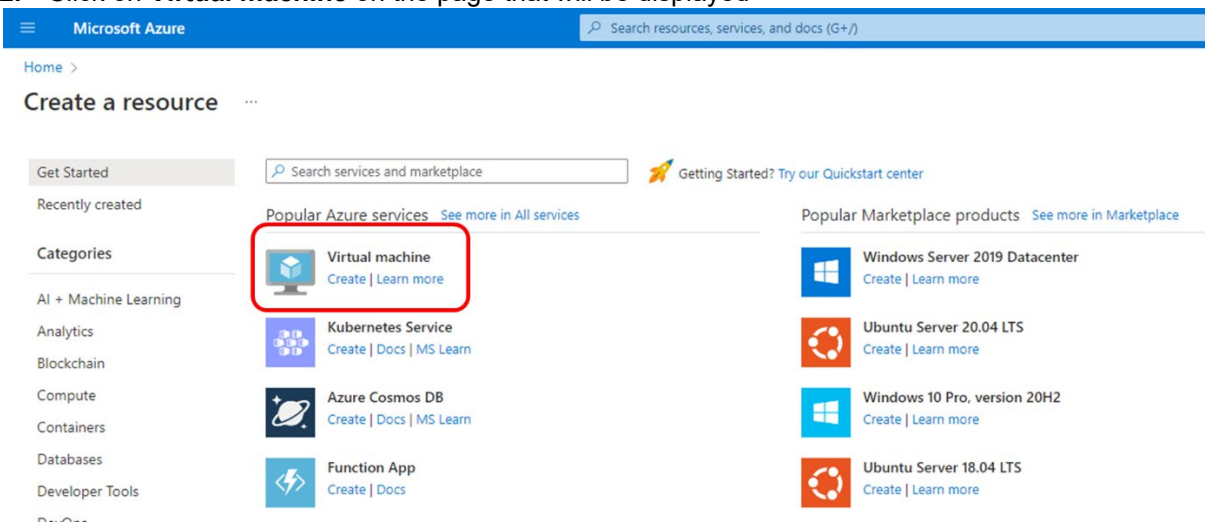
Our next step is going to be creation of a new VM (Virtual Machine) into the workload VNET.

Creation steps

1. From the main Azure Portal, click on **Create a resource**



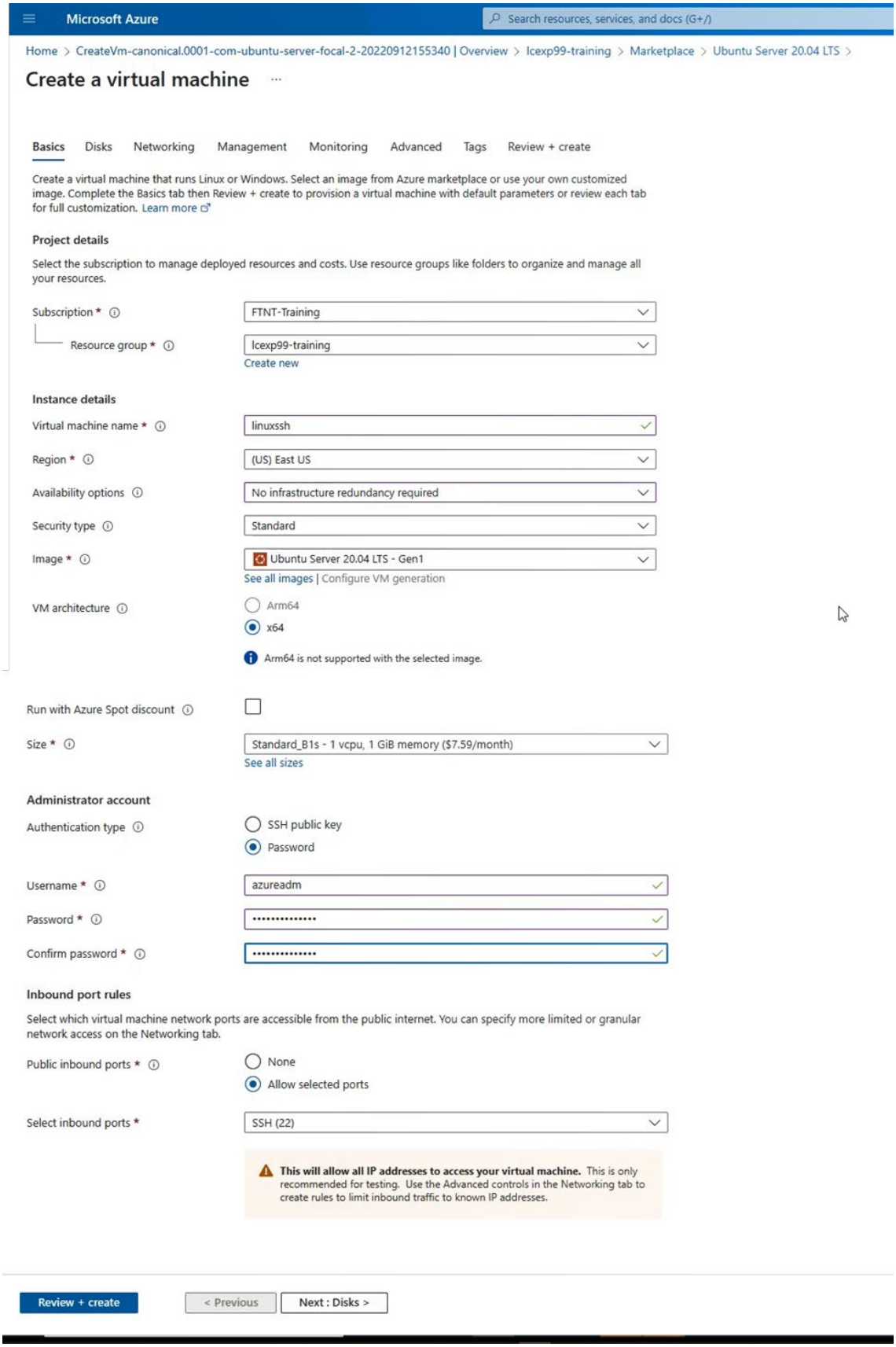
2. Click on **Virtual machine** on the page that will be displayed



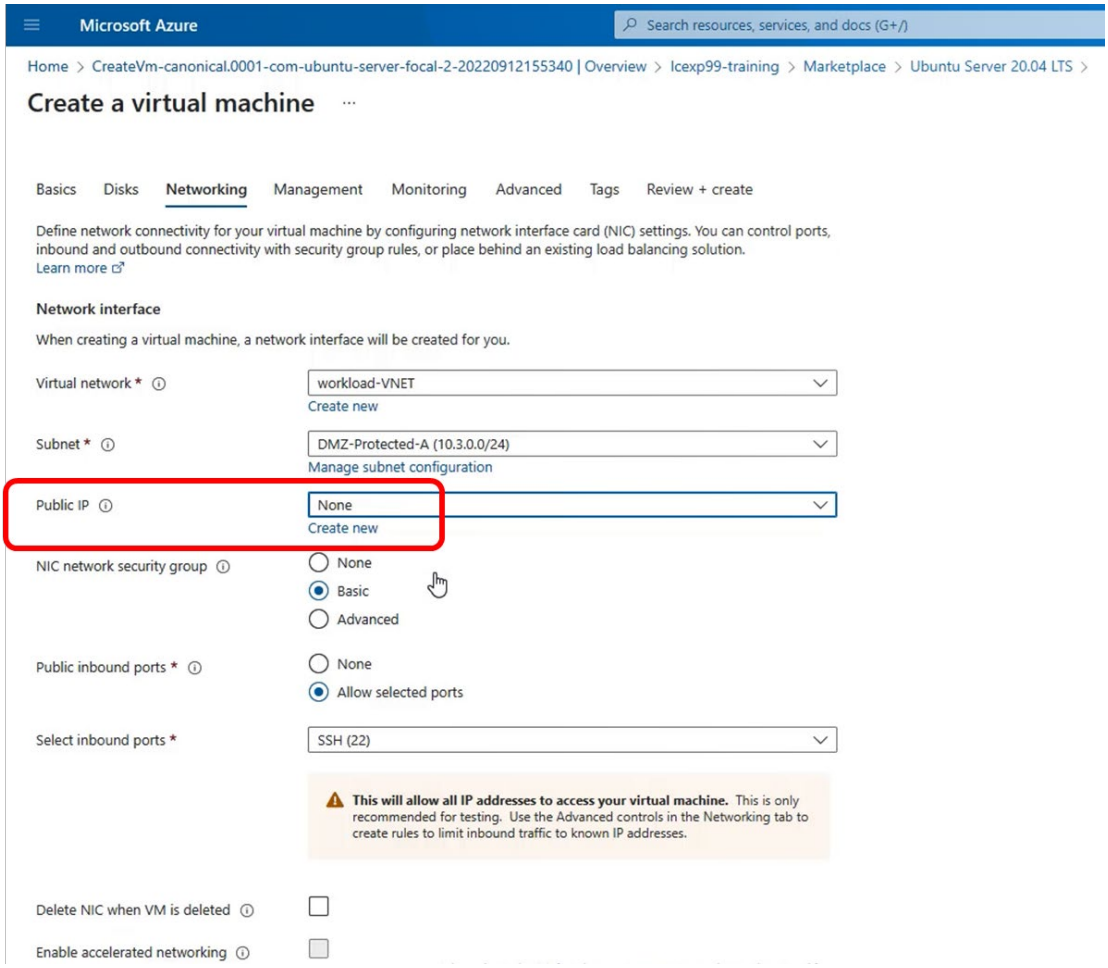
Use the following information from the table to fill out the page as showed in the image below. Some of those field will require additional click through wizards (Image, Size)

Subscription	FTNT-Training
Resource group	lcexp***<your student number>***-training
Virtual machine name	linuxssh
Region	(US) east US
Availability options	No infrastructure redundancy required
Security Type	Standard
Image	Ubuntu Server 20.04 LTS – Gen1 or Gen 2
Size	Standard_B1s – 1vcpu, 1GiB memory
Administrator authentication type	Password
Username	azureadm
Password	***<choose your own>***
Public inbound ports	Allow selected ports
Select inbound ports	SSH (22)

Task 2 - Deploy linuxssh virtual machine

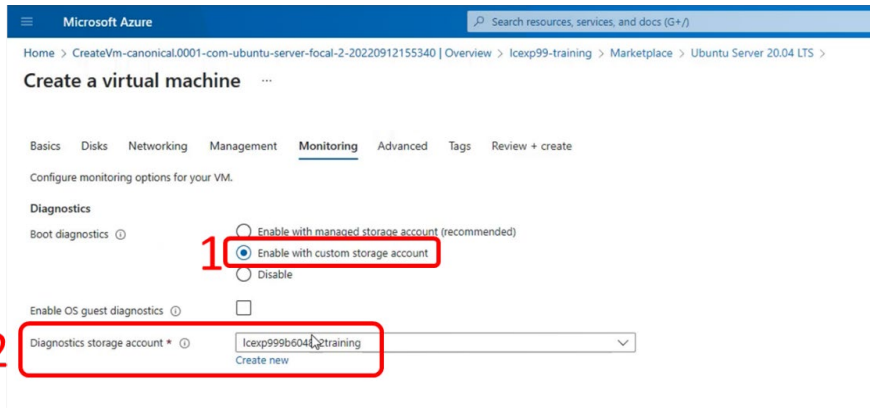


3. Click on **Next: Disks** (at the bottom) or click the **Disk** pane, there is nothing to change here
4. Click on **Next: Networking** (at the bottom) or click on the **Networking** pane.
5. In this **Networking** pane, change the Public IP address to **None** as shown

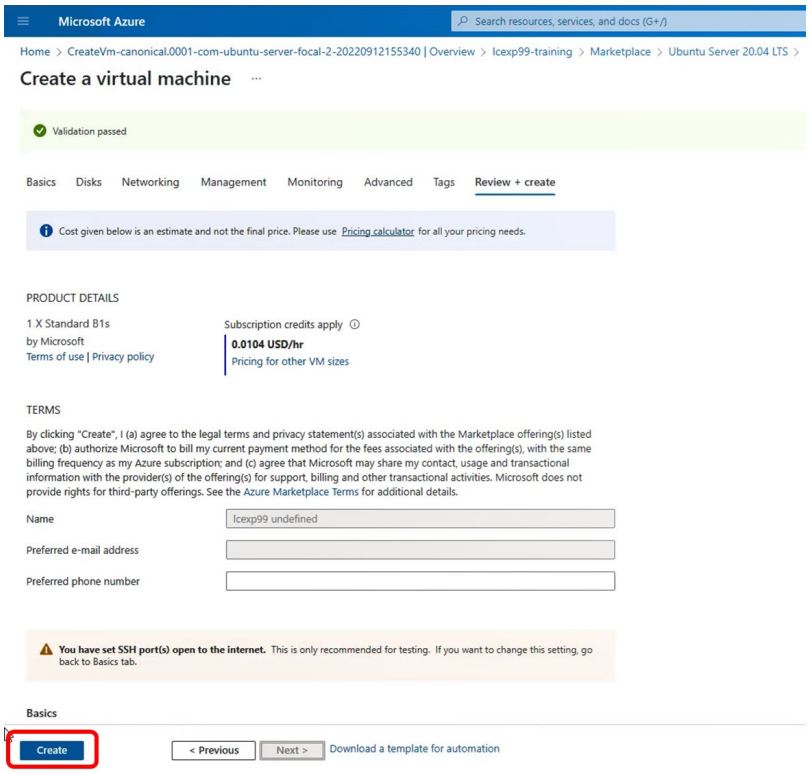


6. Click on **Next: Management** (at the bottom) or click on the **Management** pane, nothing will be changed there

7. In the Monitoring pane, under **Boot diagnostics** select **Enable with custom storage account**. A new drop-down box will appear. Select the pre-create storage account under Diagnostics storage account.



8. Click on **Next: Advanced** (at the bottom) or click the **Advanced** pane, there is nothing to change here
9. Click on **Next: Tags** (at the bottom) or click the **Tags** pane, there is nothing to change here
10. Verify that everything is set accordingly and click **Create**



11. A new notification will appear saying the deployment is in progress
12. Upon completion of the deployment, go to the list of Resource Groups, select the training Resource Group where after a few minutes the newly created VM will appear (might require web browser refresh).
13. The linuxssh VM was successfully created

Task 3 - Deploy dvwa virtual machine.

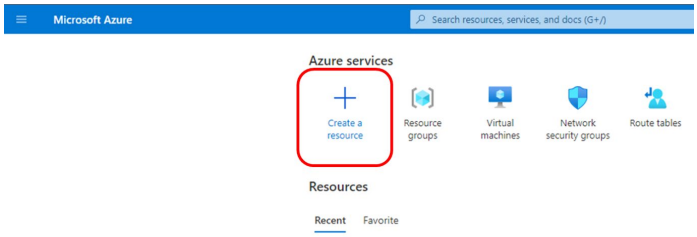
Our next step is going to be creation of the next VM (Virtual Machine) into the workload VNET. This VM will be running the software DVWA.

From the project itself: D..n (word blocked out on purpose) Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is d..n vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled classroom environment.

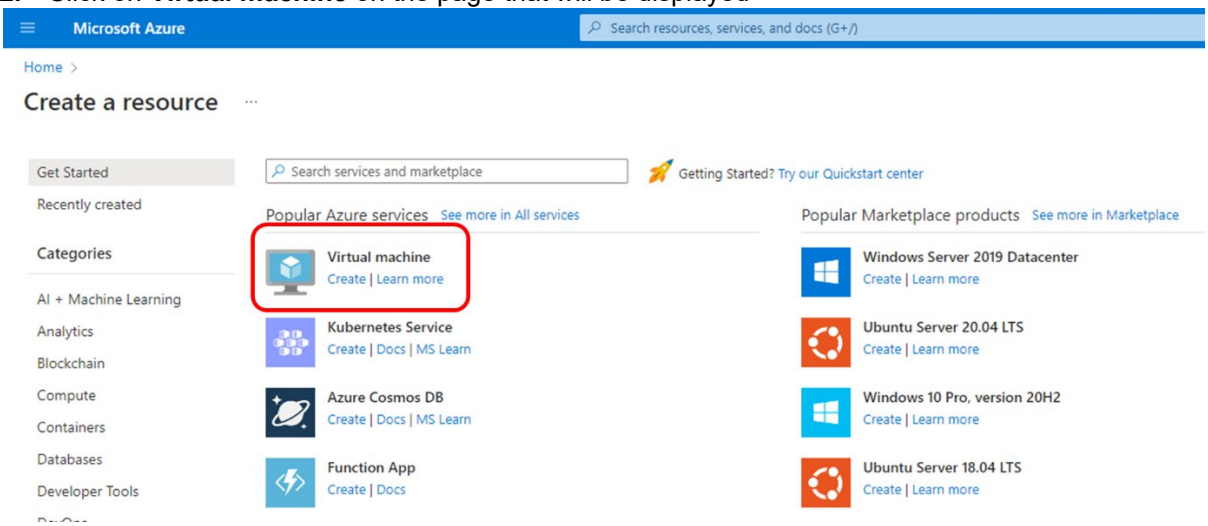
The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

Creation steps

1. From the main Azure Portal, click on **Create a resource**



2. Click on **Virtual machine** on the page that will be displayed

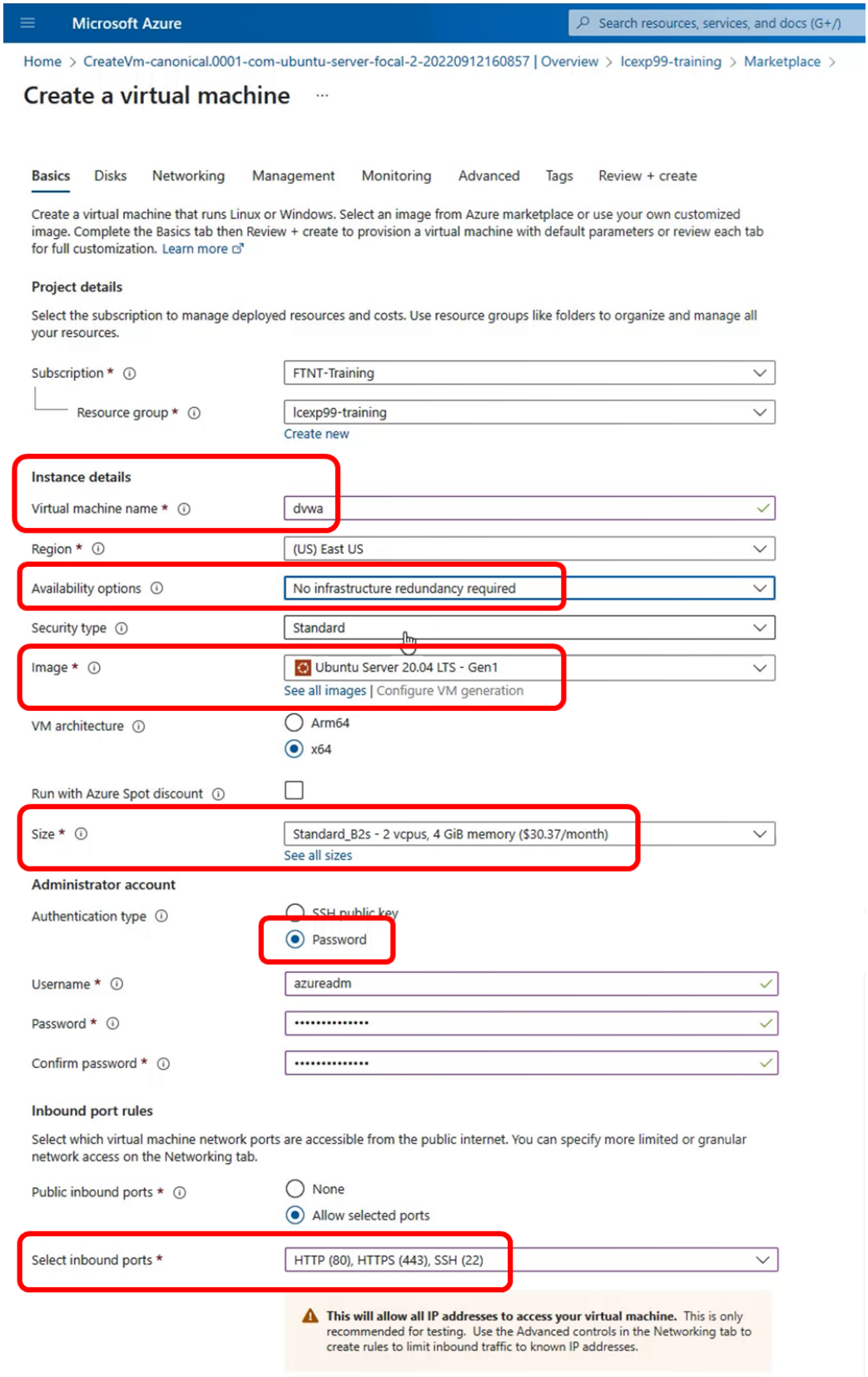


Task 3 - Deploy dvwa virtual machine.

3. Use the following information from the table to fill out the page as showed in the image below

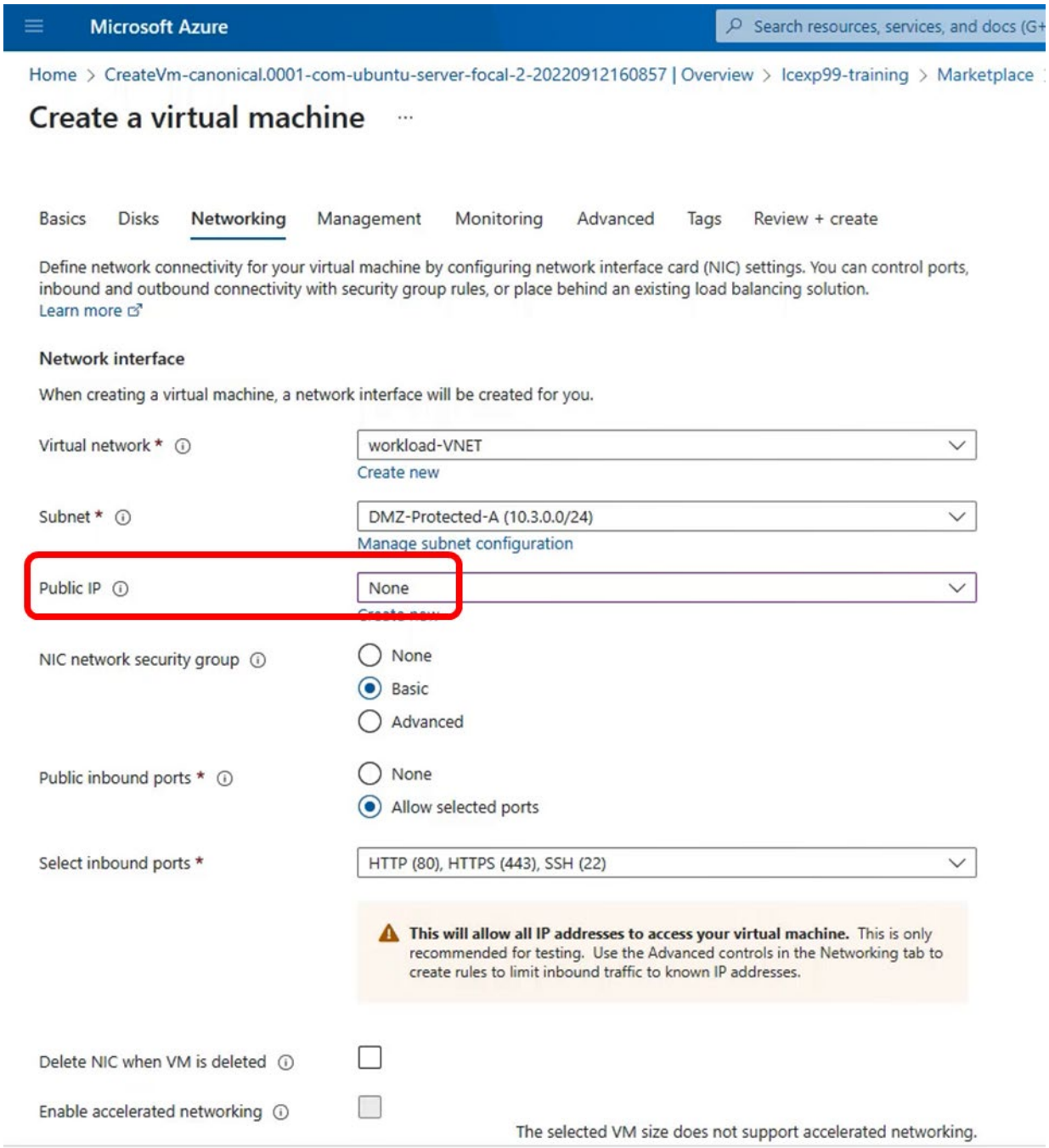
Subscription	FTNT-Training
Resource group	lcexp***<your student number>***-training
Virtual machine name	dvwa
Region	(US) east US
Availability options	No infrastructure redundancy required
Security Type	Standard
Image	Ubuntu Server 20.04 LTS – Gen1
Size	Standard_B2s – 2vcpu, 4GiB memory
Administrator authentication type	Password
Username	azureadm
Password	***<choose your own>***
Public inbound ports	Allow selected ports
Select inbound ports	SSH (22), HTTP (80), HTTPS (443)

Task 3 - Deploy dvwa virtual machine.



Task 3 - Deploy dvwa virtual machine.

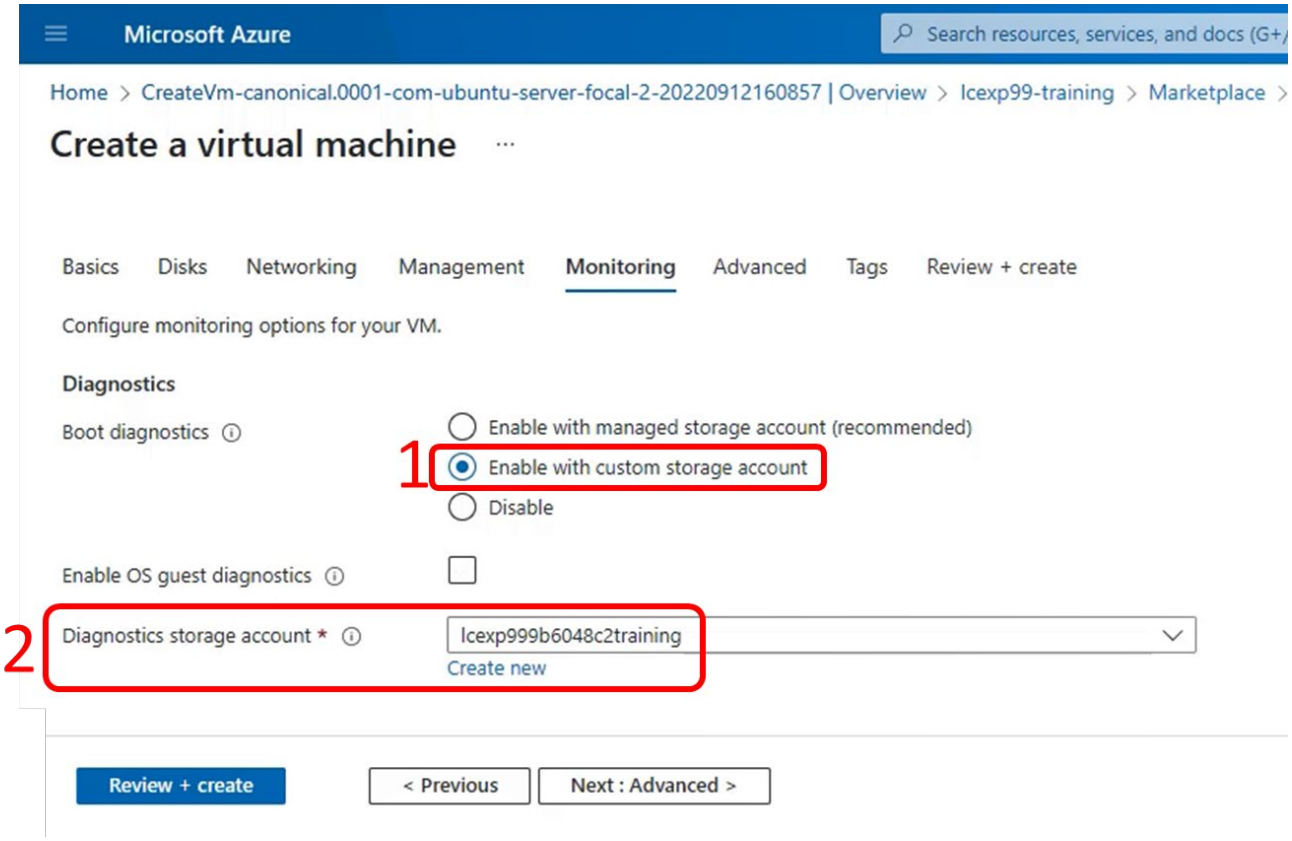
4. Click on **Next: Disks** (at the bottom) or click the **Disk** pane, there is nothing to change here
5. Click on **Next: Networking** (at the bottom) or click on the **Networking** pane.
6. In this **Networking** pane, change the Public IP address to **None** as shown



7. Click on **Next: Management** (at the bottom) or click on the **Management** pane, there is nothing to change here

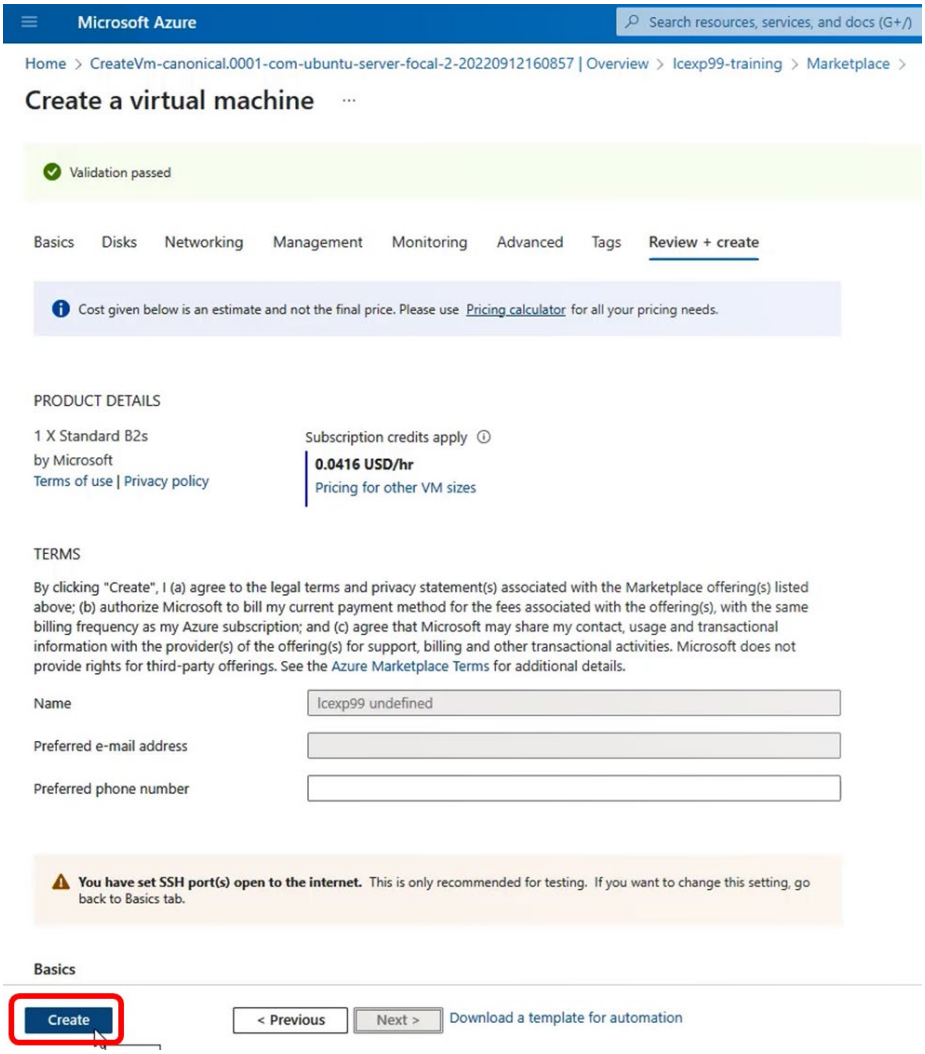
Task 3 - Deploy dvwa virtual machine.

8. In the Monitoring pane, under **Boot diagnostics** select **Enable with custom storage account**. A new drop-down box will appear. Select the pre-create storage account under Diagnostics storage account.

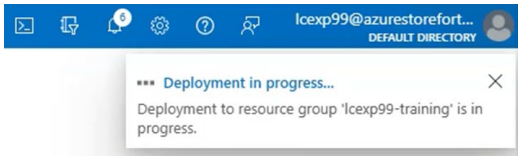


9. Click on **Next: Advanced** (at the bottom) or click the **Advanced** pane, there is nothing to change here
10. Click on **Next: Tags** (at the bottom) or click the **Tags** pane, there is nothing to change here
11. Verify that everything is set accordingly and click **Create**

Task 3 - Deploy dvwa virtual machine.

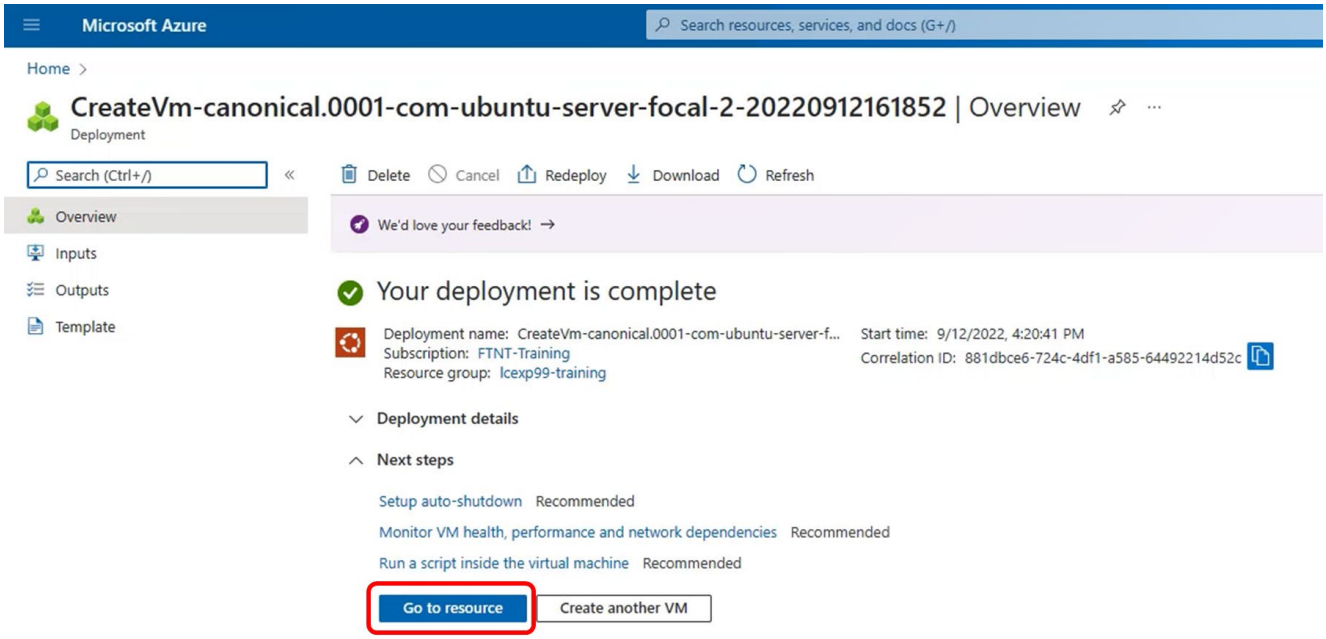


12. A new notification will appear saying the deployment is in progress

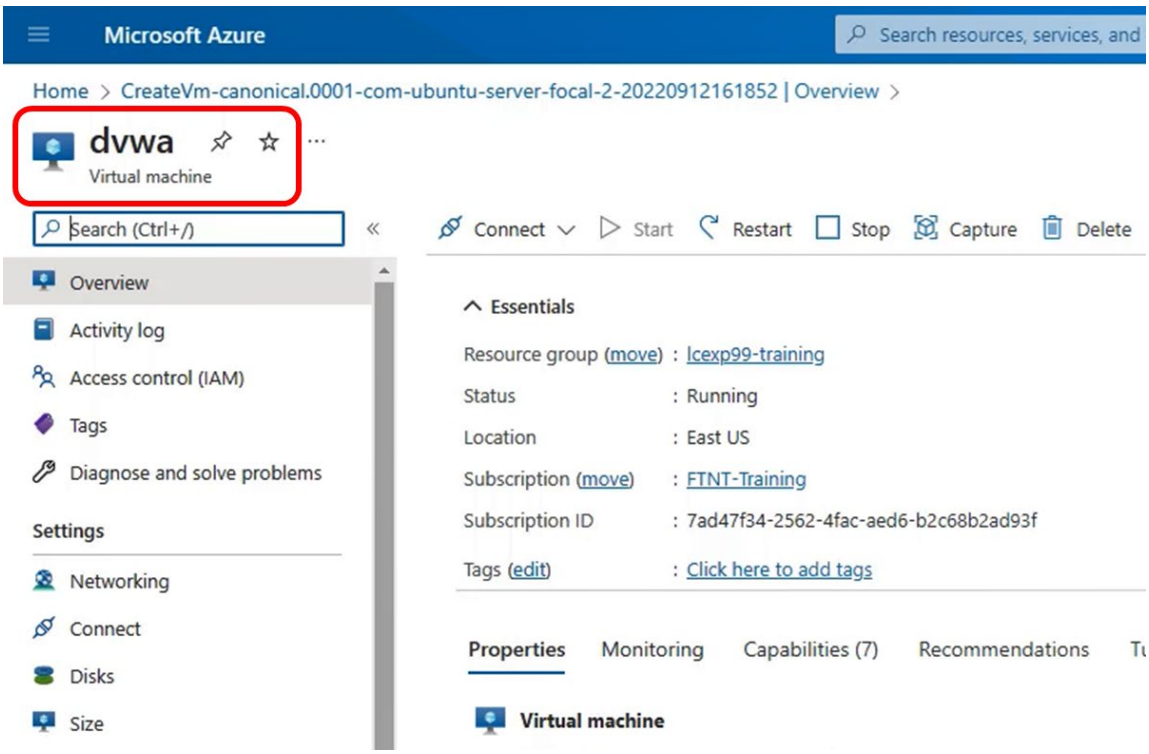


Task 3 - Deploy dvwa virtual machine.

13. Upon completion of the deployment, click on **Go to resource**

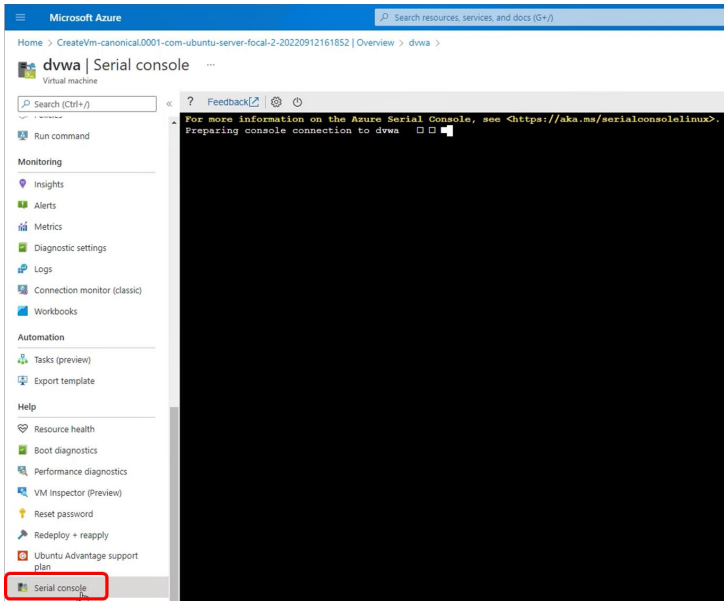


14. The screen should look like this, if it does not yet, please wait around 5 minutes or so

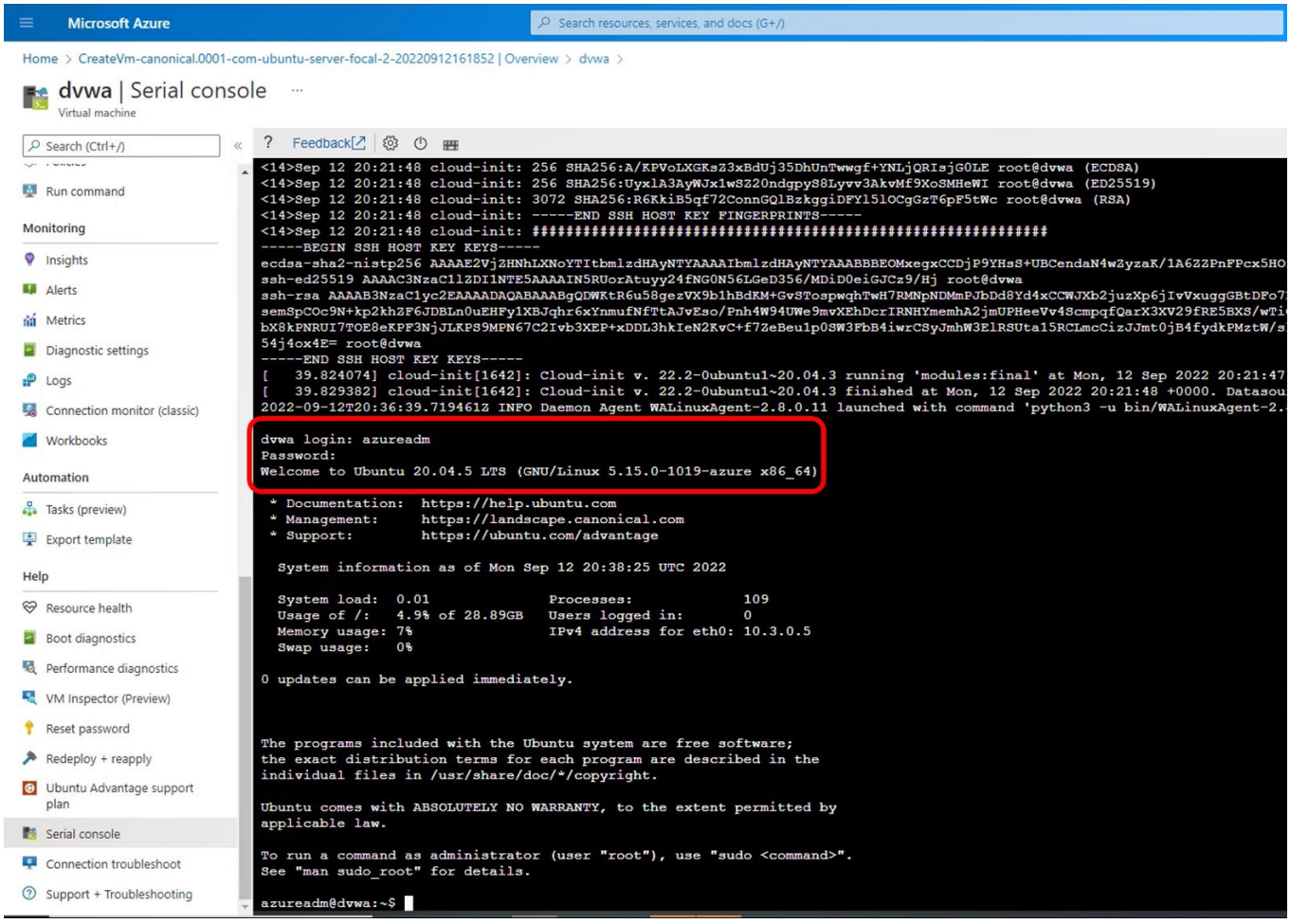


Task 3 - Deploy dvwa virtual machine.

15. In the Virtual machine left menu, scroll all the way down and select **Serial console**



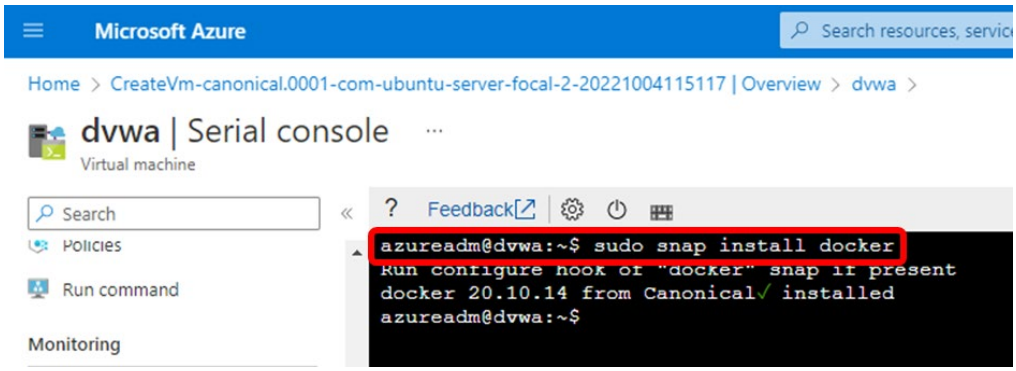
16. Login with the previously created credentials (**azureadm** and the chosen password)



Task 3 - Deploy dvwa virtual machine.

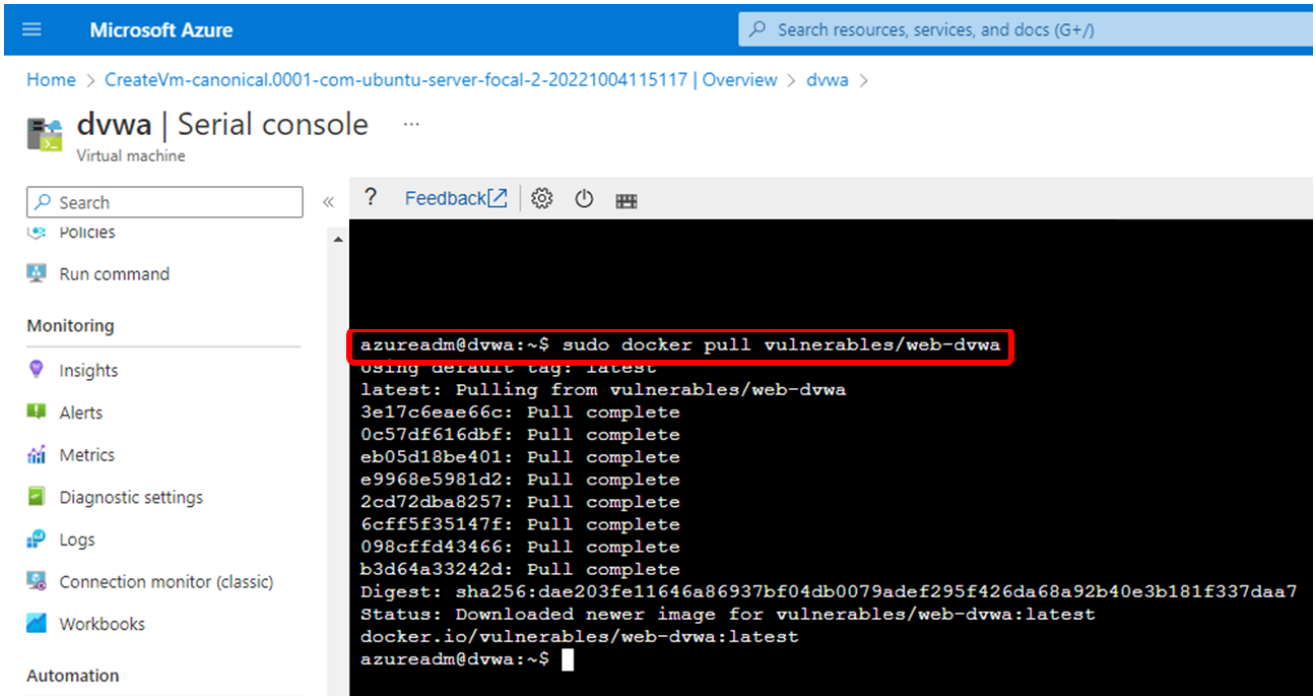
17. Install the docker subsystem by entering the following command:

```
sudo snap install docker
```



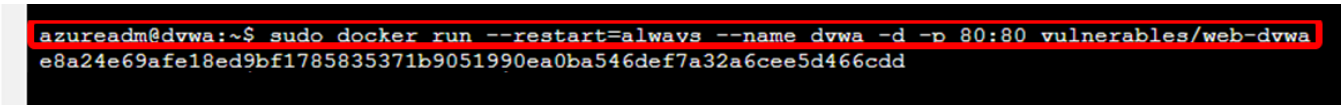
18. Next install DVWA by entering the following command:

```
sudo docker pull vulnerables/web-dvwa
```



19. Next configure DVWA to start using the following command (all in one line):

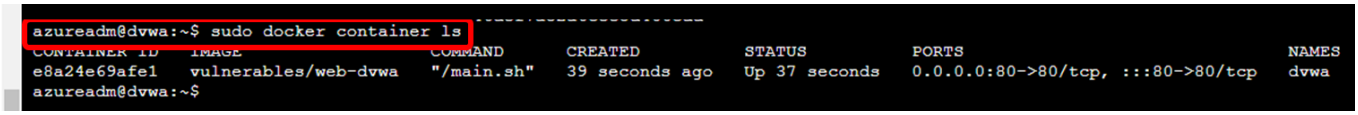
```
sudo docker run --restart=always --name dvwa -d -p 80:80
vulnerables/web-dvwa
```



Task 3 - Deploy dvwa virtual machine.

20. Confirm that DVWA installed correctly using the following command:

```
sudo docker container ls
```



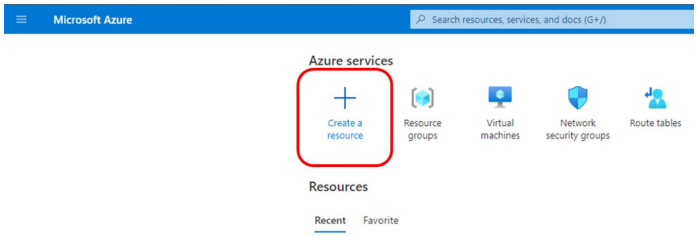
21. The DVWA VM was successfully deployed

Task 4 - Deploy FortiGate Active-Passive

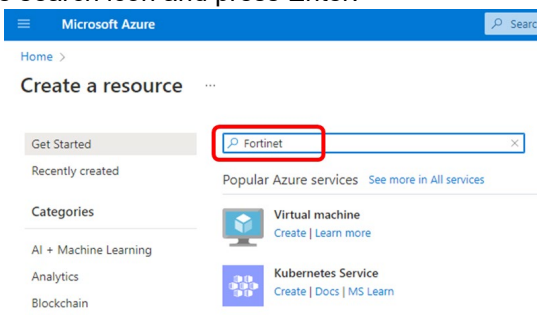
The next step is the deployment of the of the FortiGate firewalls (in Active-Passive mode) along with associated network resources including the virtual network for the Internet Egress Hub.

Creation steps

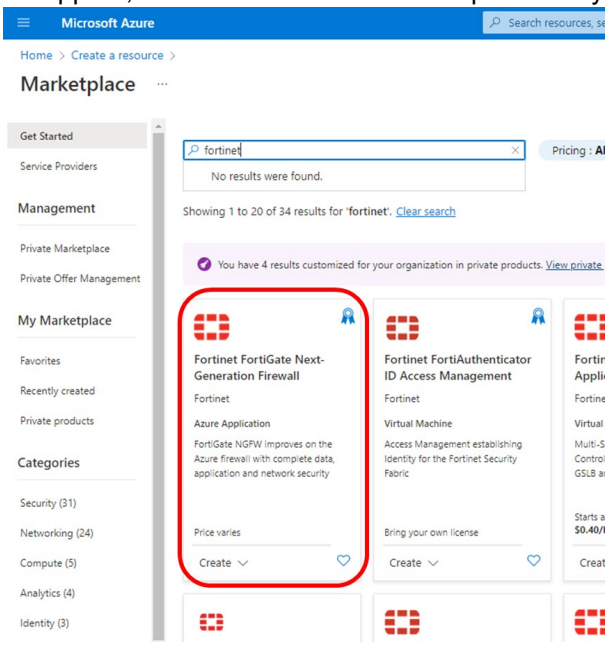
1. From the main Azure Portal, click on **Create a resource**



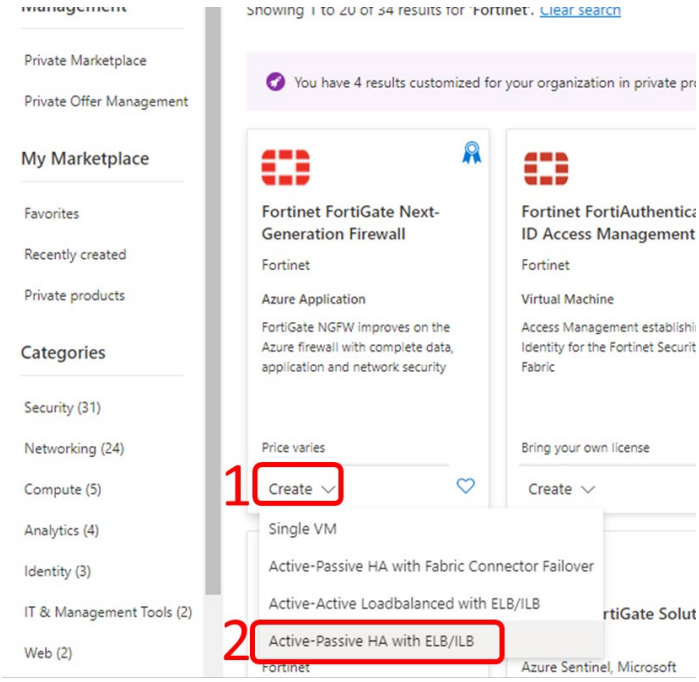
2. Type **Fortinet** next to the search icon and press Enter.



3. The following results will appear, look at the FortiGate Marketplace Entry

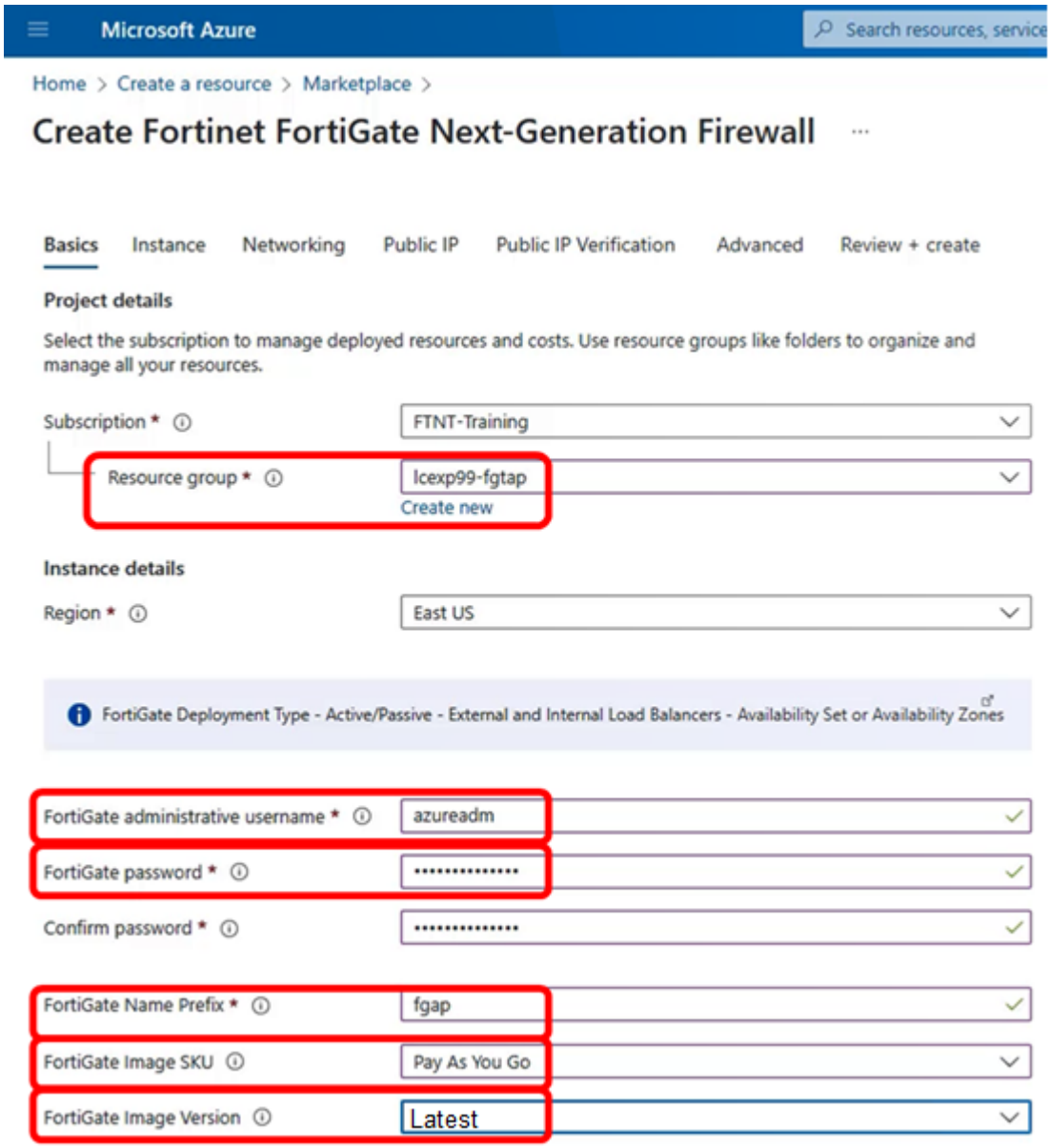


4. In that same FortiGate entry, click on **Create**, then click on **Active-Passive HA with ELB/ILB**



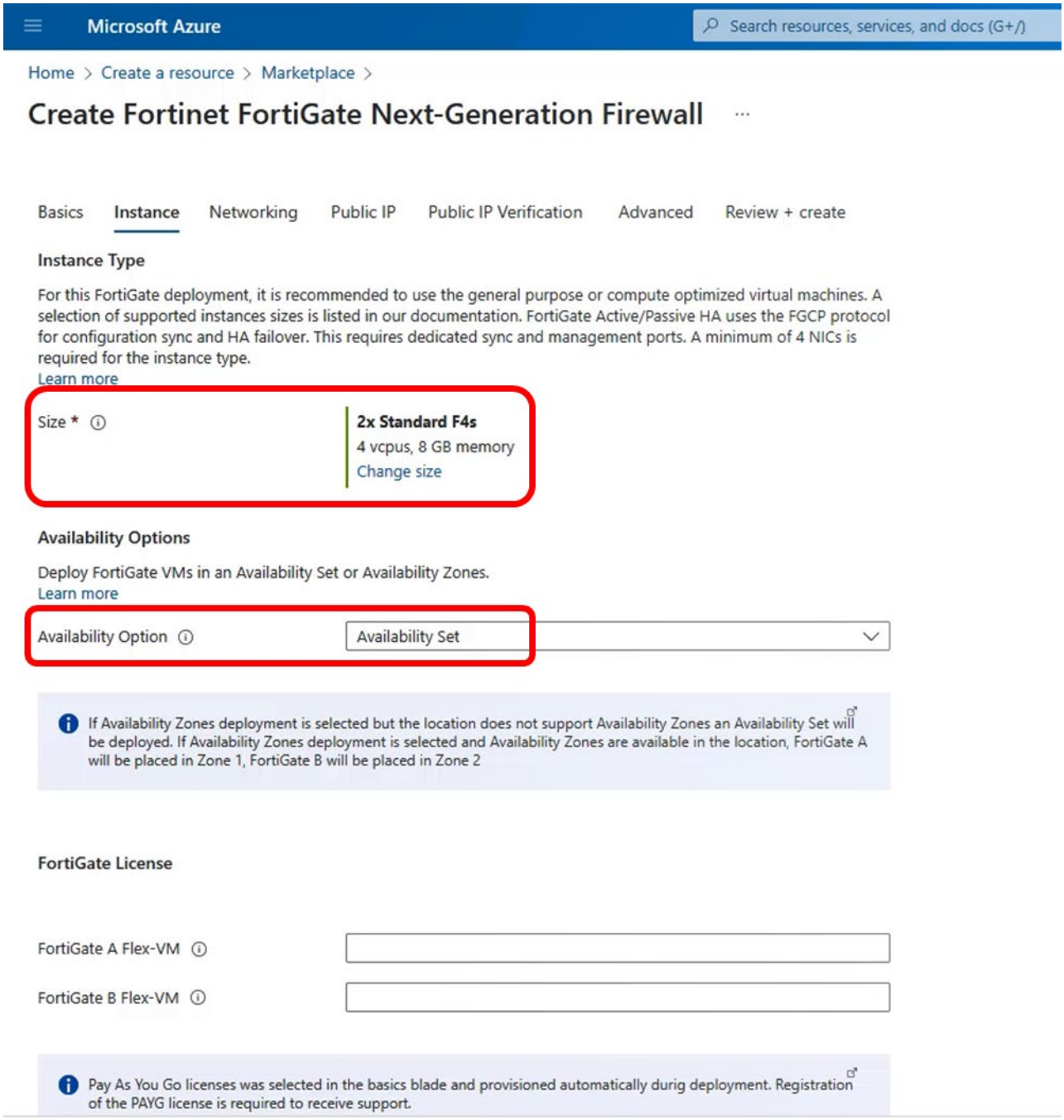
5. Use the following information from the table to fill out the page as showed in the image below

Subscription	FTNT-Training
Resource group	lcexp***<your student number>***-fgtap
Region	(US) east US
FortiGate Administrative Username	azureadm
FortiGate password	***<choose your own>***
FortiGate Name Prefix	fgap
FortiGate Image SKU	Pay As You Go
FortiGate Image Version	Latest



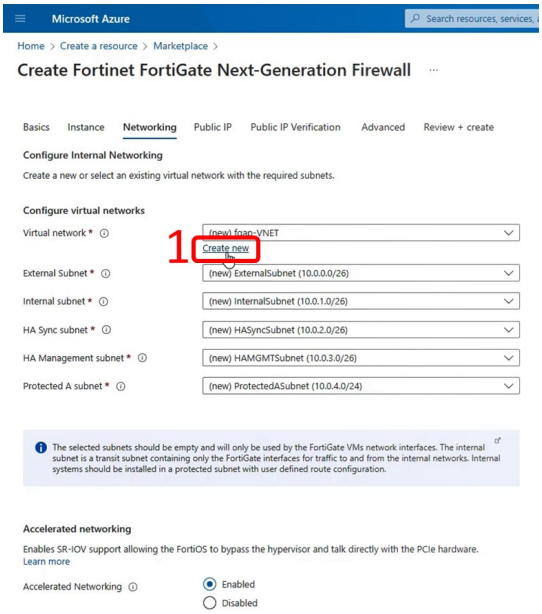
6. Click on **Next: Instance** or click on the **Instance** pane
7. Use the following information from the table to fill out the page as showed in the image below

Size	2x Standard F4s
Availability Option	Availability Set



8. Click on **Next: Networking** or click on the **Networking** pane

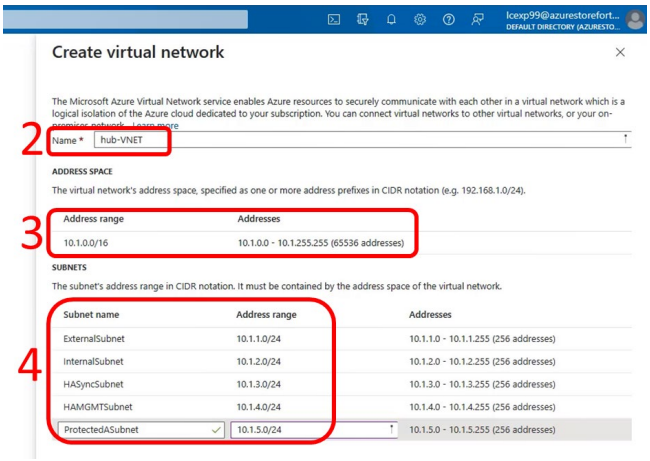
9. Click **Create new** under Virtual network



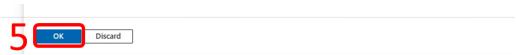
10. Use the following information from the table to fill out the page as showed in the image below

Name	hub-VNET
Address range	10.1.0.0/16

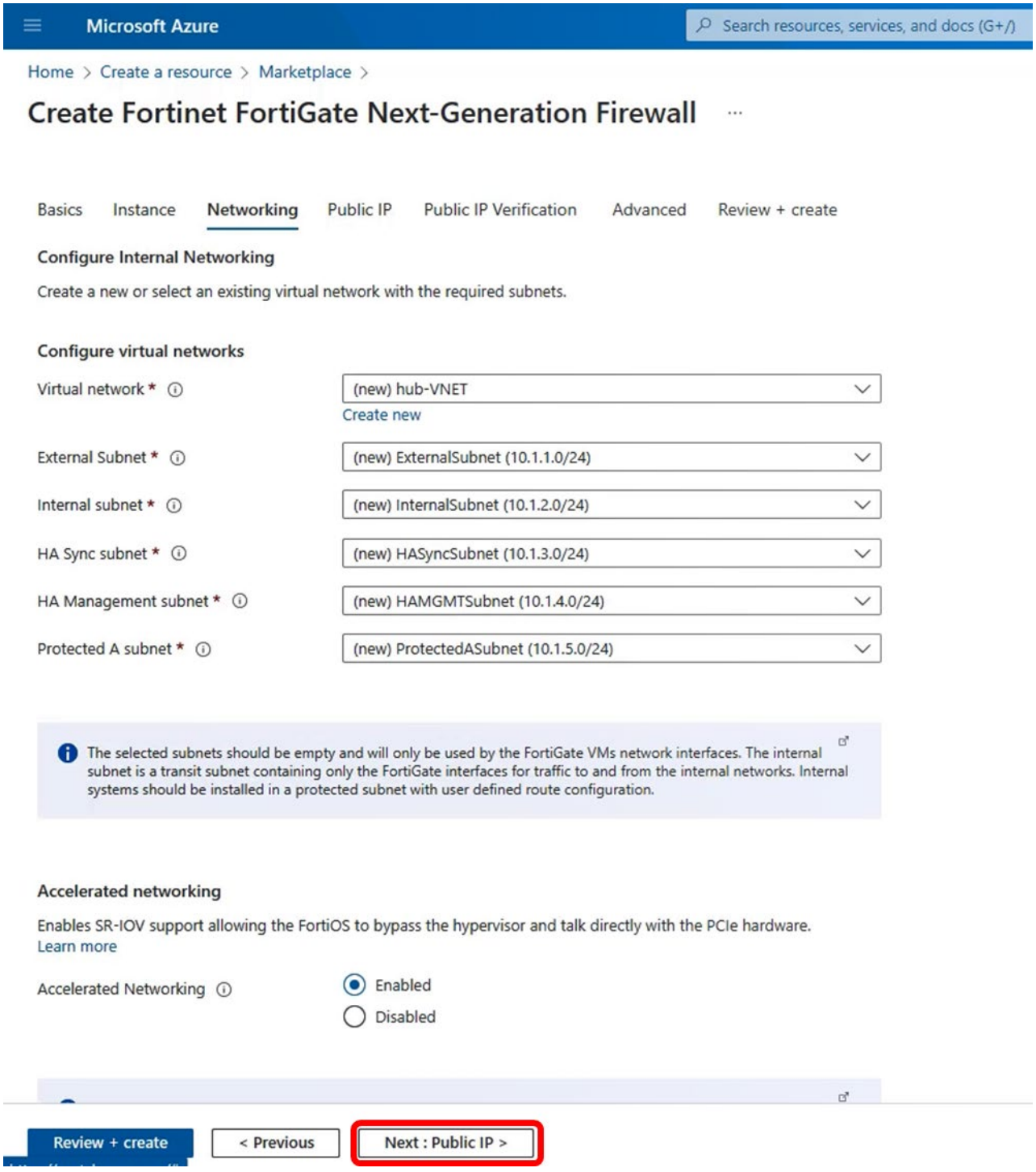
Subnet name	**Address range**
ExternalSubnet	10.1.1.0/24
InternalSubnet	10.1.2.0/24
HASyncSubnet	10.1.3.0/24
HAMGMTSubnet	10.1.4.0/24
ProtectedASubnet	10.1.5.0/24



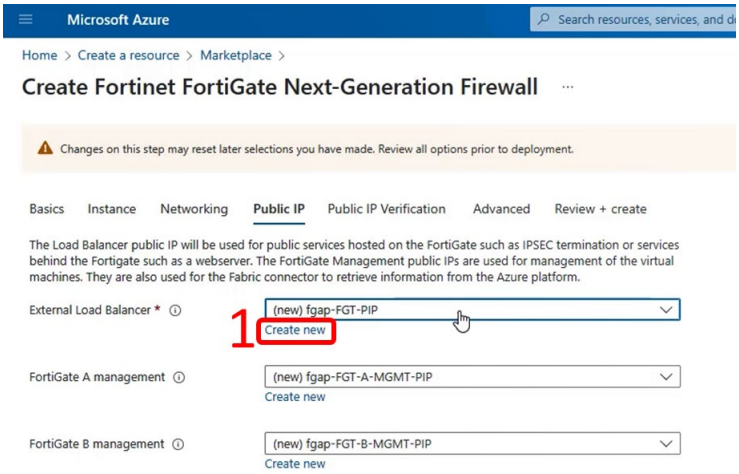
11. Click OK to return to the networking pane



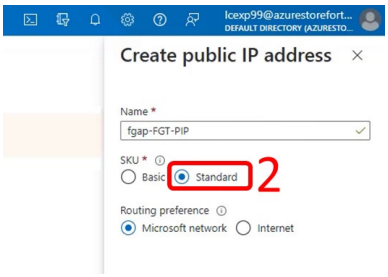
12. Confirm information entered matches the screen below and then click **Next: Public IP**



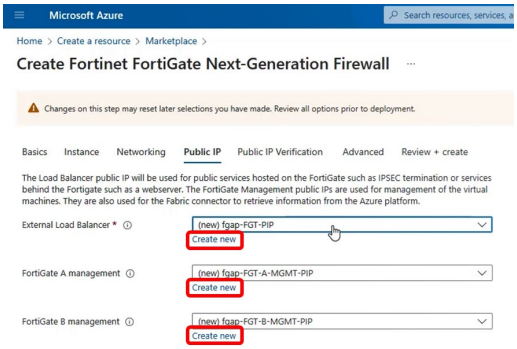
13. Under External Load Balancer, click **Create new** which will open a new pane on the right



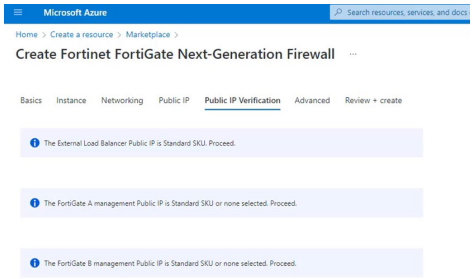
14. In the right pane named Create public IP address, select SKU **Standard**



15. Repeat step 13 and 14 for both FortiGate fgap-FGT-A management and FortiGate fgap-FGT-B management

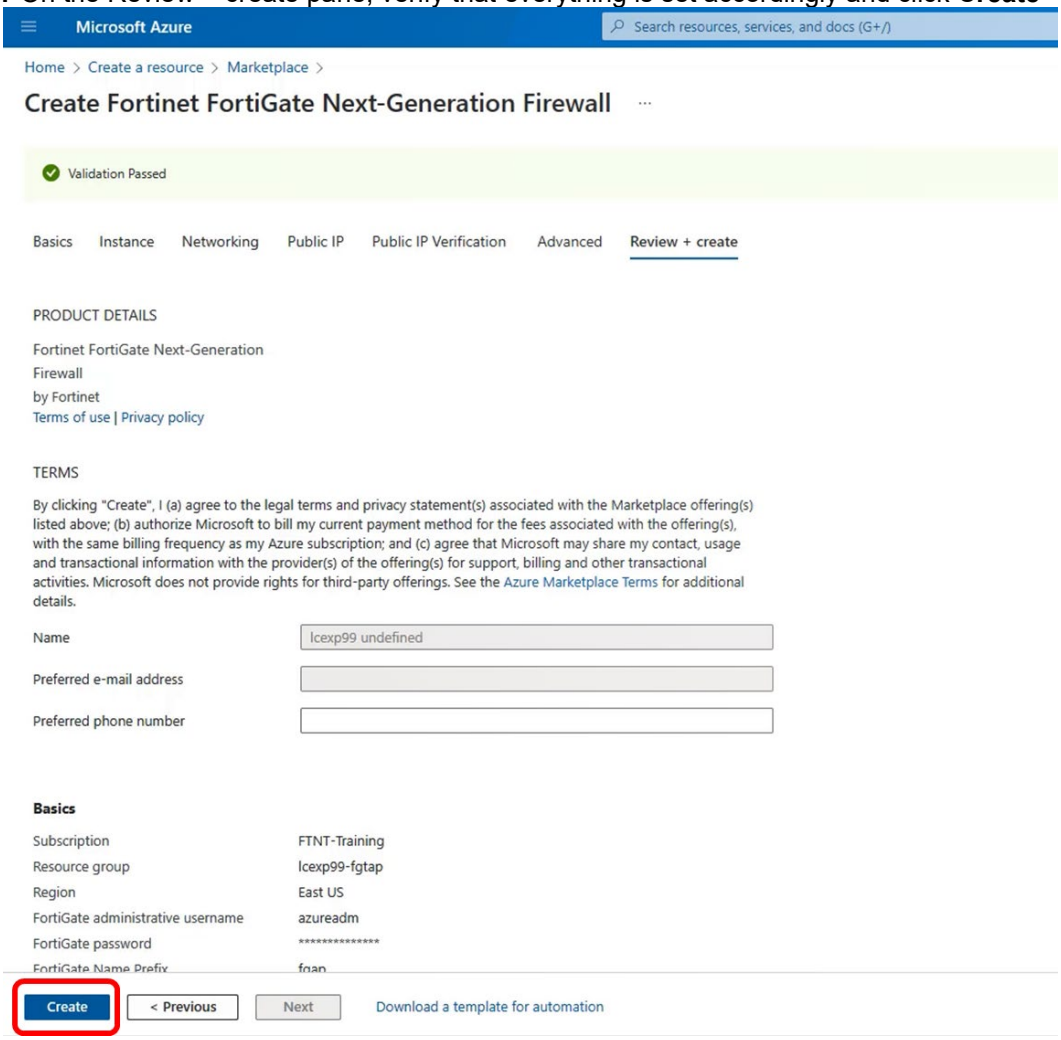


16. Click on **Next: Public IP Verification** at the bottom
17. Confirm the Public IP have been validated

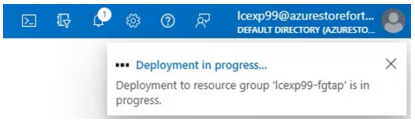


18. Click on **Next: Advanced** at the bottom, there is nothing to change in the Advanced pane

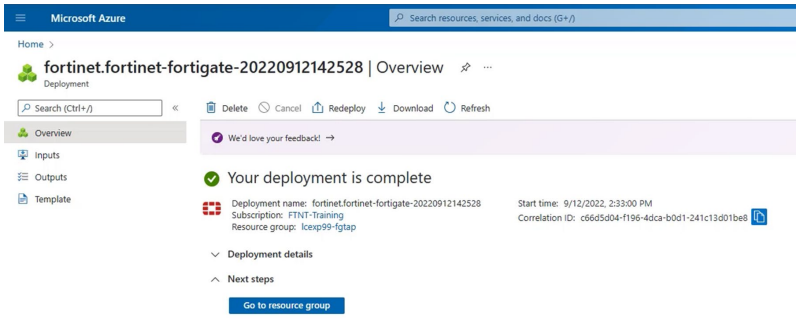
19. On the Review + create pane, verify that everything is set accordingly and click **Create**



20. A notification of the deployment start will display

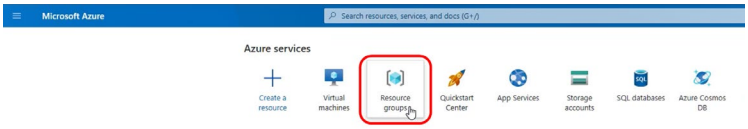


21. This template deploys several resources, expect 5 minutes for the deployment to complete

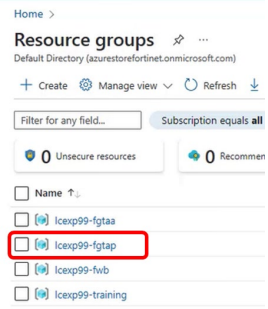


22. Since there is a limit of 200 route tables for each individual Azure Subscription, and that the route table deployed by this template is not being used, it needs to be deleted.

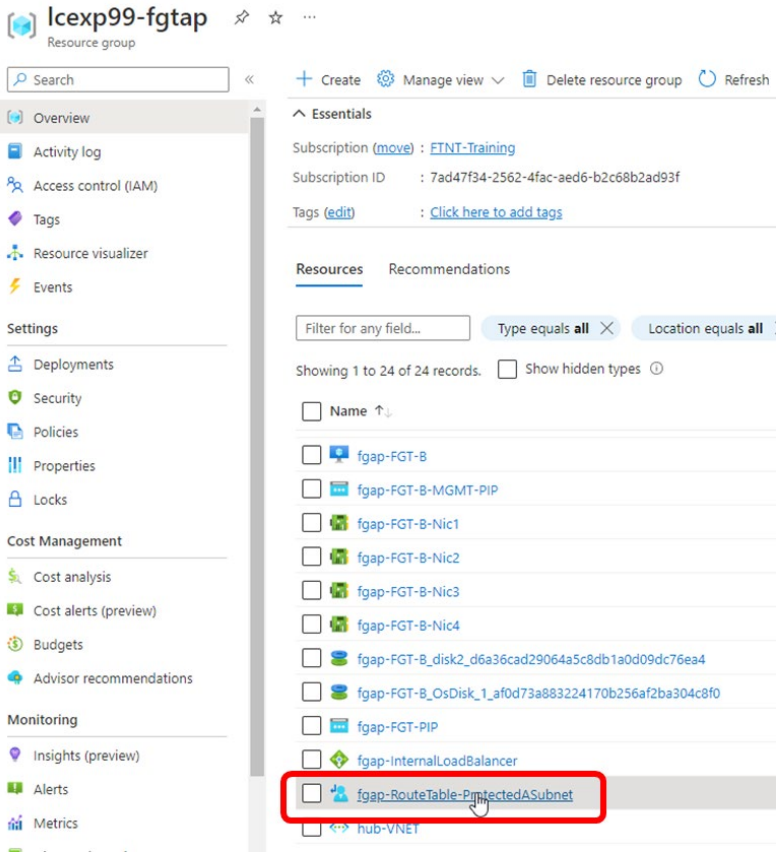
23. From the main Azure Portal, click on **Resource groups**



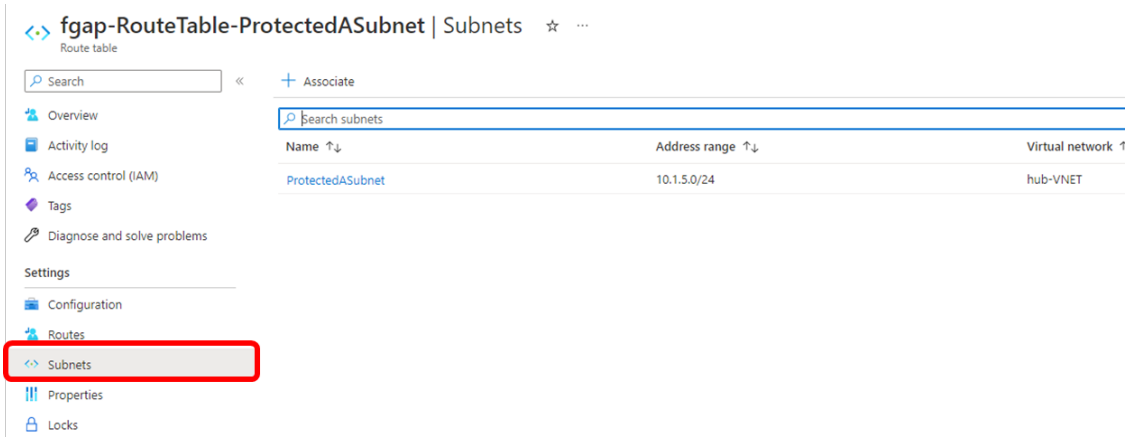
24. Click on the lcexp***<your student number>***-fgtap resource group name itself to open a new pane on the right.



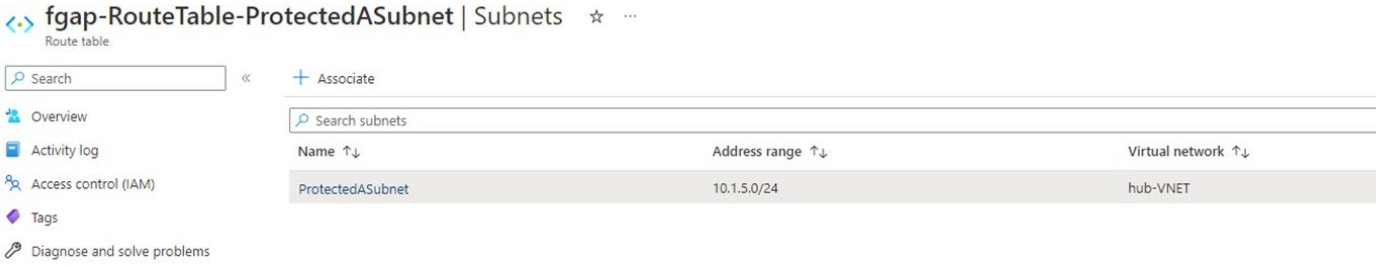
25. Scroll all the way down and click on the name **fgap-RouteTable-ProtectedASubnet**



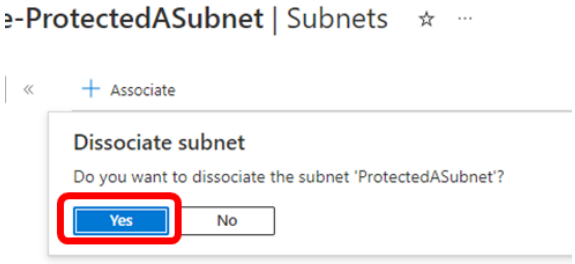
26. In the left Route table menu, click on **Subnets**



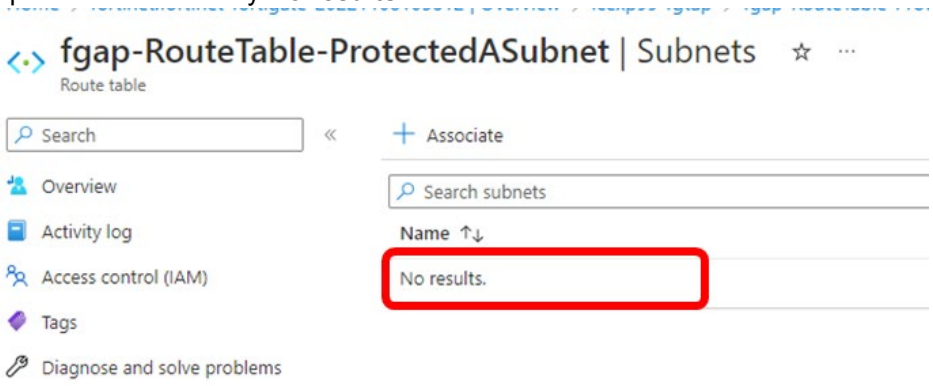
27. Click on the three dots **…** on the right side and then **Dissociate**



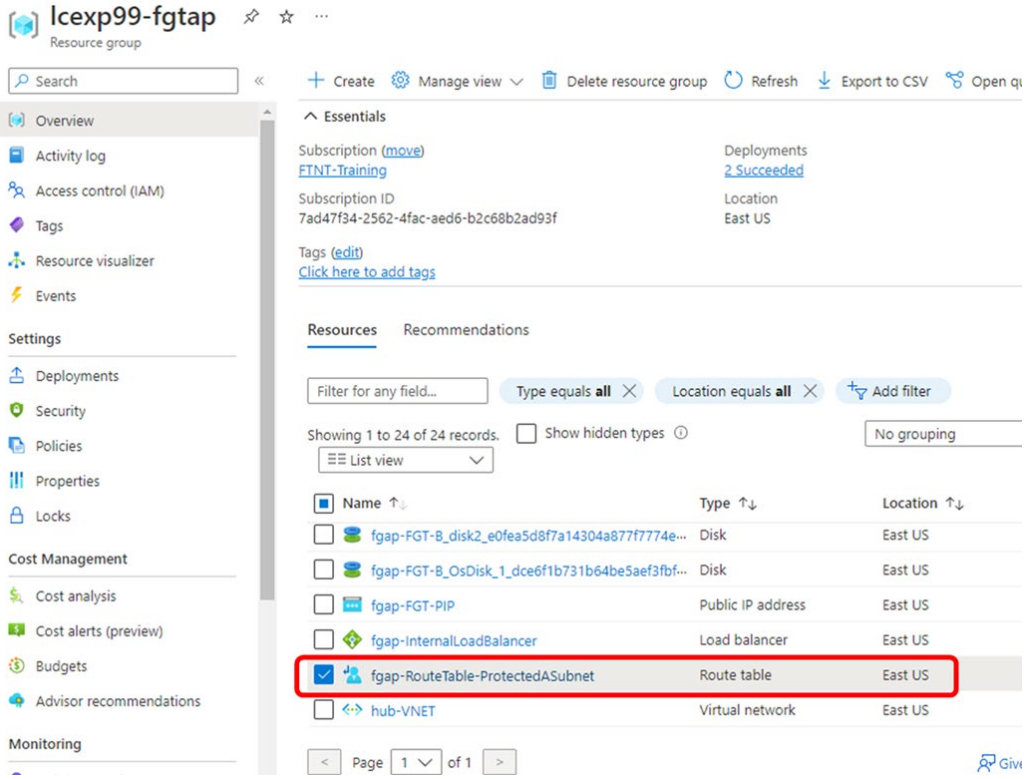
28. Confirm by clicking on **Yes**



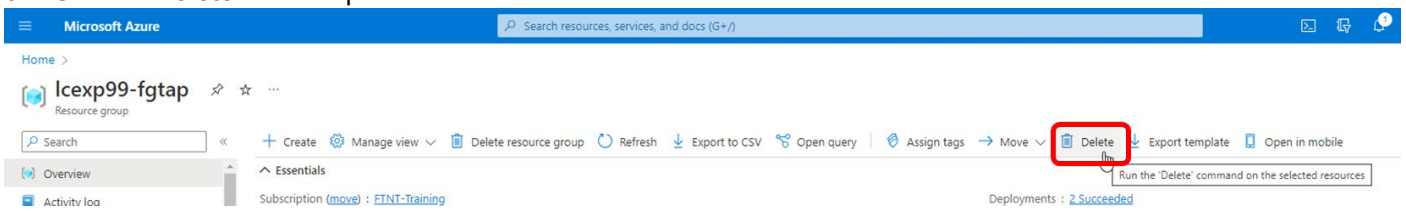
29. The right pane should now say **No results.**



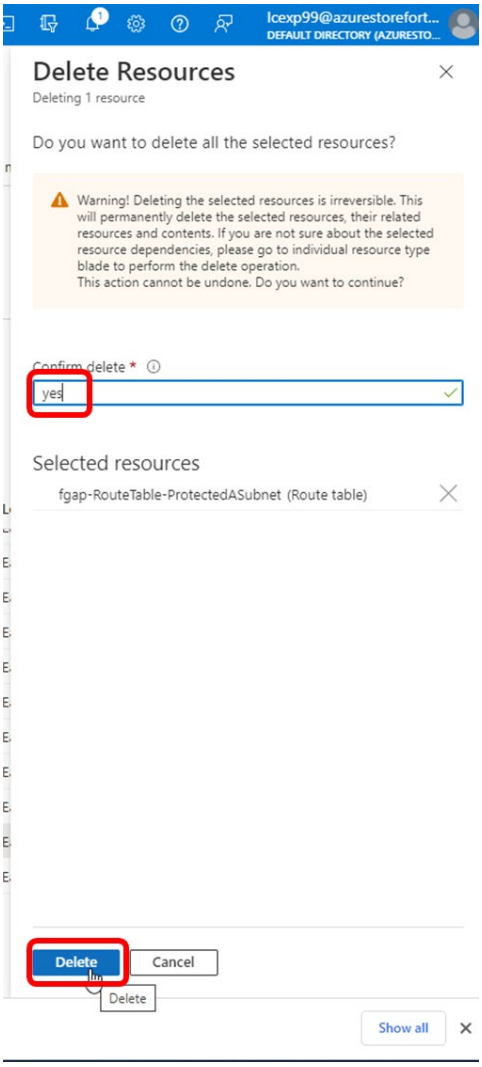
30. Go back to on the lcexp***<your student number>***-fgtaa resource group and then scroll all the way down and select the route table named **fgap-RouteTable-ProtectedASubnet**



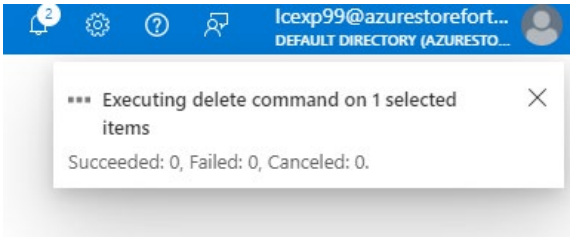
31. Click on **Delete** on the top menu



32. Type in **yes** to confirm and then click **Delete**



33. A notification will appear



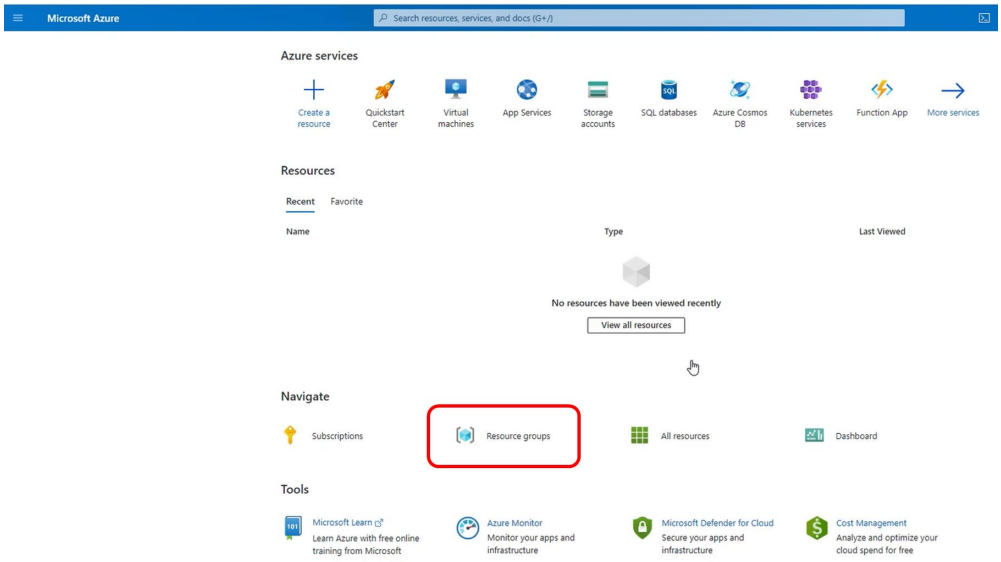
34. Upon completion, the deployment is now complete

Task 5 - Configure VNET Peering FGAP

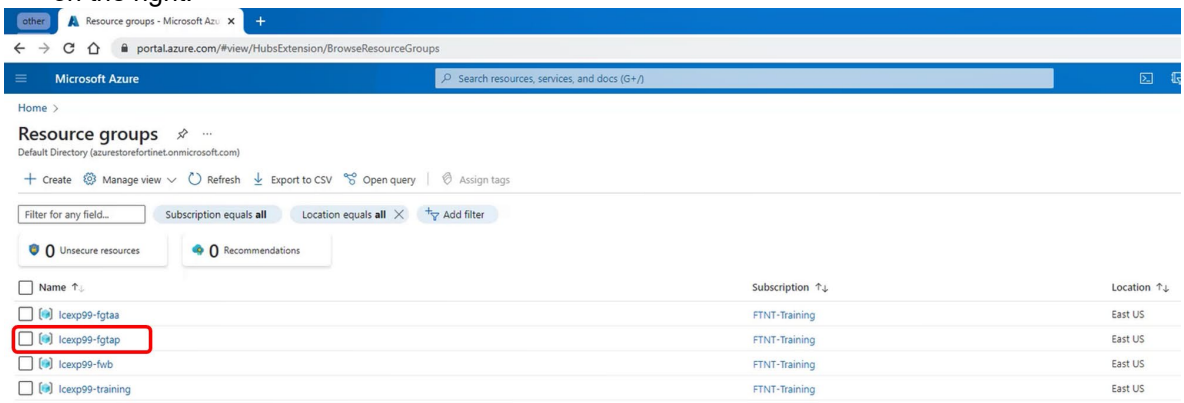
The next step is the configuration of the virtual network (VNET) peering between the Workload VNET and the FortiGate FGAP VNET to allow for intercommunications between the two VNETs.

Configuration steps

1. From the main Azure Portal, click on **Resource groups**

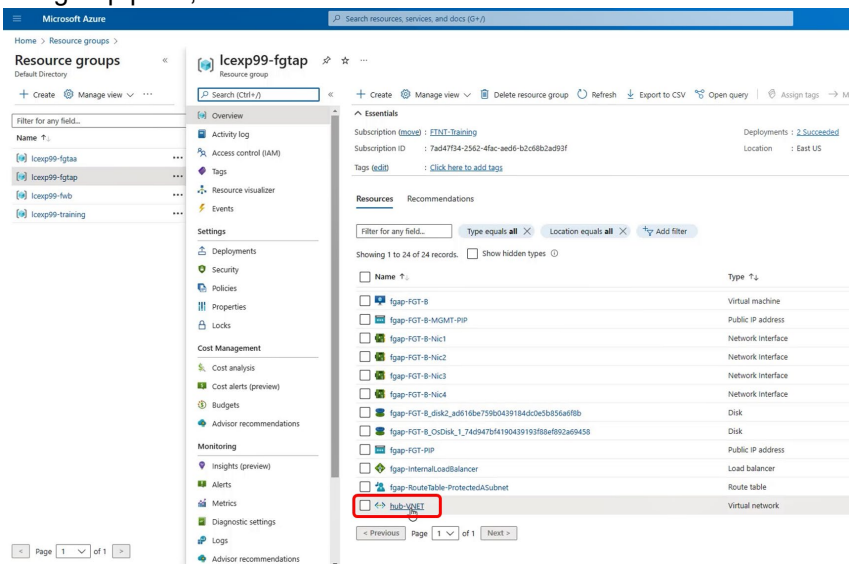


2. Click on the lcexp***<your student number>***-fgtap resource group name itself to open a new pane on the right.

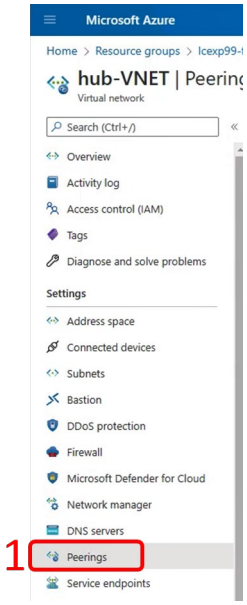


Task 5 - Configure VNET Peering FGAP

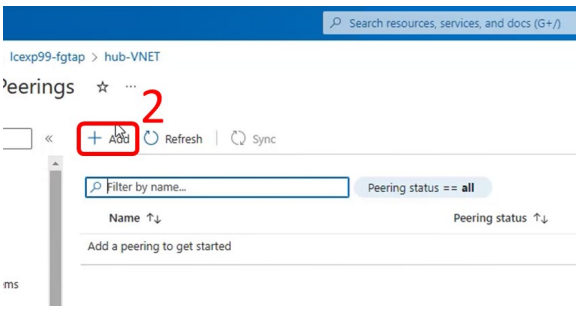
3. In the resource group pane, scroll down and click on the name hub-VNET



4. In the Virtual network left menu, scroll down to click **Peerings**

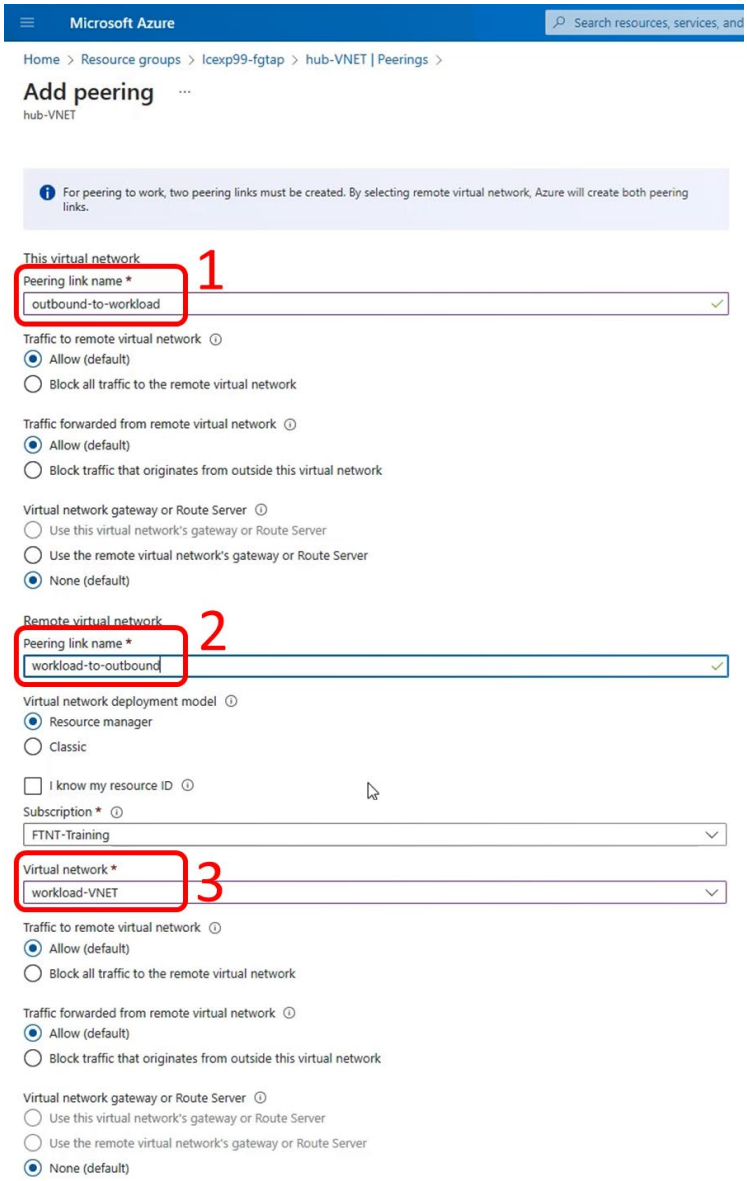


5. In the right pane, click **+ Add**



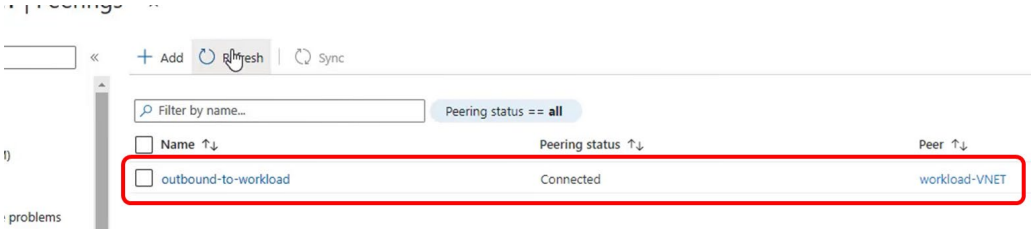
6. Use the following information from the table to fill out the page as showed in the image below

This virtual network **Peering link name**	outbound-to-workload
Remote virtual network **Peering link name**	workload-outbound
Remote virtual network **Virtual network**	workload-VNET

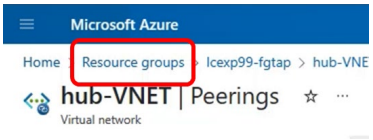


7. At the bottom of the pane, click **Add**

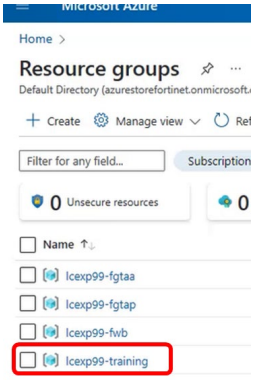
8. Confirm the peering status shows **Connected** as per the screenshot below, you might have to wait a few minutes occasionally clicking the **Refresh** button:



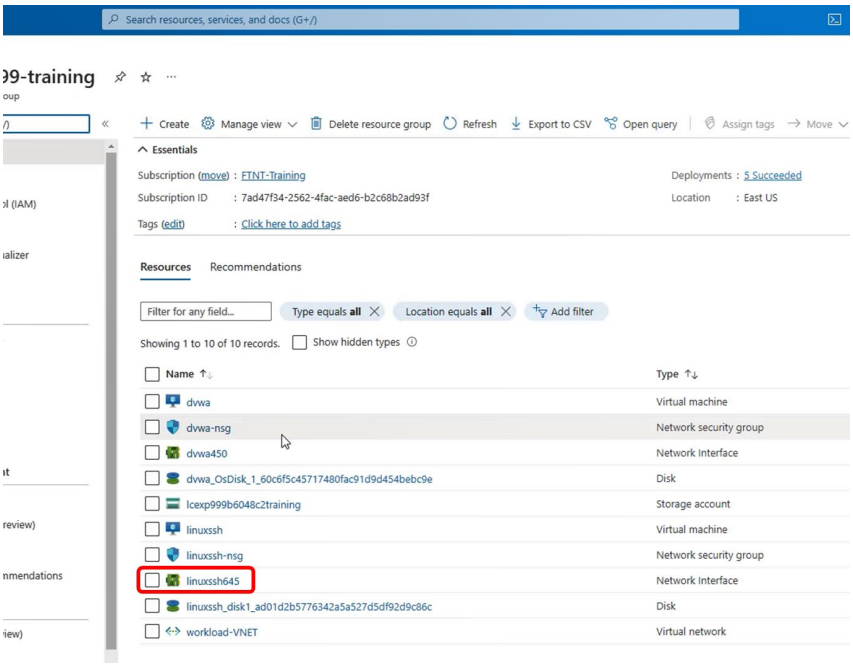
9. Next navigate away from this pane by click on Resource groups in the upper left menu



10. Click on the lcexp***<your student number>***-training resource group

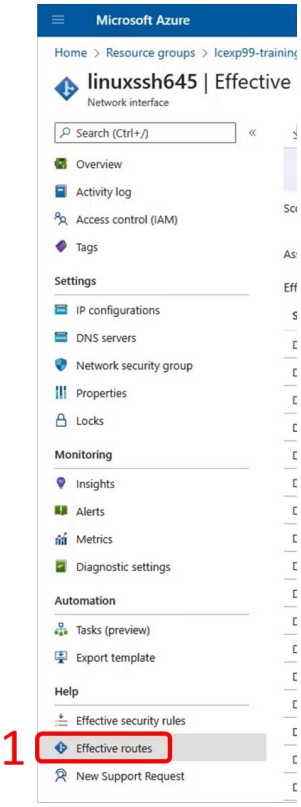


11. In the right pane, click on the name of the linuxssh Network interface



Task 5 - Configure VNET Peering FGAP

12. In the left Network interface menu, scroll all the way down and click on **Effective routes**



13. Confirm the routing entry for the VNET peering is showing as per below. This view is very useful for troubleshooting Azure routing issues.

Scope: Network interface (linuxssh645)

Associated route table: -

Effective routes

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address	User Defined Route Name
Default	Active	10.3.0.0/16	Virtual network	-	-
Default	Active	10.1.0.0/16	VNet peering	-	-
Default	Active	0.0.0.0/0	Internet	-	-
Default	Active	10.0.0.0/8	None	-	-
Default	Active	100.64.0.0/10	None	-	-
Default	Active	172.16.0.0/12	None	-	-
Default	Active	25.48.0.0/12	None	-	-
Default	Active	25.4.0.0/14	None	-	-

2

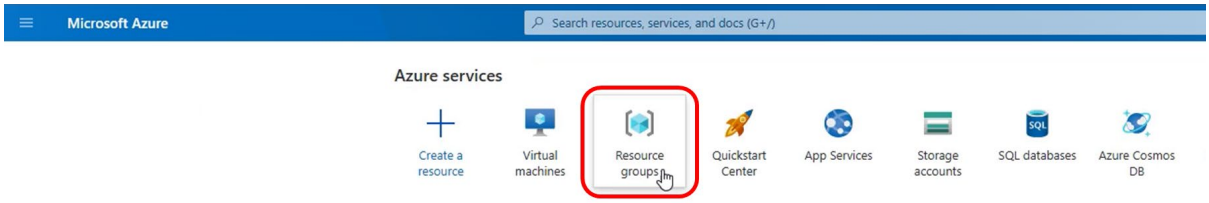
14. The VNET peering is complete

Task 6 - Configure Workload subnet UDR

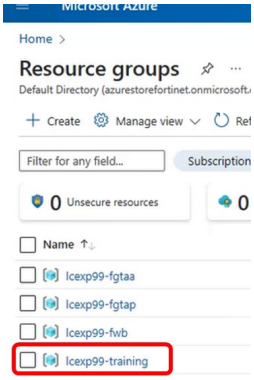
The next step is the creation and configuration of the user defined route to force the traffic destined to the Internet from the workload DMZ subnet to go out via the FortiGate firewalls.

Creation and configuration steps

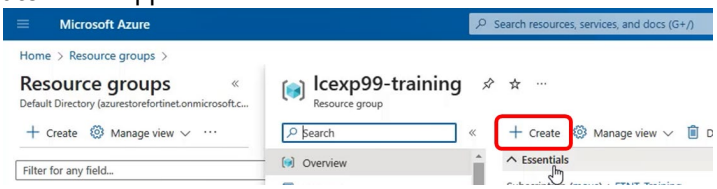
1. From the main Azure Portal, click on **Resource groups**



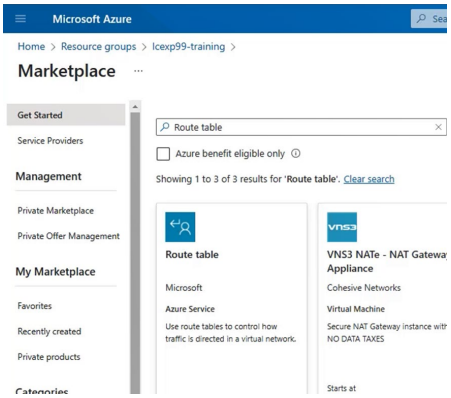
2. Click on the lcexp***<your student number>***-training resource group name itself to open a new pane on the right.



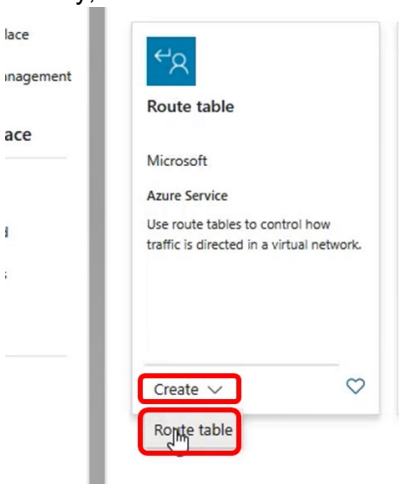
3. Click on the **+ Create** in the upper middle



4. In the Marketplace pane, search for **Route Table**

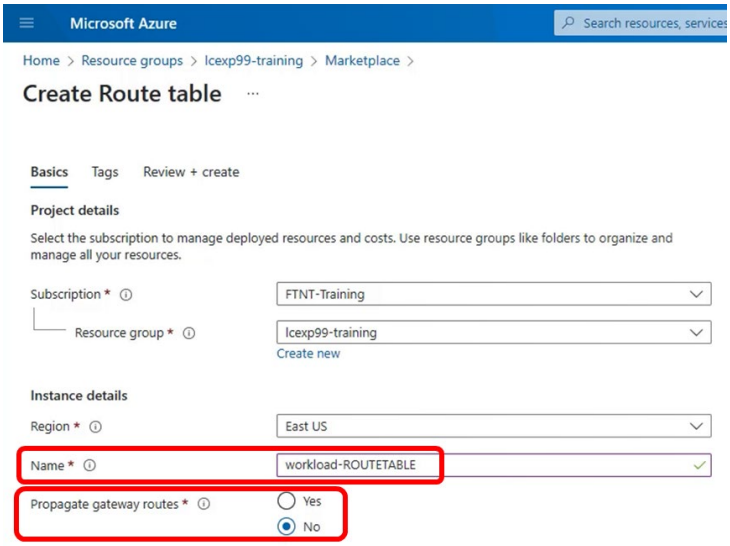


5. At the bottom of the Route table entry, click on **Create** and **Route table**



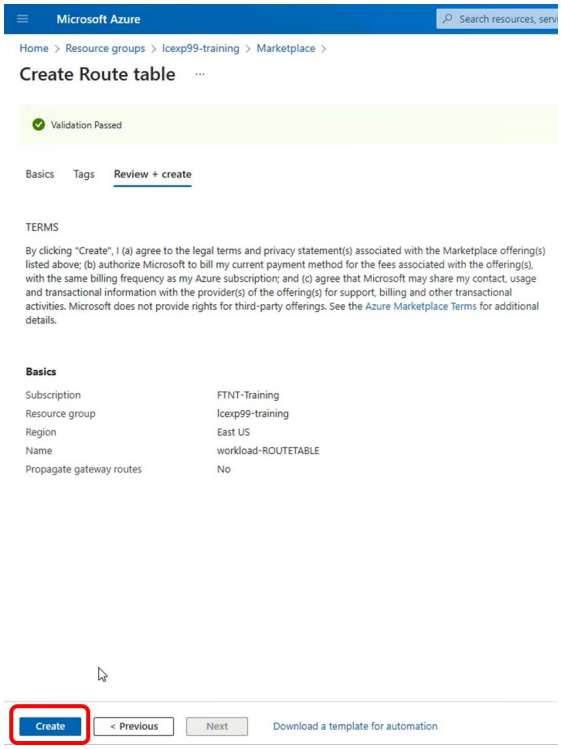
6. In the Create Route table pane, use the following information from the table to fill out the page as showed in the image below

Name	Workload-ROUTETABLE
Propagate gateway routes	no



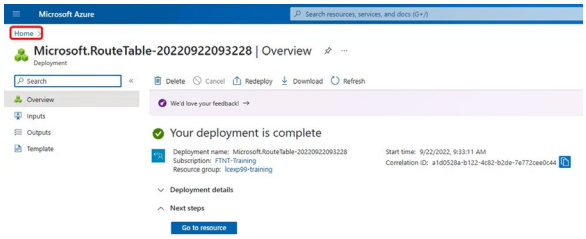
7. Click on **Next: Tags** at the bottom, there is nothing to change in the Tags pane
8. Click on **Review + create** at the bottom

9. Click on **Create** after confirming the information entered.



10. As before a prompt will show that the deployment is in progress. From this point forward in the lab guide, this step will be omitted for brevity

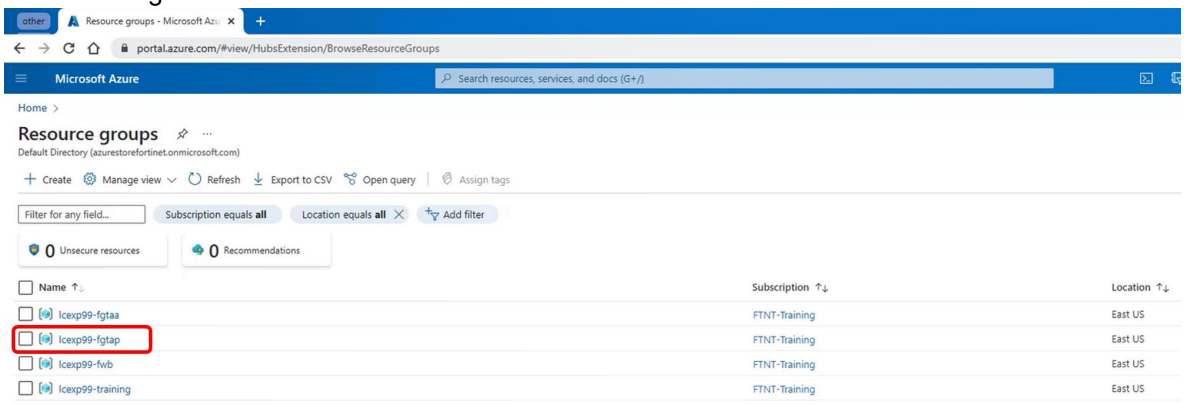
11. From the deployment completion screen, click on **Home** in the upper right corner



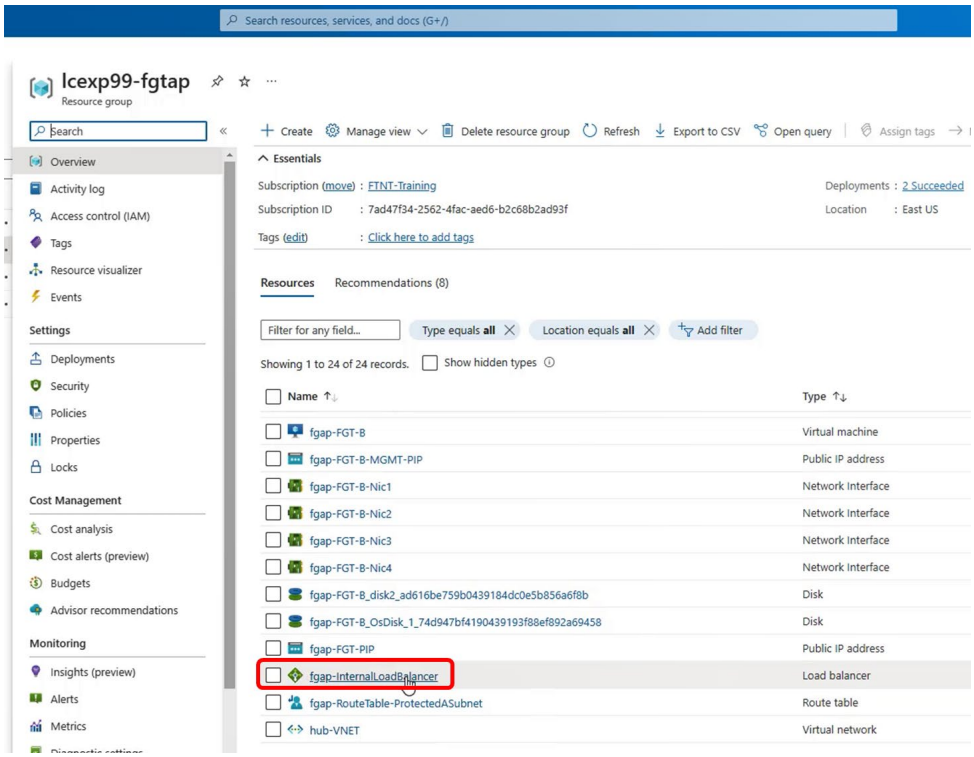
12. Click on **Resource groups**

Task 6 - Configure Workload subnet UDR

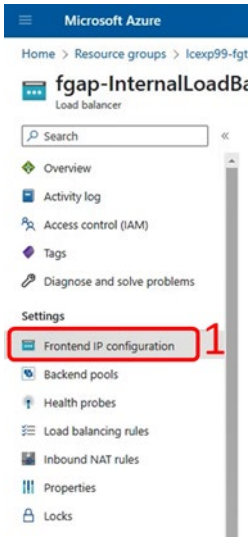
13. Click on the lcexp***<your student number>***-fgtap resource group name itself to open a new pane on the right.



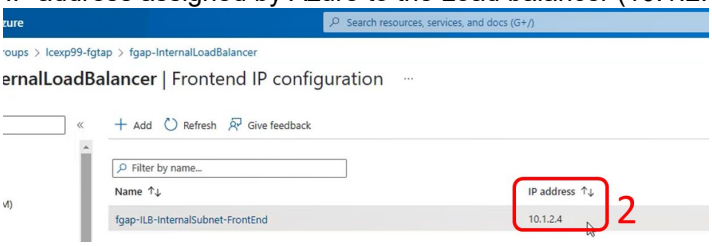
14. In the resource group pane, scroll down and click on the name **fgap-internalLoadBalancer**



15. In the left Load Balancer menu, click on **Frontend IP configuration**

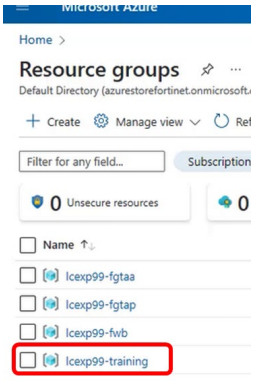


16. Make note of the IP address assigned by Azure to the Load balancer (10.1.2.4 in this example)



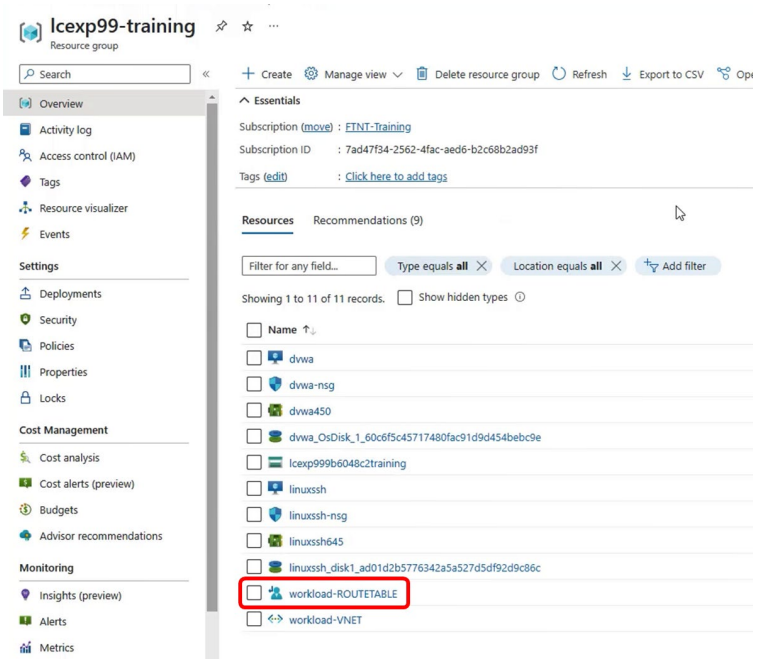
17. Click back on home and then **Resource groups**

18. Click on the lcexp***<your student number>***-training resource group name itself to open a new pane on the right.

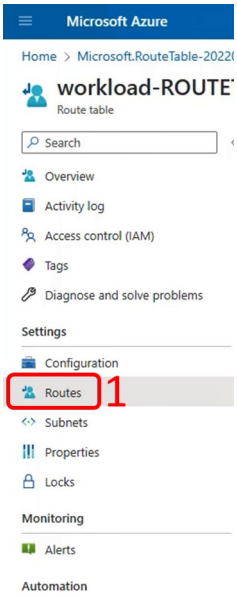


Task 6 - Configure Workload subnet UDR

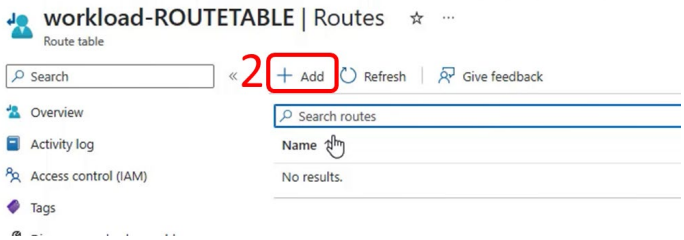
19. Scroll down and click on the name itself of the route table workload-ROUTETABLE



20. In the Route table menu on the left, click on **Routes**



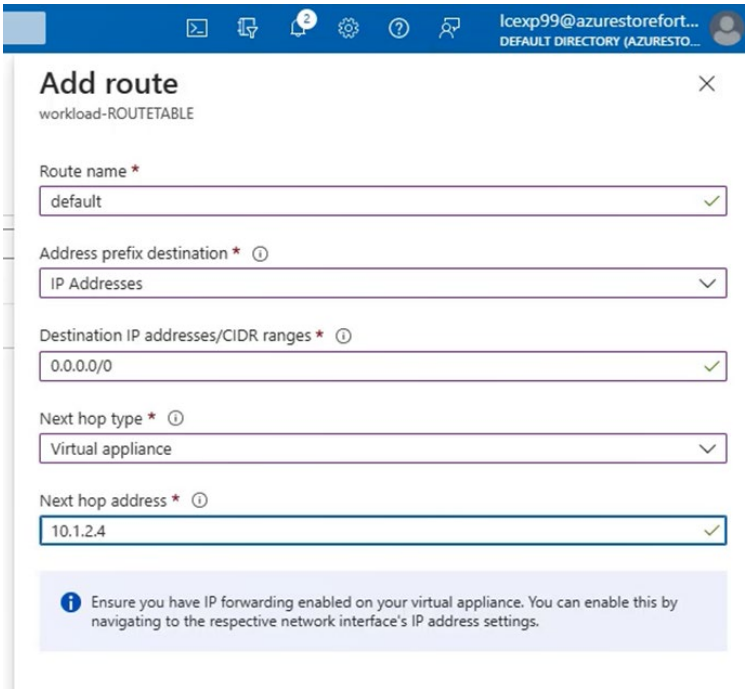
21. In the right pane, click on **+ Add**



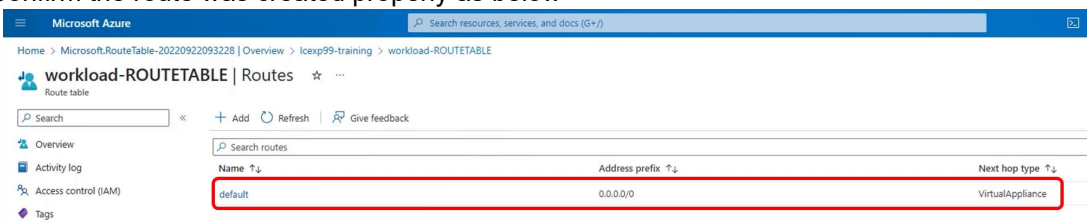
Task 6 - Configure Workload subnet UDR

22. Use the following information from the table to fill out the page as showed in the image below

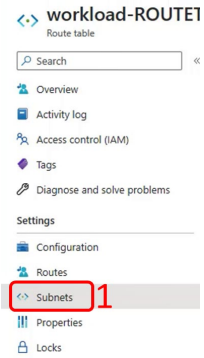
Route name	default
Address prefix destination	IP Addresses
Destination IP address/CIDR ranges	0.0.0.0/0
Next hop type	Virtual appliance
Next hop address	10.1.2.4



23. Click **Add**
24. Confirm the route was created properly as below

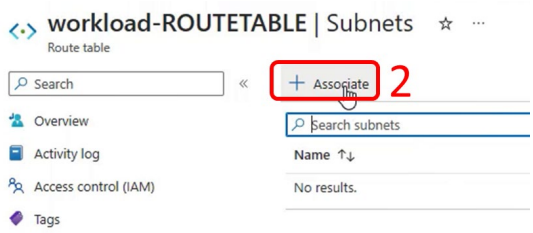


25. Scroll down on the Route table left menu to Subnets



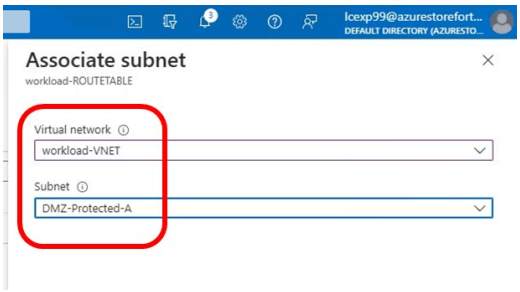
Task 6 - Configure Workload subnet UDR

26. Next click on **+ Associate**

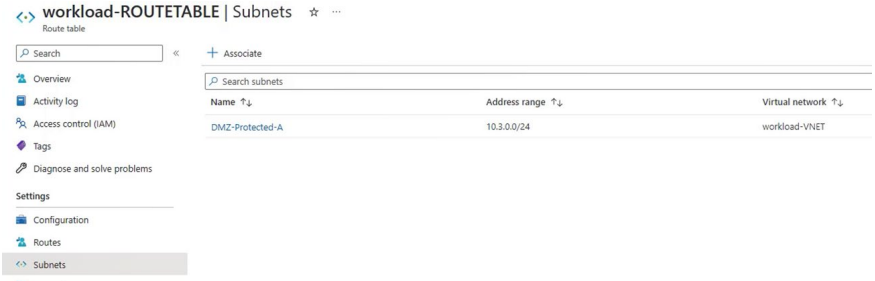


27. Use the following information from the table to fill out the right pane as showed in the image below, then click **Accept**

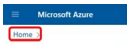
Virtual network	Workload-VNET
Subnet	DMZ-Protected-A



28. Confirm the subnet association was successful as per the screen below:



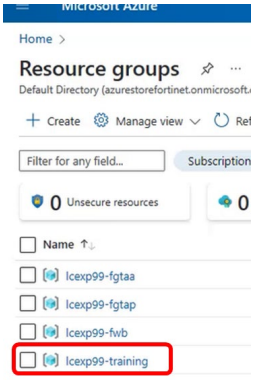
29. Click on **Home** in the upper left corner



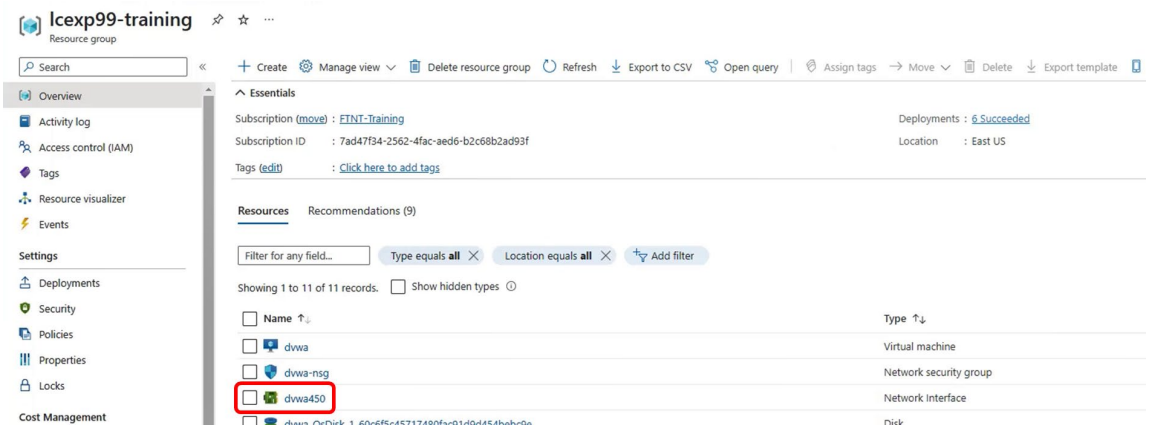
30. Click on **Resource groups**

Task 6 - Configure Workload subnet UDR

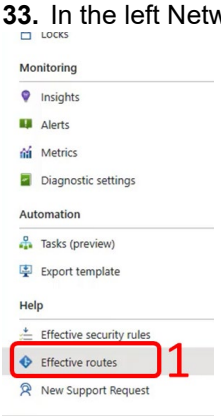
31. Click on the lcexp***<your student number>***-training resource group



32. In the right pane, click on the name of the dvwa Network interface, the number that is part of the name is random for each student.

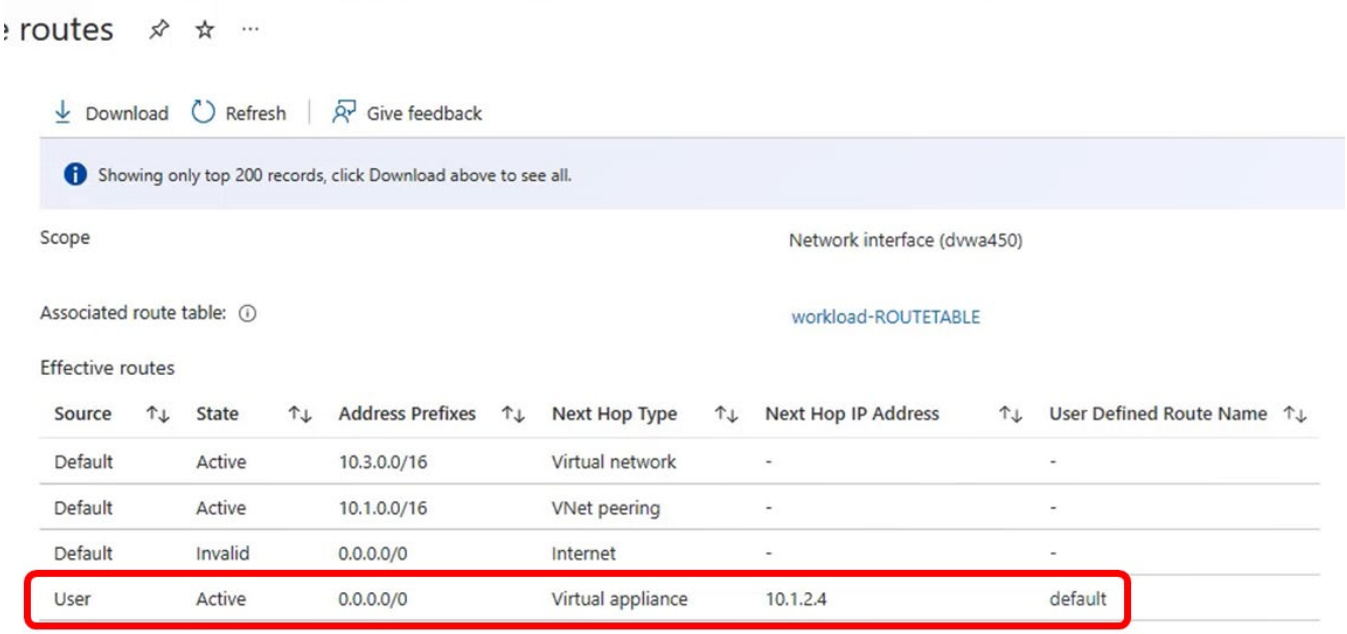


33. In the left Network interface menu, scroll down to click on **Effective routes**

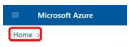


Task 6 - Configure Workload subnet UDR

34. In the right Effective routes pane, confirm the user defined route previously defined as per below



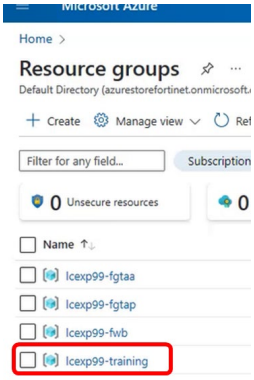
35. Click on **Home** in the upper left corner



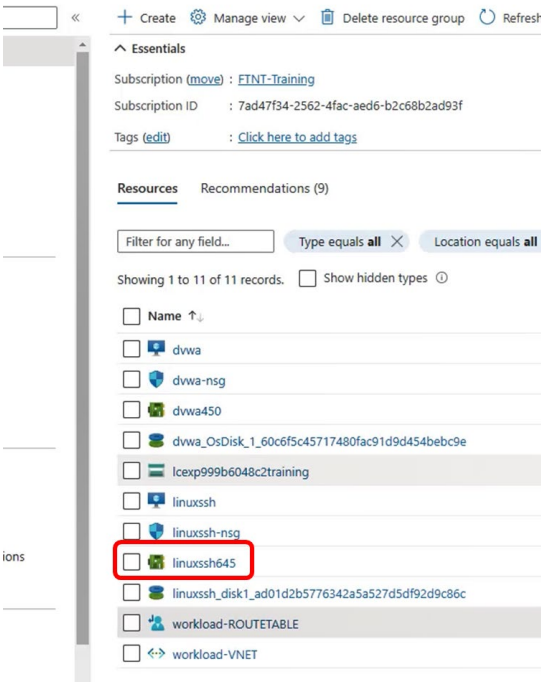
36. Click on **Resource groups**

Task 6 - Configure Workload subnet UDR

37. Click on the lcexp***<your student number>***-training resource group

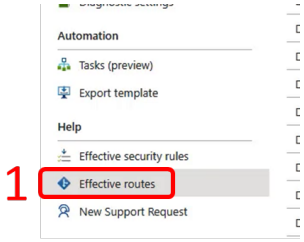


38. In the right pane, click on the name of the linuxssh Network interface. The numbers that are part of the name are random.

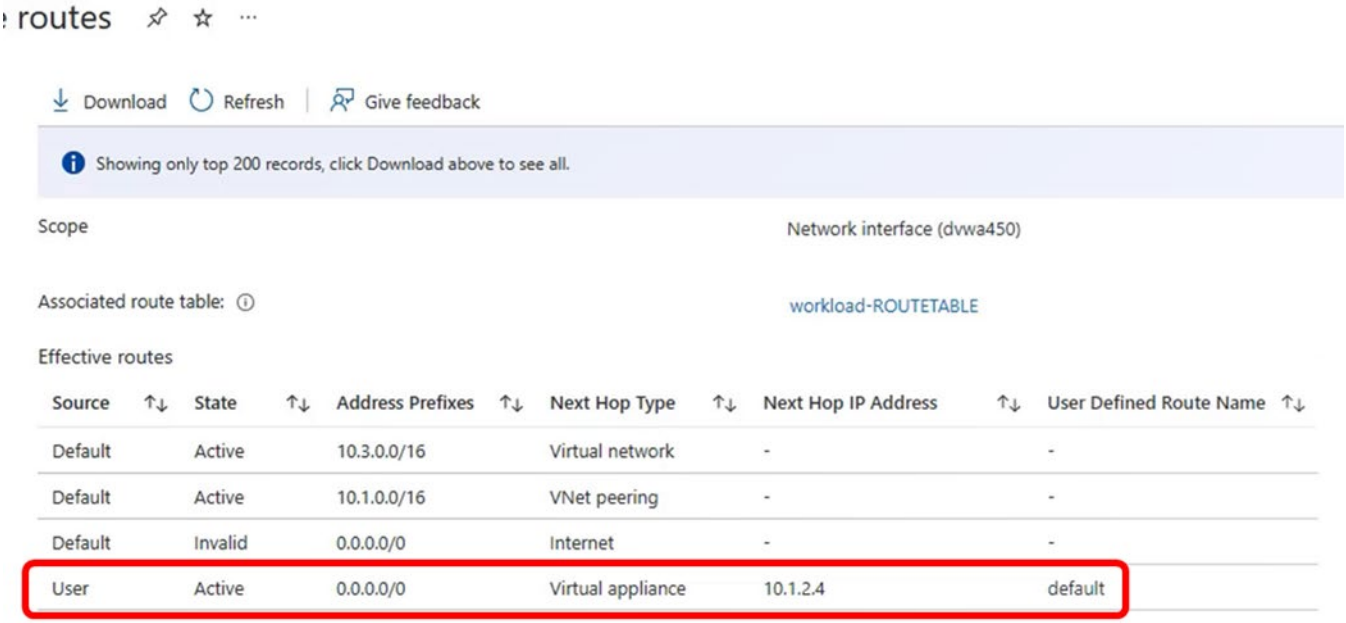


Task 6 - Configure Workload subnet UDR

39. In the left Network interface menu, scroll all the way down and click on **Effective routes**



40. In the right Effective routes pane, confirm the user defined route previously defined as per below



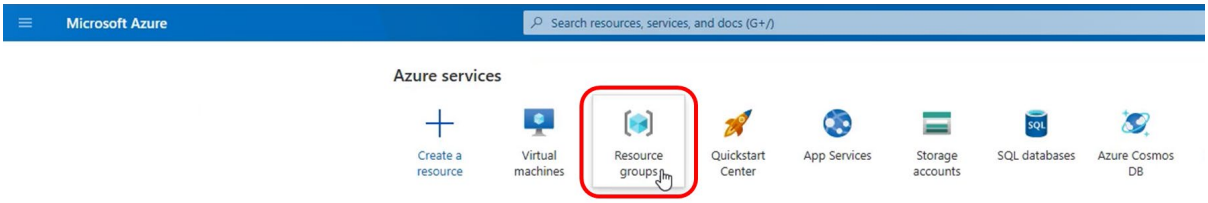
41. The user defined route has been deployed successfully

Task 7 - Configure FortiGate Active Passive

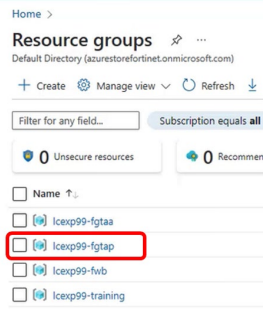
The next step is the configuration of the FortiGate firewalls deployed in Active-Passive mode located in the Inbound VNET.

Configuration steps

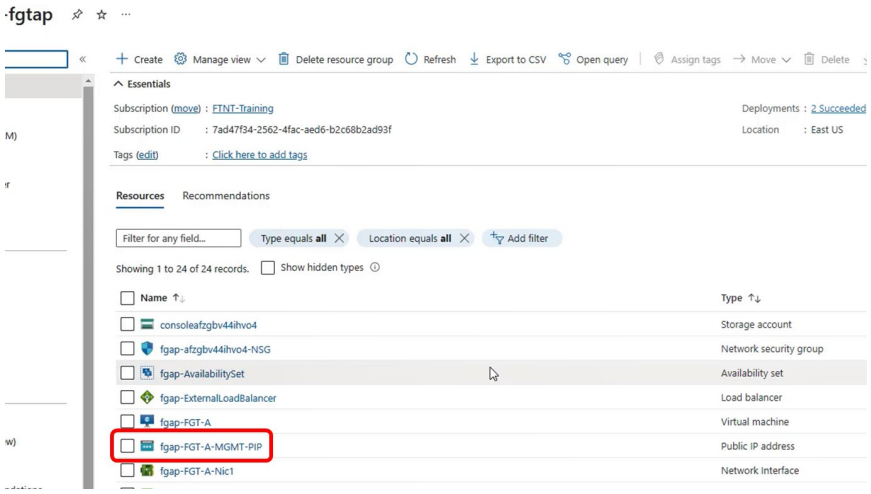
1. From the main Azure Portal, click on **Resource groups**



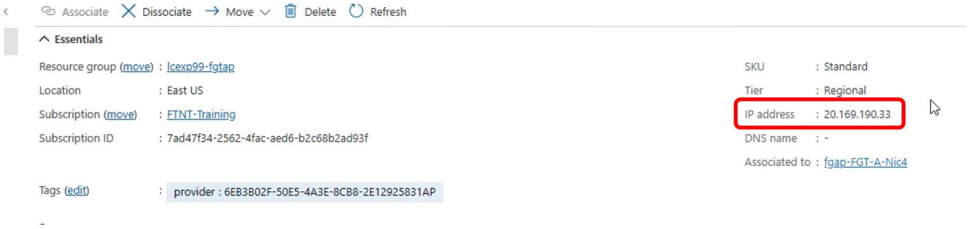
2. Click on the lcexp***<your student number>***-fgtap resource group name itself to open a new pane on the right.



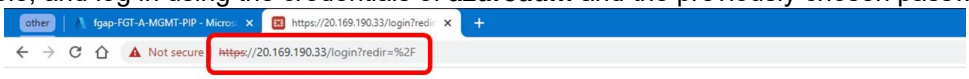
3. In the right pane, click on the public IP named **fgpa-FGT-A-MGMT-PIP**

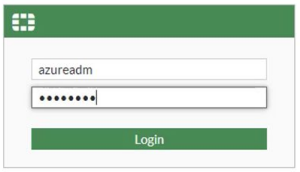


4. Make note of the public IP address of the management interface of FortiGate fgap-FGT-A, 20.169.190.33 in this example

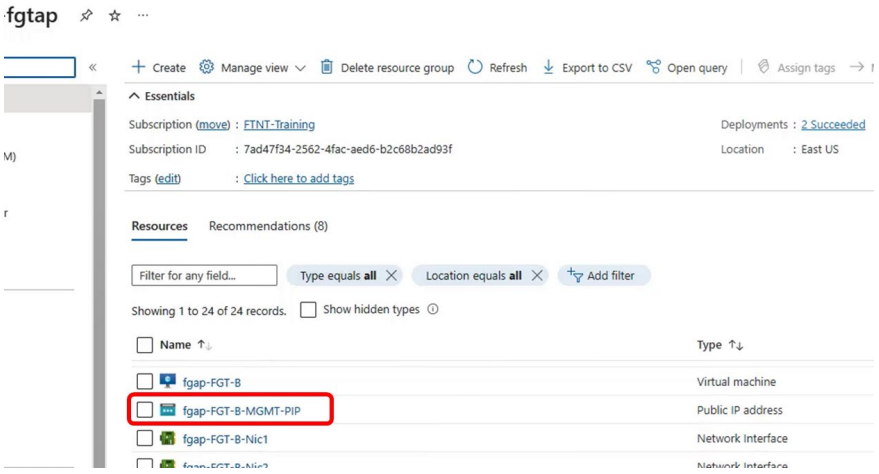


5. Open a new web browser tab to https of that public IP address, https://20.169.190.33 in this example, and log in using the credentials of **azureadm** and the previously chosen password.

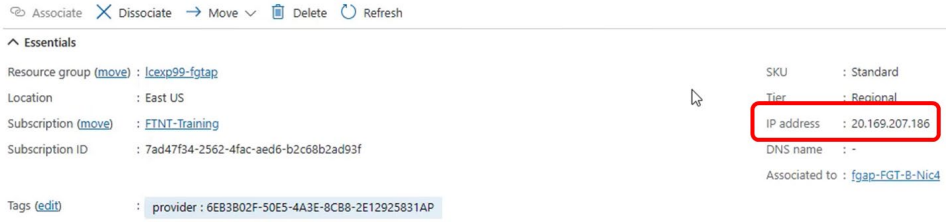




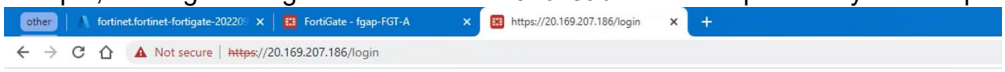
6. Go back to the lcexp***<your student number>***-fgtap resource group
7. In the right pane, click on the public IP named **fgpa-FGT-B-MGMT-PIP**

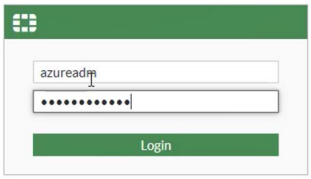


8. Make note of the public IP address of the management interface of FortiGate fgap-FGT-B, 20.169.207.186 in this example

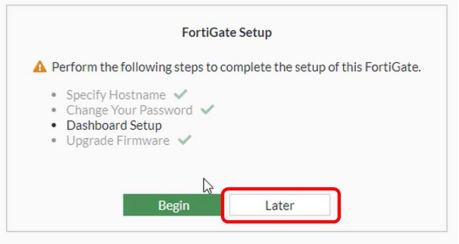


9. Open another new web browser tab to https of that public IP address, https://20.169.207.186 in this example, and log in using the credentials of **azureadm** and the previously chosen password.

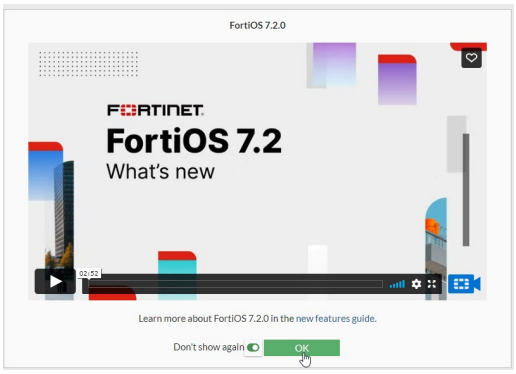




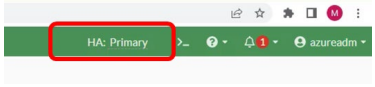
10. On both FortiGate web browser tabs dismiss the FortiGate Setup prompt by clicking **Later**



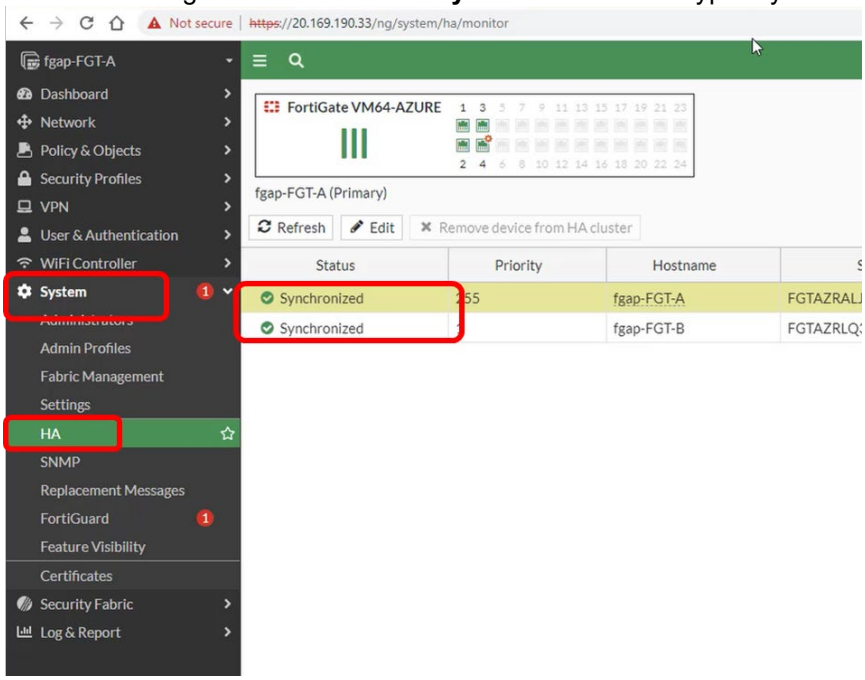
11. Dismiss the subsequent prompt as well by clicking **OK**



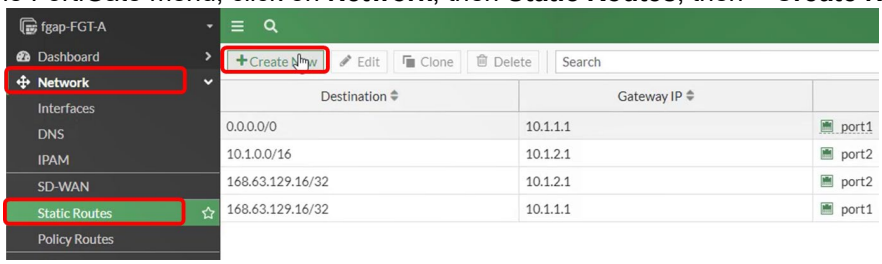
12. Near the upper right corner, confirm the FortiGate selected says HA: Primary. If it says HA: Secondary, change to the web browser tab of the other FortiGate



13. In the left FortiGate menu of the primary FortiGate, click on **System** and then on **HA**, ensure that both FortiGate are showing under the status of **Synchronized**. This typically takes 5 minutes.

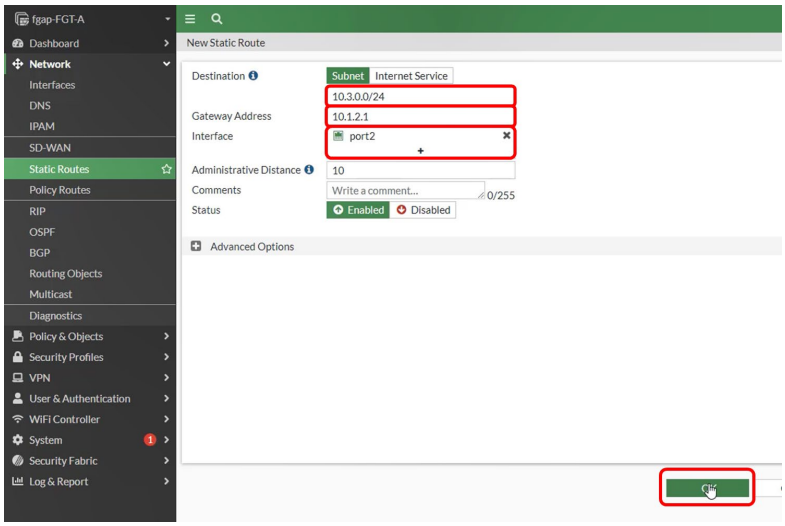


14. In the same FortiGate menu, click on **Network**, then **Static Routes**, then **+ Create New**

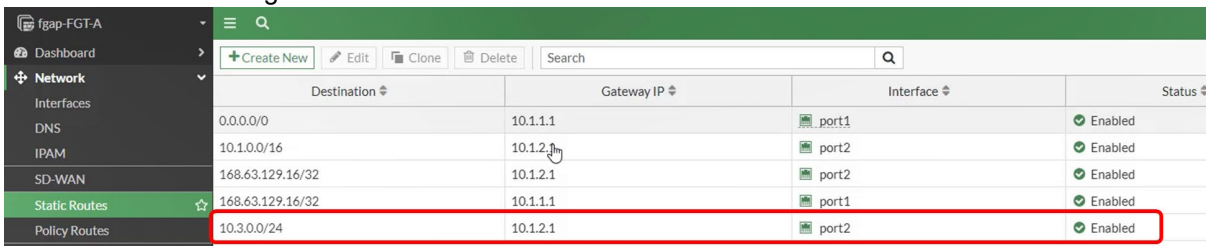


15. Use the following information from the table to fill out the New Static Route as showed in the image below then click **OK**

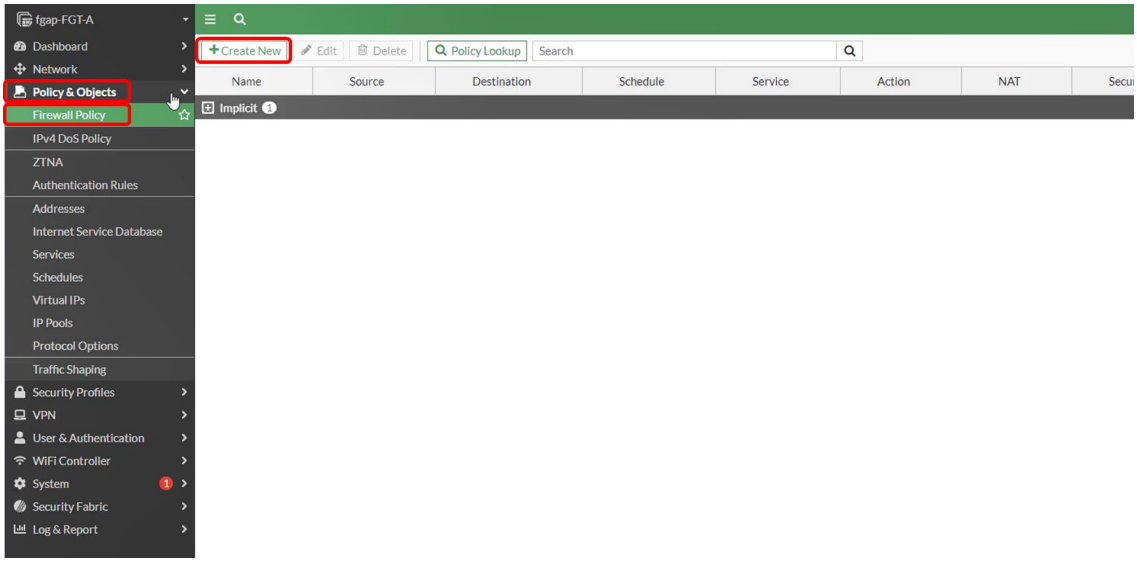
Destination	Subnet 10.3.0.0/24
Gateway Address	10.1.2.1
Interface	port2



16. Confirm the routing entries with the screen below

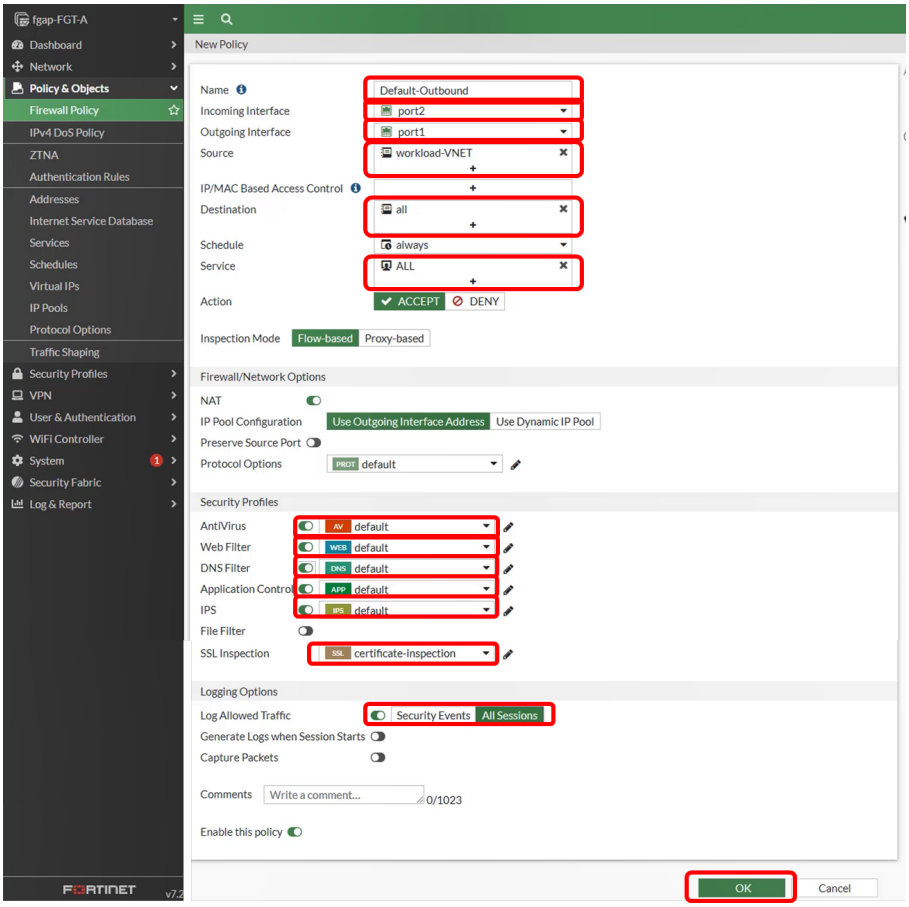


17. In the same FortiGate menu, click on **Policy and Objects**, then **Firewall Policy**, then **+ Create New**



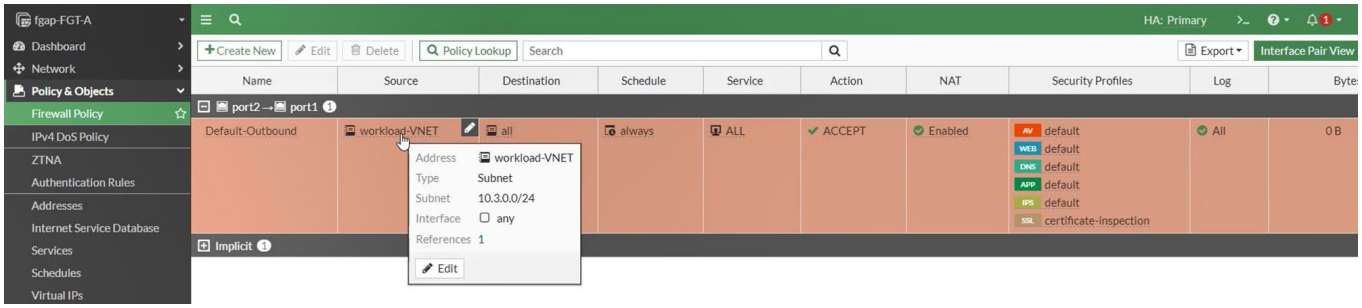
18. Use the following information from the tables to fill out the Policy as showed in the image below then click **OK**

Name	Default-Outbound
Incoming Interface	port2
Outgoing Interface	port1
Source	**Create New Address** **Name** workload-VNET **Type** Subnet **IP/Netmask** 10.3.0.0/24
Destination	all
Service	ALL
AntiVirus	Enabled with default
Web Filter	Enabled with default
DNS Filter	Enabled with default
Application Control	Enabled with default
IPS	Enabled with default
SSL Inspection	certificate-inspection
Log Allowed Traffic	All Sessions



Task 7 - Configure FortiGate Active Passive

19. Confirm the Policy created with the screen below



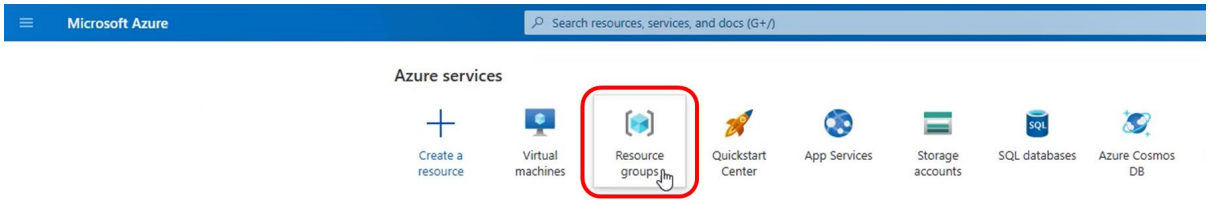
20. You have completed the configuration of the FortiGate Active Passive firewalls

Task 8 – Confirm VM outbound access

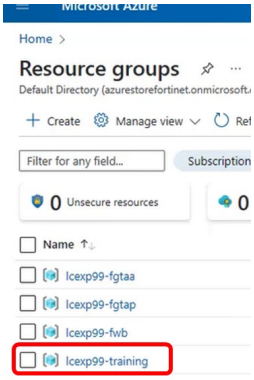
The next step is the confirmation of the traffic destined to the Internet from the VMs in the workload DMZ subnet to go out via the FortiGate FGAP firewalls located in the outbound VNET.

Creation and configuration steps

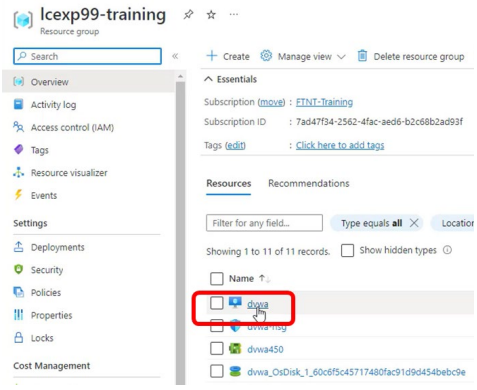
1. From the main Azure Portal, click on **Resource groups**



2. Click on the lcexp***<your student number>***-training resource group name itself to open a new pane on the right.

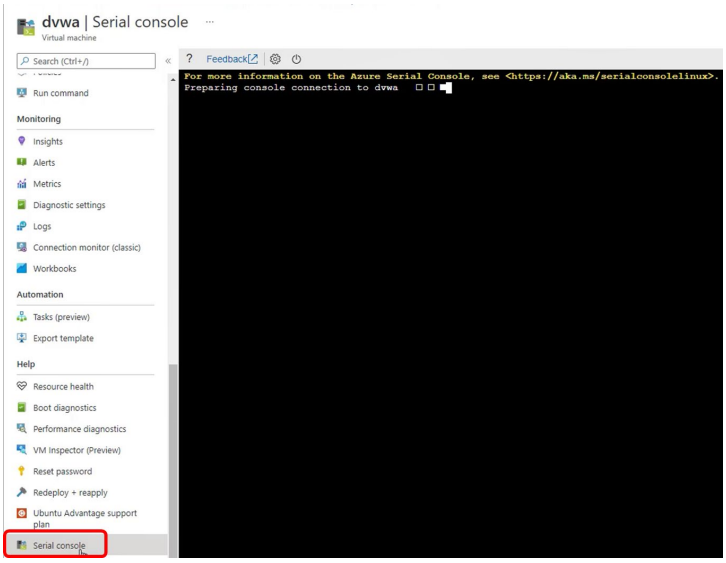


3. In the right pane, click on the name of the dvwa Virtual Machine

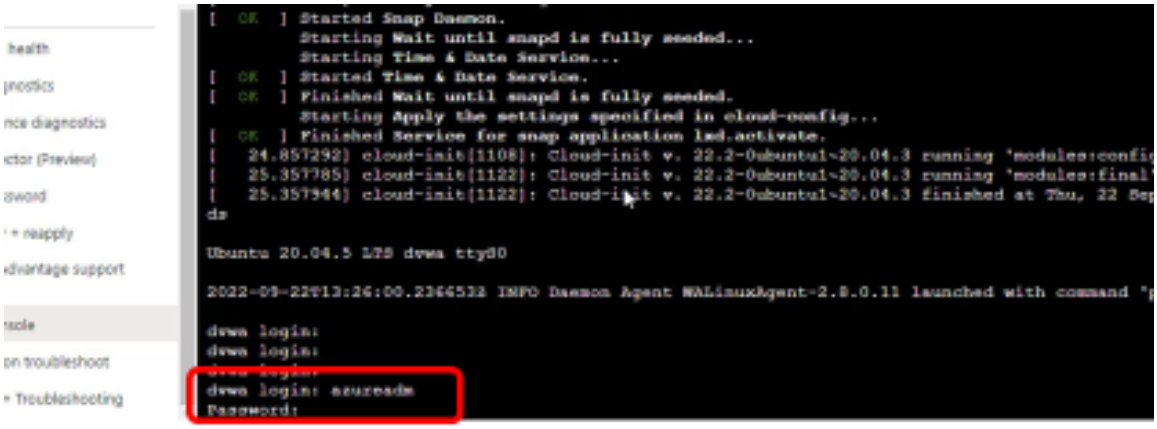


Task 8 – Confirm VM outbound access

4. In the Virtual machine left menu, scroll all the way down and select **Serial console**

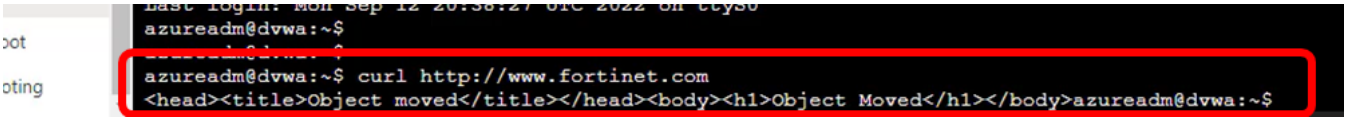


5. Login with the previously created credentials (**azureadm** and the chosen password)



6. Next confirm the VM has outbound access by using the command below

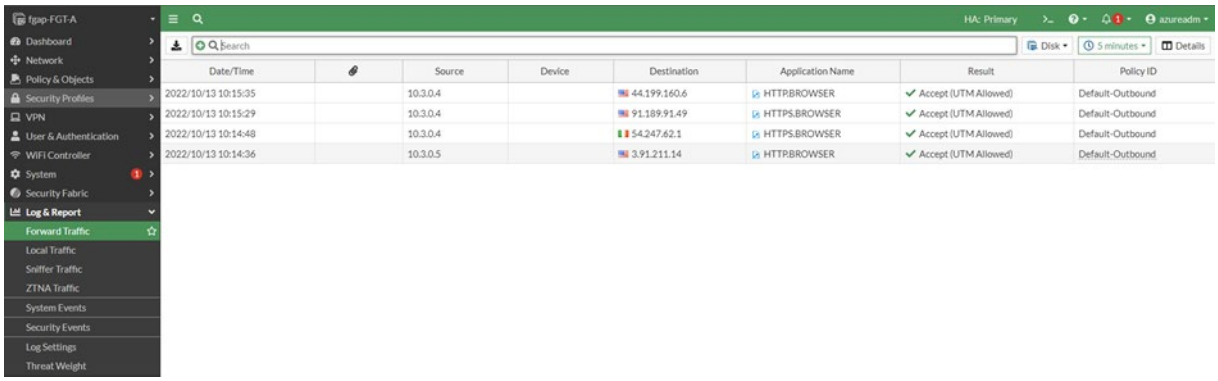
```
curl http://www.fortinet.com
```



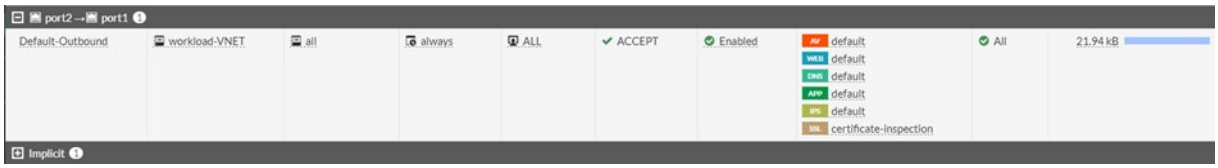
7. Repeat steps 3 to 6 for VM linuxssh

Task 8 – Confirm VM outbound access

8. Next in the same FortiGate menu, click **Log & Report** then **Forward Traffic**. Confirm the traffic is indeed passing through the FortiGate



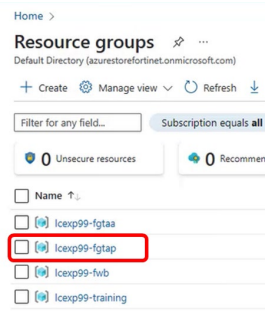
9. In the same FortiGate menu, click on **Policy and Objects**, then **Firewall Policy**, then confirm the number of bytes transferred is also increasing in that particular security policy



10. Due to service quota limitations in the Azure training account, the entire content of the FGAP resource groups needs to be deleted. In a normal production environment, this would not happen.

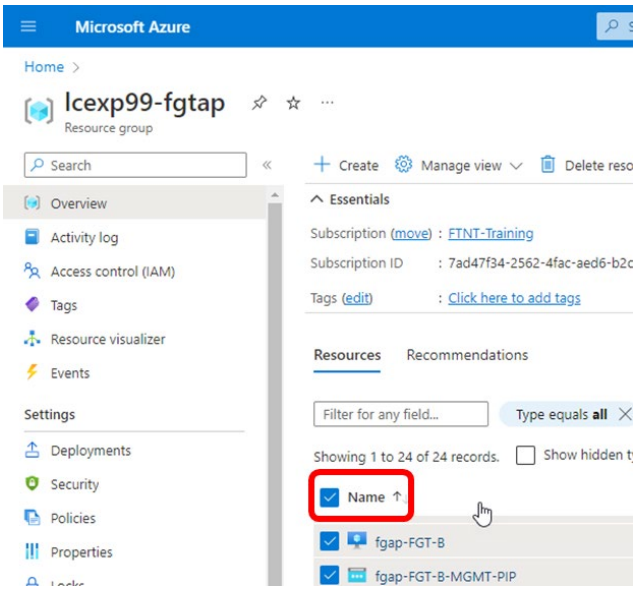
11. From the main Azure Portal, click on **Resource groups**

12. Click on the lcexp***<your student number>***-fgtap resource group name itself to open a new pane on the right.

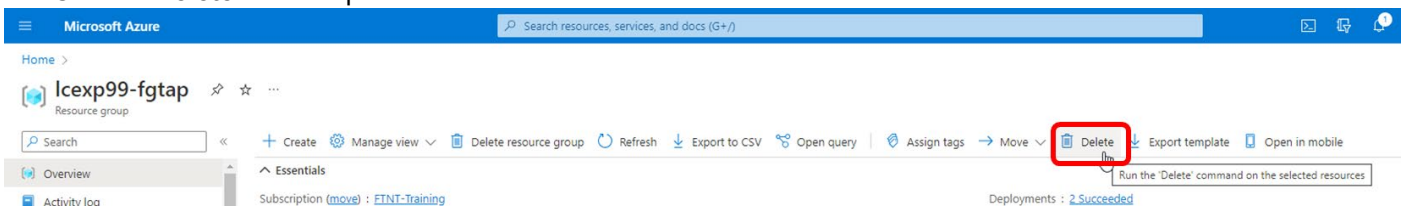


Task 8 – Confirm VM outbound access

13. Click on the ☐ (square) next to the Name header to automatically select all the items in the resource group

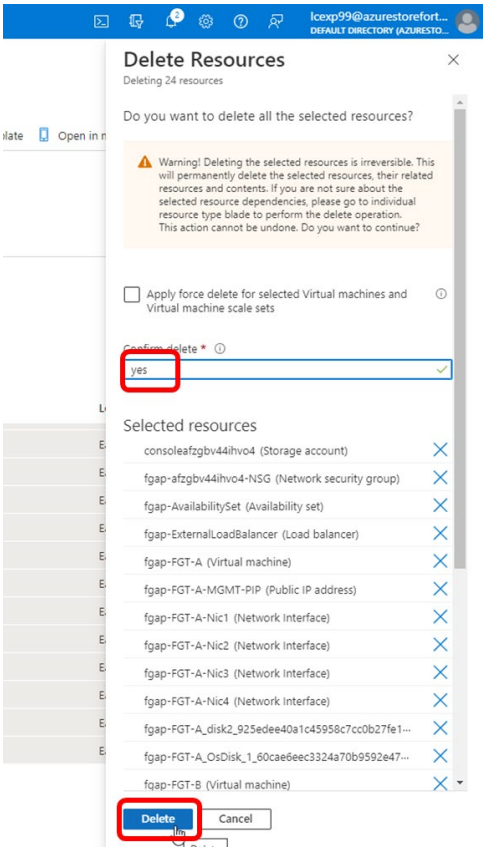


14. Click on **Delete** on the top menu



Task 8 – Confirm VM outbound access

15. Type in **yes** to confirm and then click **Delete**



16. A notification will appear (omitted for brevity)

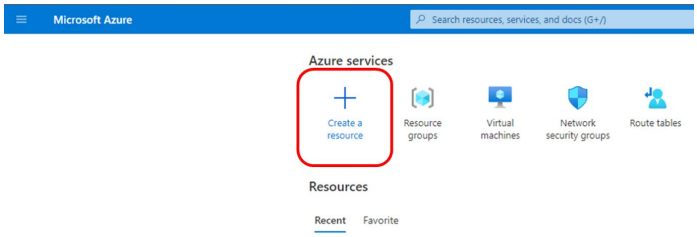
17. Upon completion, this task is now complete

Task 9 - Deploy FortiGate Active-Active

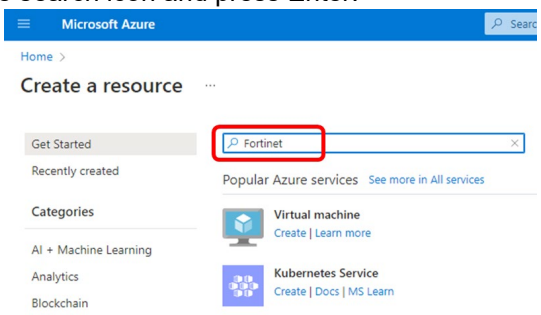
The next step is the deployment of the of the FortiGate firewalls (in Active-Active) along with associated network resources including the virtual network for the Internet Ingress Hub.

Deployment steps

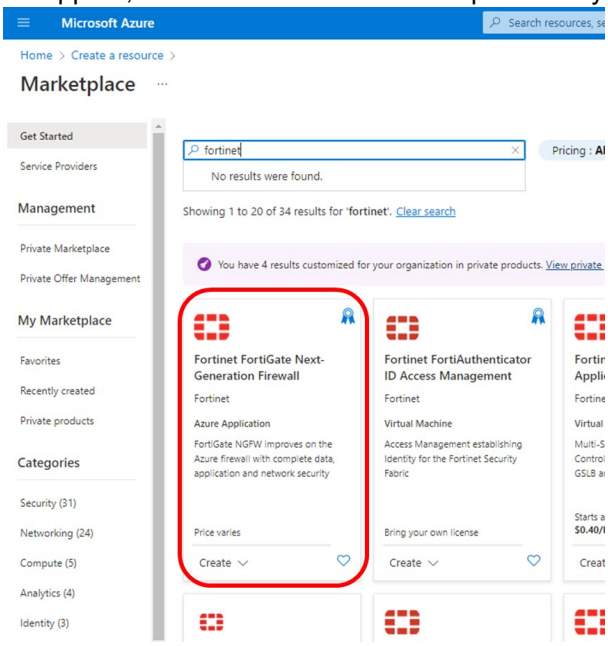
1. From the main Azure Portal, click on **Create a resource**



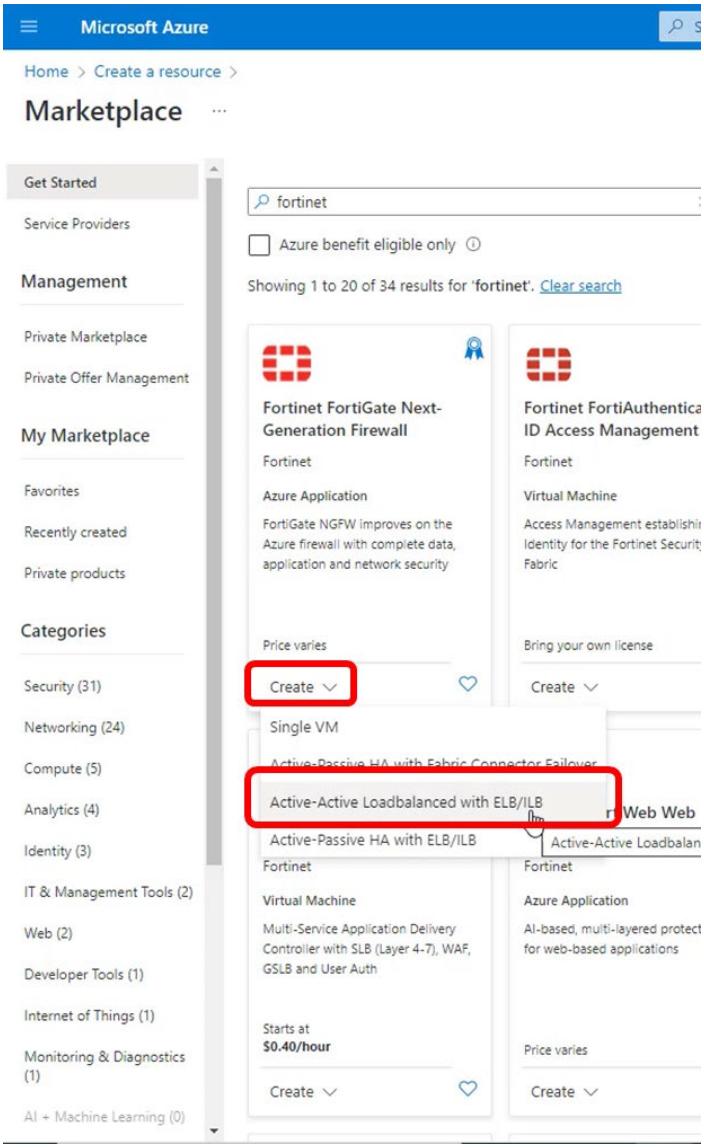
2. Type **Fortinet** next to the search icon and press Enter.



3. The following results will appear, look at the FortiGate Marketplace Entry

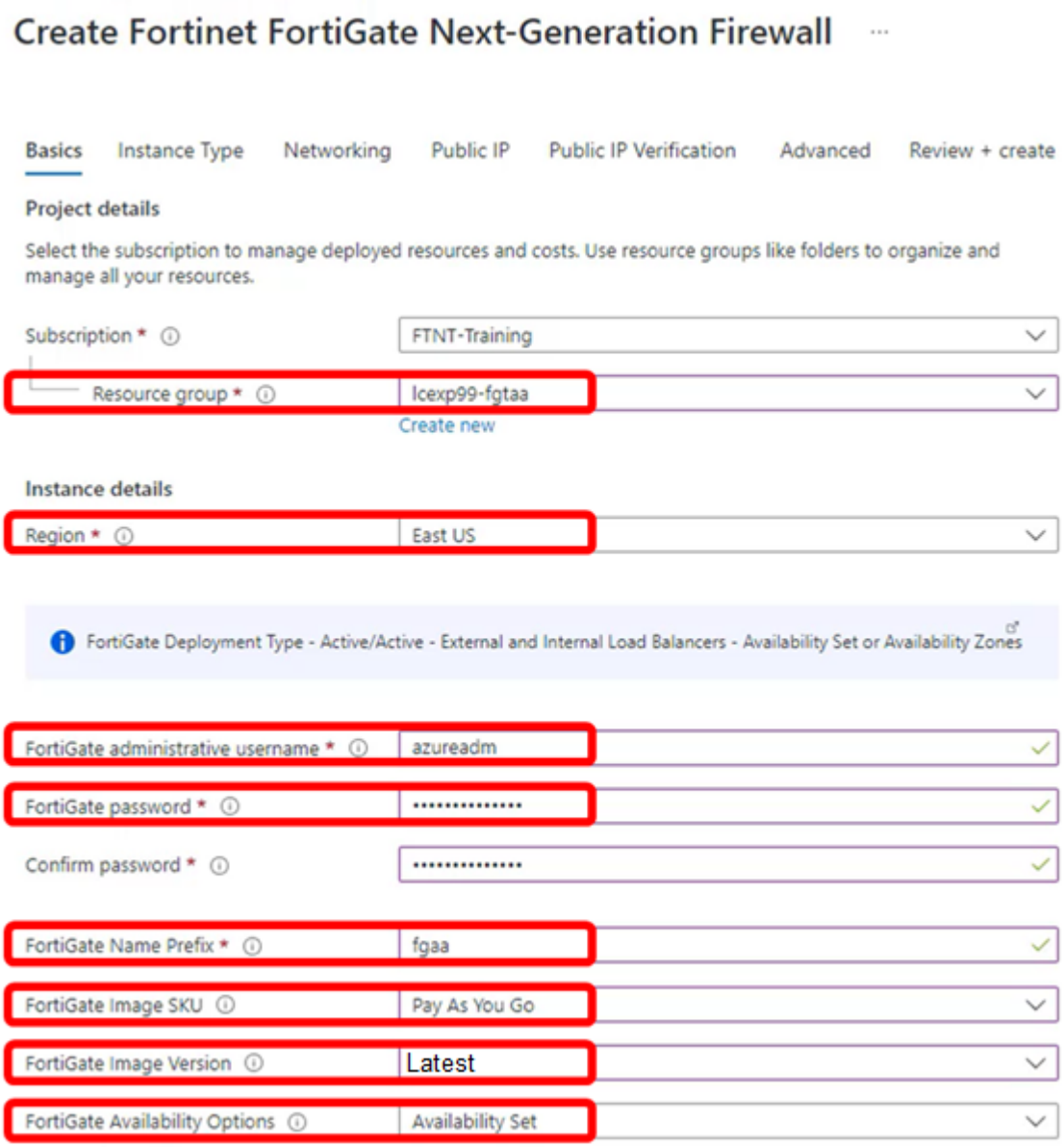


4. In that same FortiGate entry, click on **Create**, then click on **Active-Active LoadBalanced with ELB/ILB.**



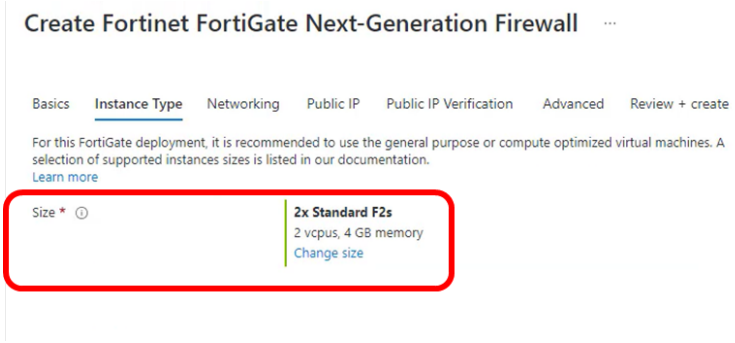
5. Use the following information from the table to fill out the page as showed in the image below

Subscription	FTNT-Training
Resource group	lcexp***<your student number>***-fgtaa
Region	(US) east US
FortiGate Administrative Username	azureadm
FortiGate password	***<choose your own>***
FortiGate Name Prefix	fgaa
FortiGate Image SKU	Pay As You Go
FortiGate Image Version	Latest

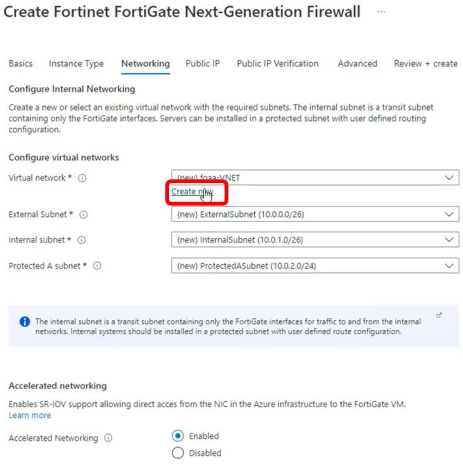


6. Click on **Next: Instance** or click on the **Instance** pane
7. Use the following information from the table to fill out the page as showed in the image below

Size	2x Standard F2s



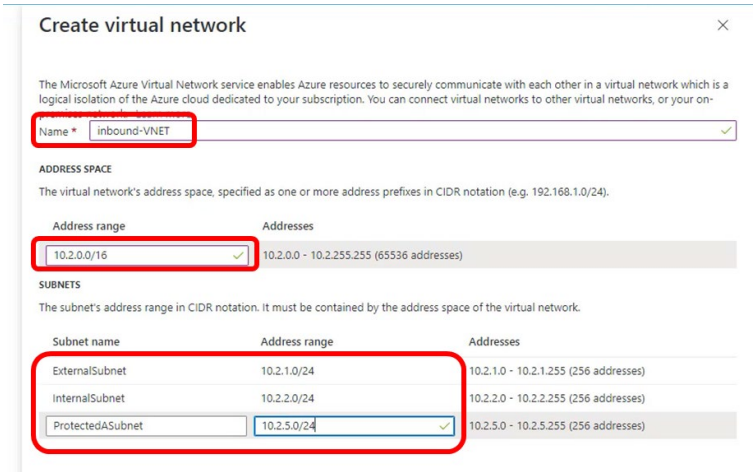
8. Click on **Next: Networking** or click on the **Networking** pane
9. Click **Create new** under Virtual network



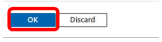
10. Use the following information from the table to fill out the page as showed in the image below, removing any default information

Name	inbound-VNET
Address range	10.2.0.0/16

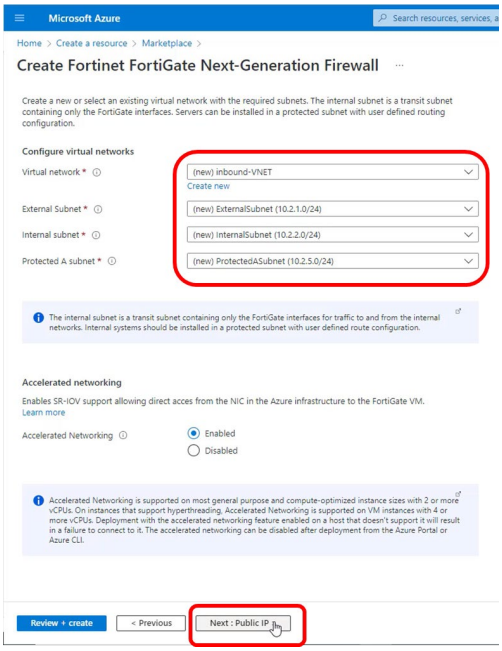
Subnet name	**Address range**
ExternalSubnet	10.2.1.0/24
InternalSubnet	10.2.2.0/24
ProtectedASubnet	10.2.5.0/24



11. Click **OK** to return to the networking pane

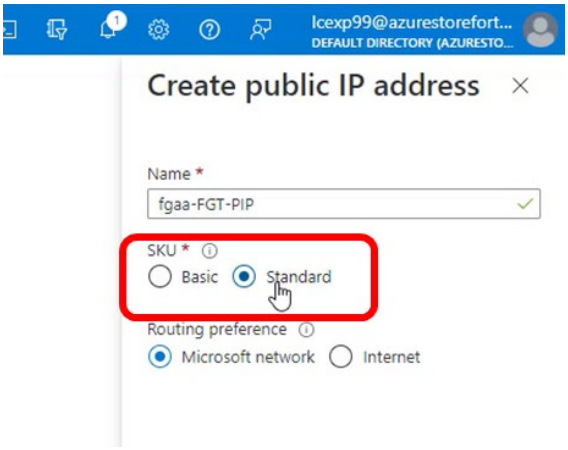


12. Confirm information entered matches the screen below and then click **Next: Public IP**



13. Under Public IP address, click **Create new** which will open a new pane on the right

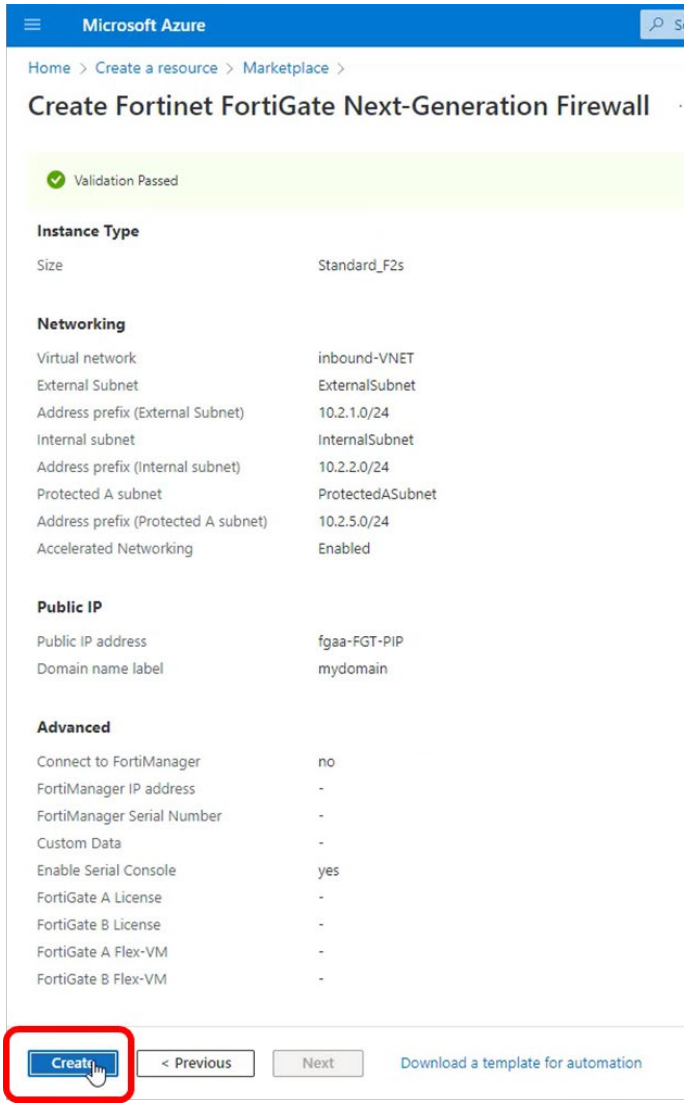
14. In the right pane named Create public IP address, select SKU **Standard** then click **OK** to return to the left pane



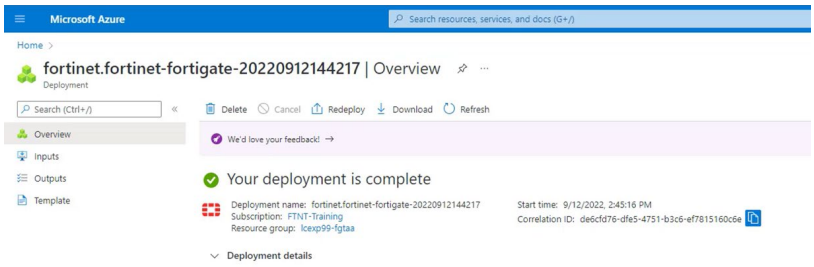
15. Click on **Next: Public IP Verification** at the bottom, then click on **Accept**
16. Confirm the Public IP has been validated

17. Click on **Next: Advanced** at the bottom, there is nothing to change in the Advanced pane
18. Click on **Next: Review + create** at the bottom

19. On the Review + create pane, verify that everything is set accordingly and click **Create**

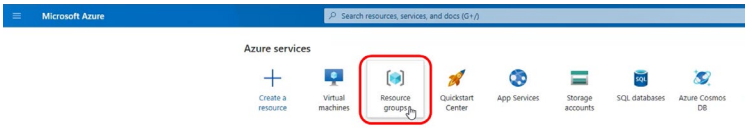


20. This template deploys several resources, expect 5 minutes for the deployment to complete

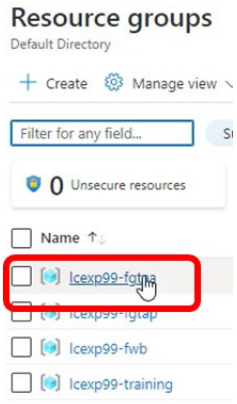


21. Since there is a limit of 200 route tables for each individual Azure Subscription, and that the route table deployed by this template is not being used by this lab, it needs to be disassociated and then deleted.

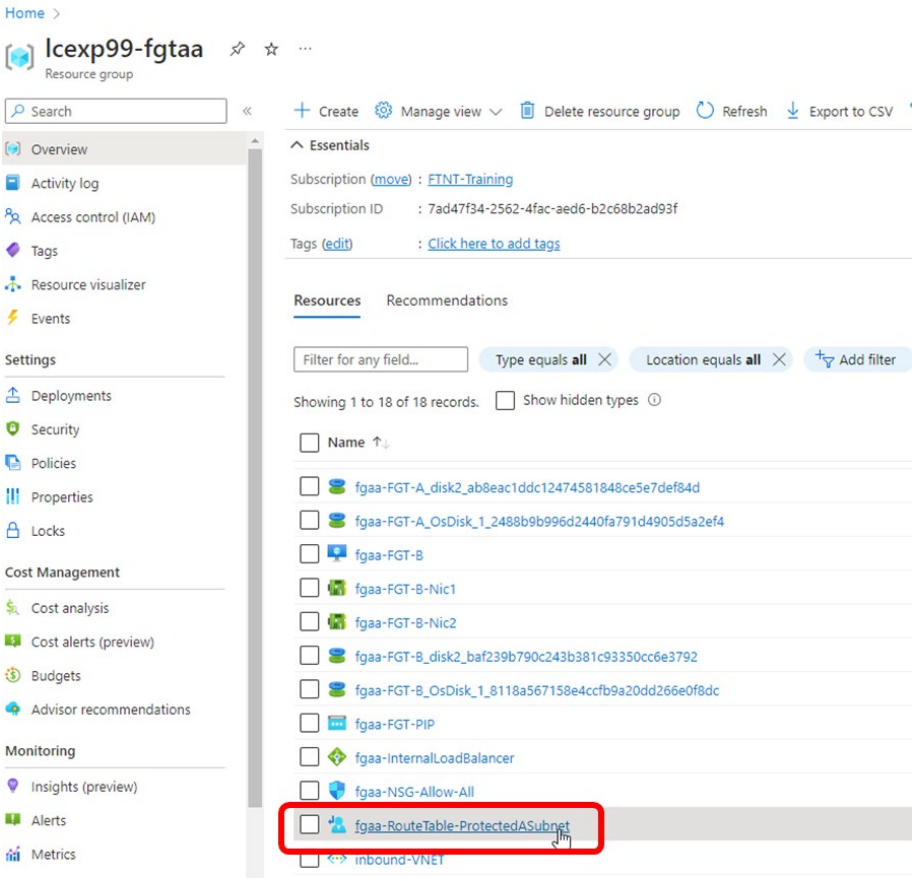
22. From the main Azure Portal, click on **Resource groups**



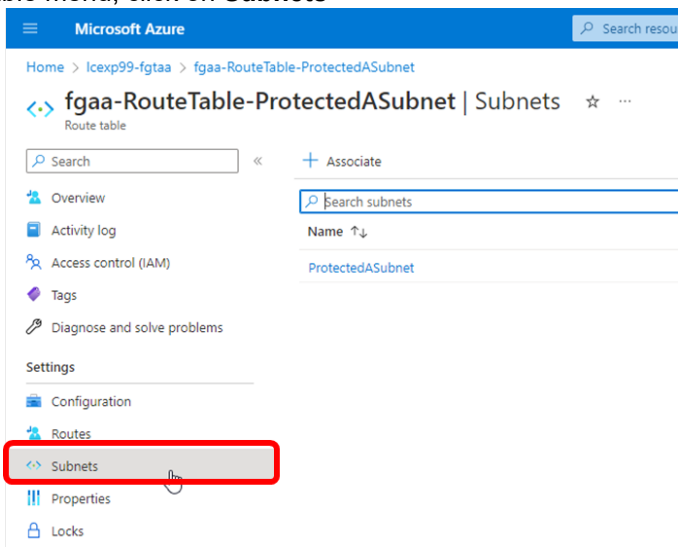
23. Click on the lcexp***<your student number>***-fgtaa resource group name itself to open a new pane on the right.



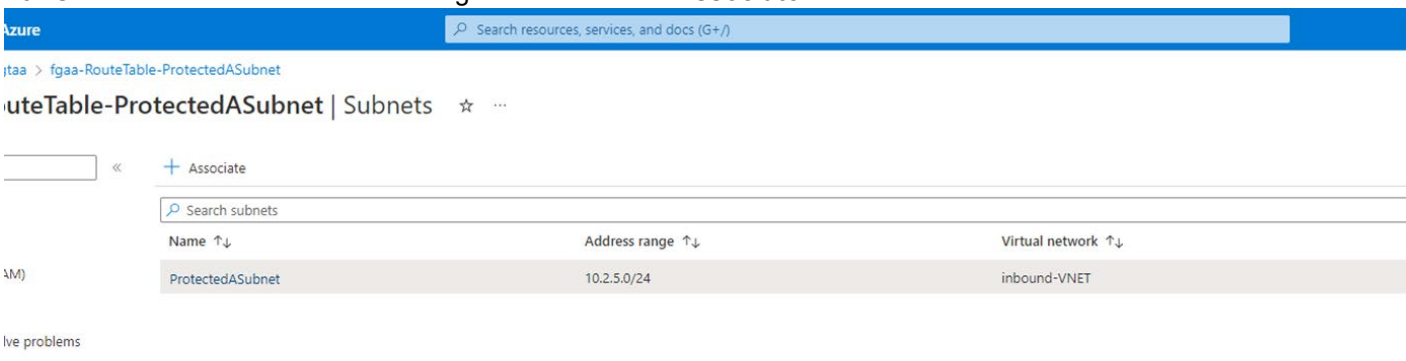
24. Scroll all the way down and click on the name **fgaa-RouteTable-ProtectedASubnet**



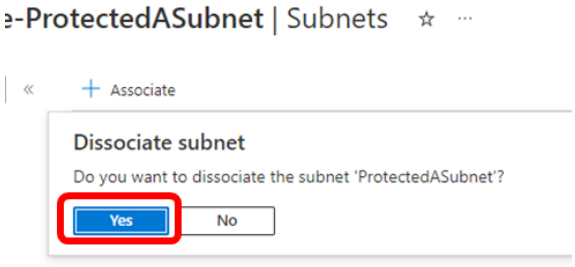
25. In the left Route table menu, click on **Subnets**



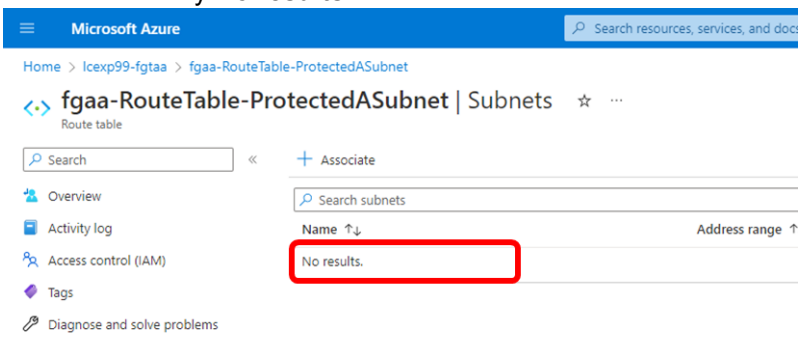
26. Click on the three dots **…** on the right side and then **Dissociate**



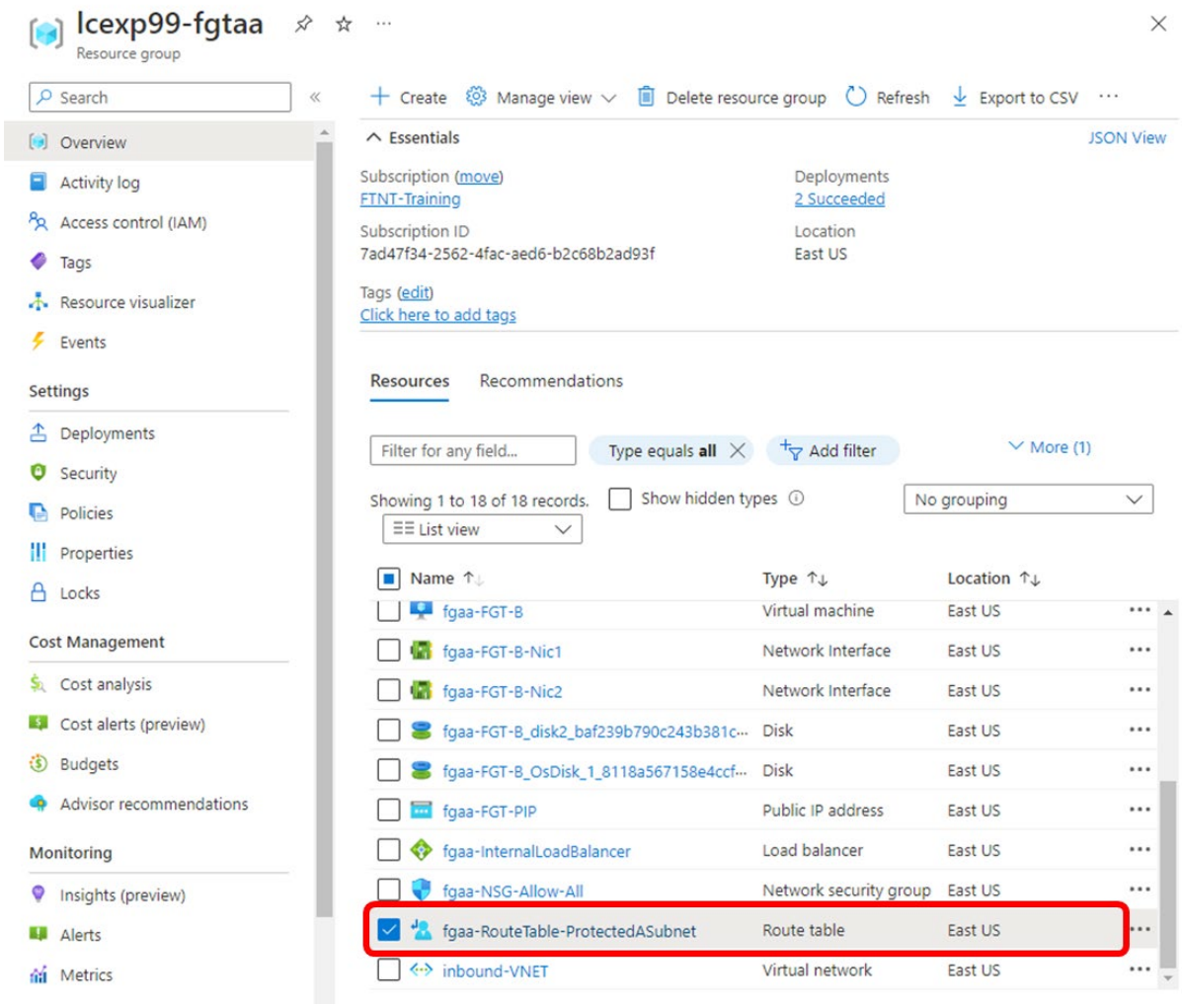
27. Confirm by clicking on Yes



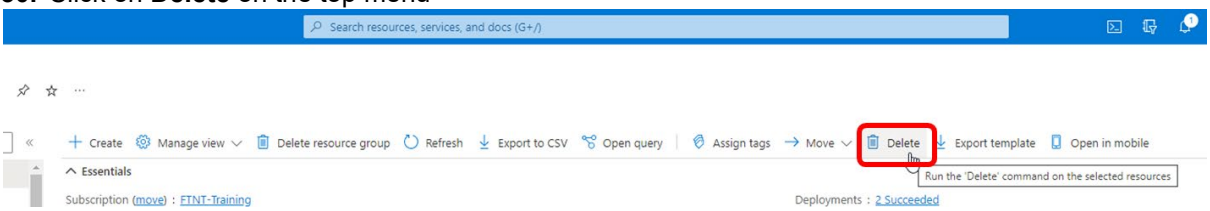
28. The right pane should now say **No results.**



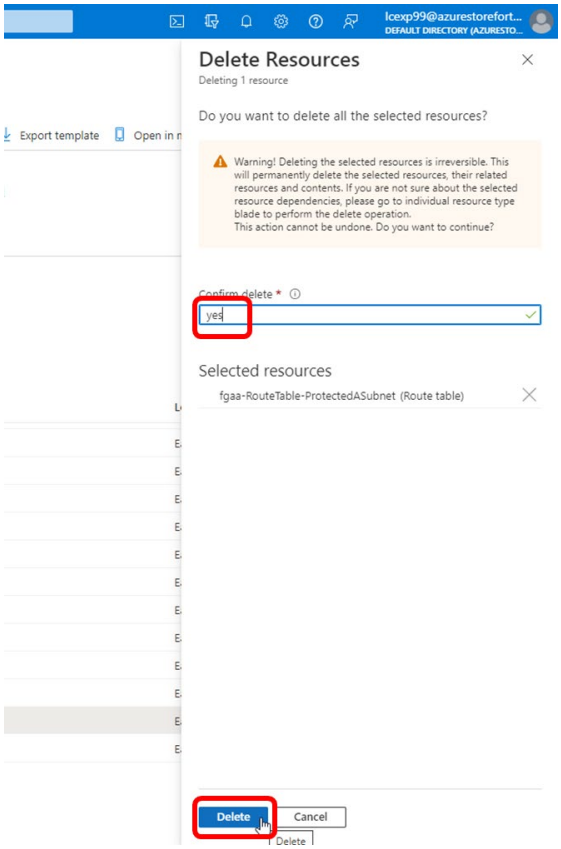
29. Go back to on the lcexp***<your student number>***-fgtaa resource group and then scroll all the way down and select the route table named **fgaa-RouteTable-ProtectedASubnet**



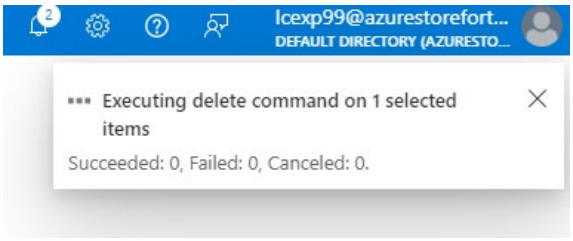
30. Click on **Delete** on the top menu



31. Type in **yes** to confirm and then click **Delete**



32. A notification will appear



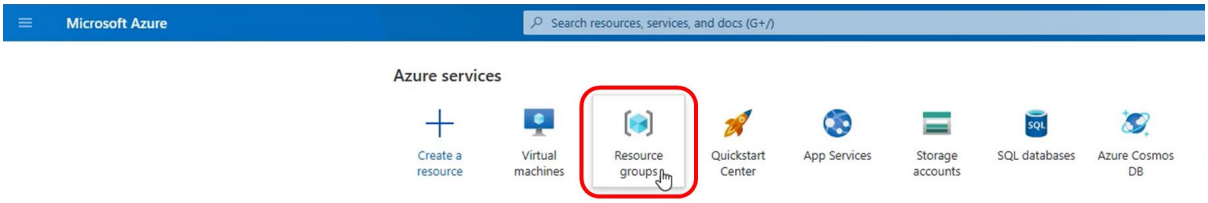
33. Upon completion, the deployment is now complete

Task 10 - Configure VNET Peering FGAA

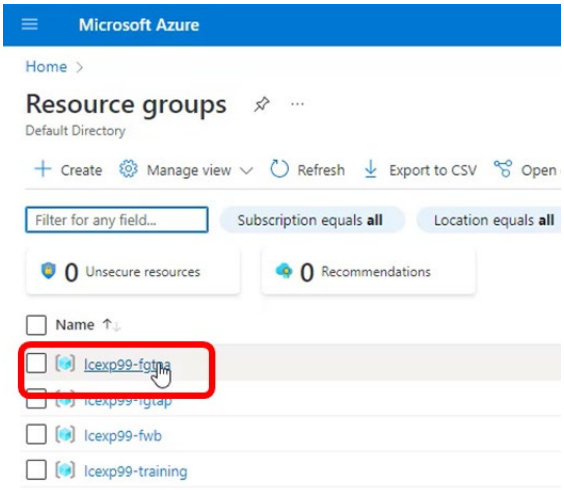
The next step is the configuration of the virtual network (VNET) peering between the Workload VNET and the FortiGate FGAA VNET to allow for intercommunications between the two VNETs.

Configuration steps

34. From the main Azure Portal, click on **Resource groups**

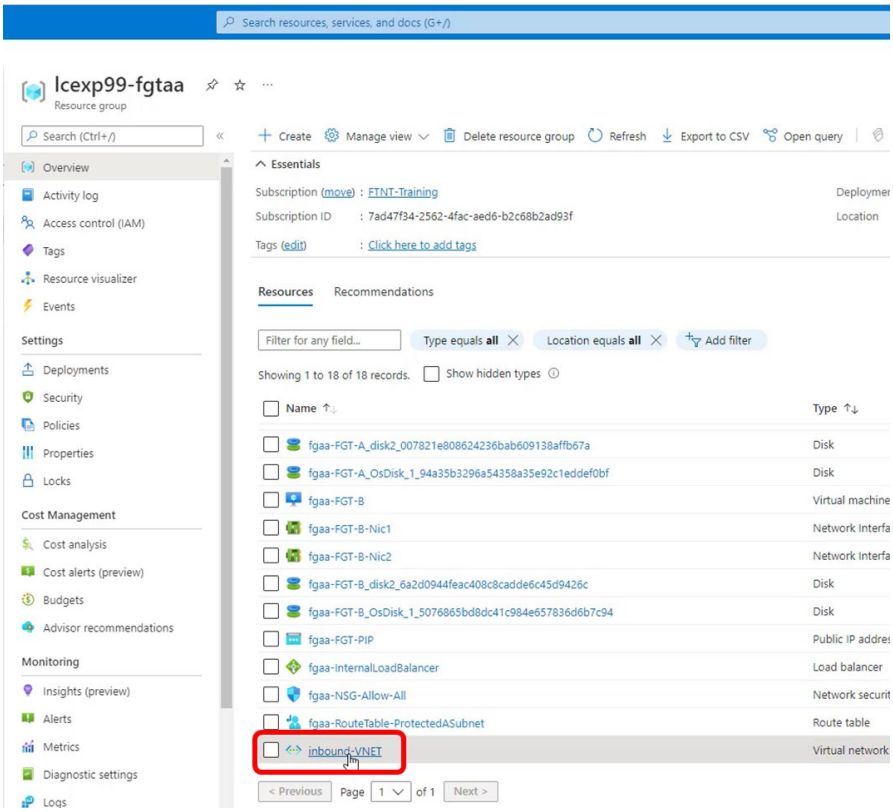


35. Click on the lcexp***<your student number>***-fgtaa resource group name itself to open a new pane on the right.

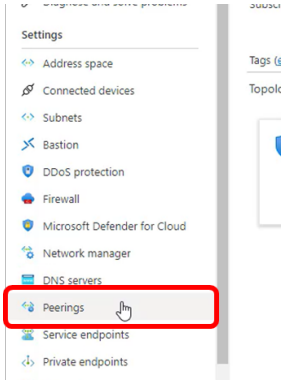


Task 10 - Configure VNET Peering FGAA

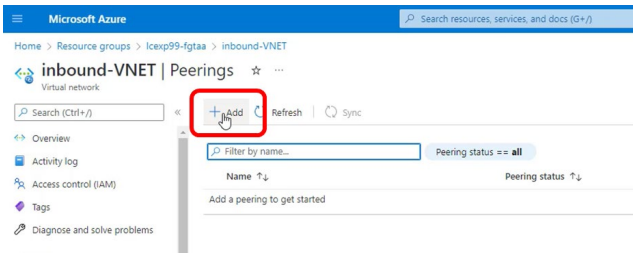
36. In the resource group pane, scroll down and click on the name inbound-VNET



37. In the Virtual network left menu, scroll down to click **Peerings**

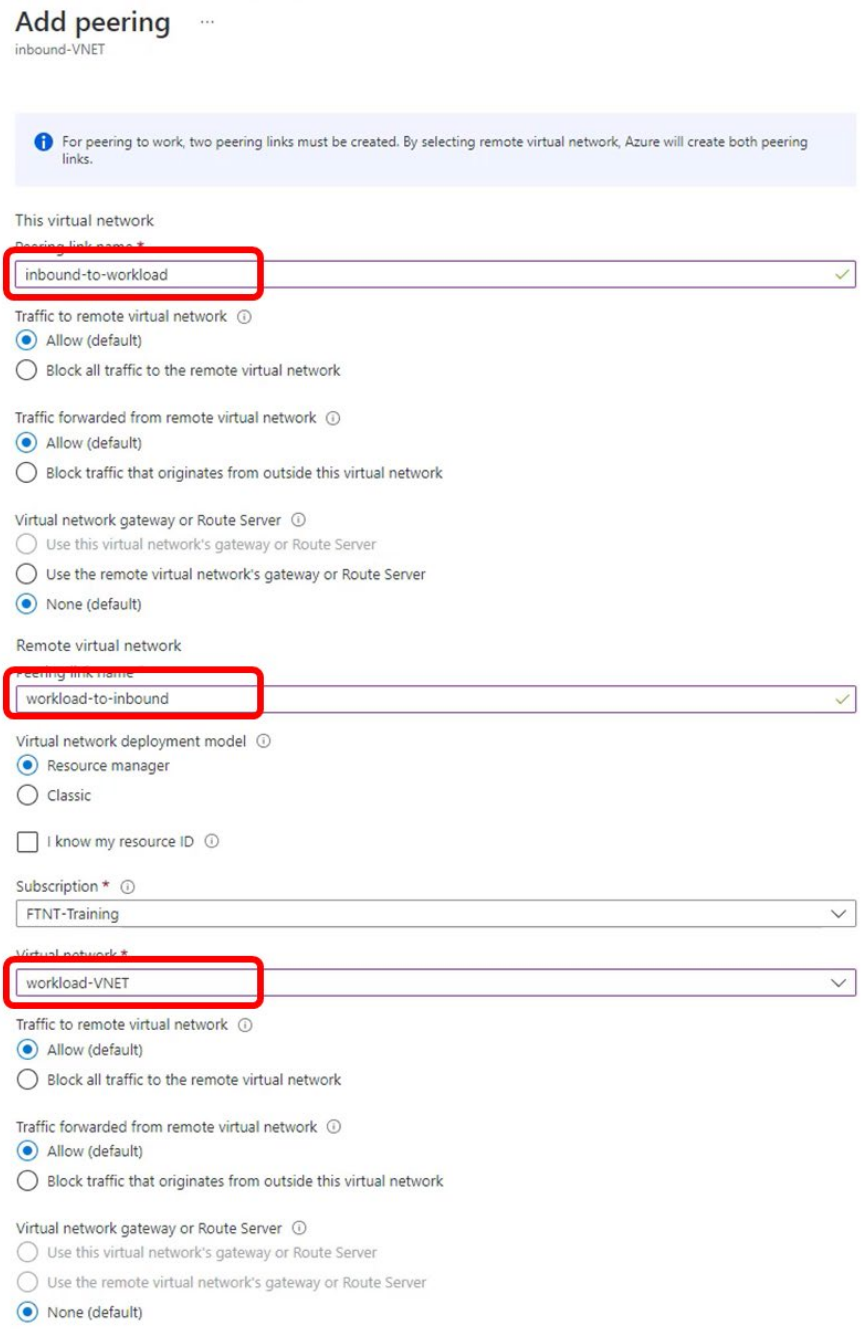


38. In the right pane, click **+ Add**



39. Use the following information from the table to fill out the page as showed in the image below

This virtual network **Peering link name**	inbound-to-workload
Remote virtual network **Peering link name**	workload-inbound
Remote virtual network **Virtual network**	workload-VNET

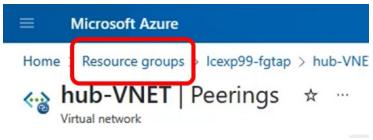


40. At the bottom of the pane, click **Add**

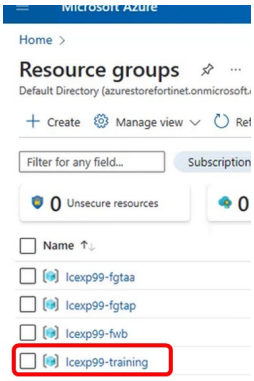
Task 10 - Configure VNET Peering FGAA

41. Confirm the peering status shows **Connected** as per the screenshot below, you might have to wait a few minutes occasionally clicking the **Refresh** button:

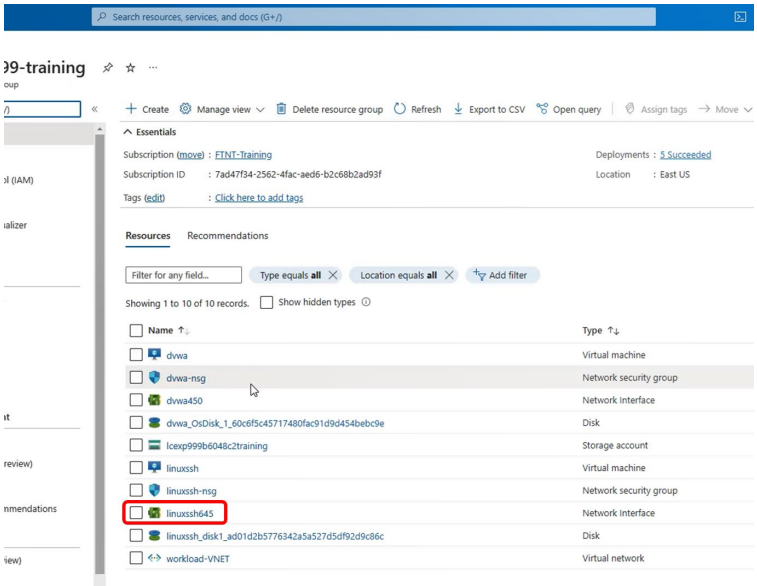
42. Next navigate away from this pane by click on Resource groups in the upper left menu



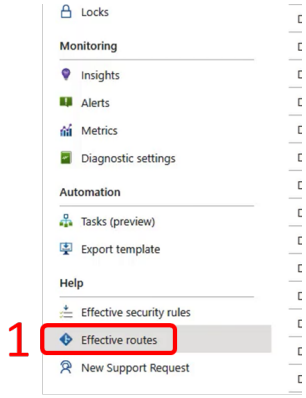
43. Click on the lcexp***<your student number>***-training resource group



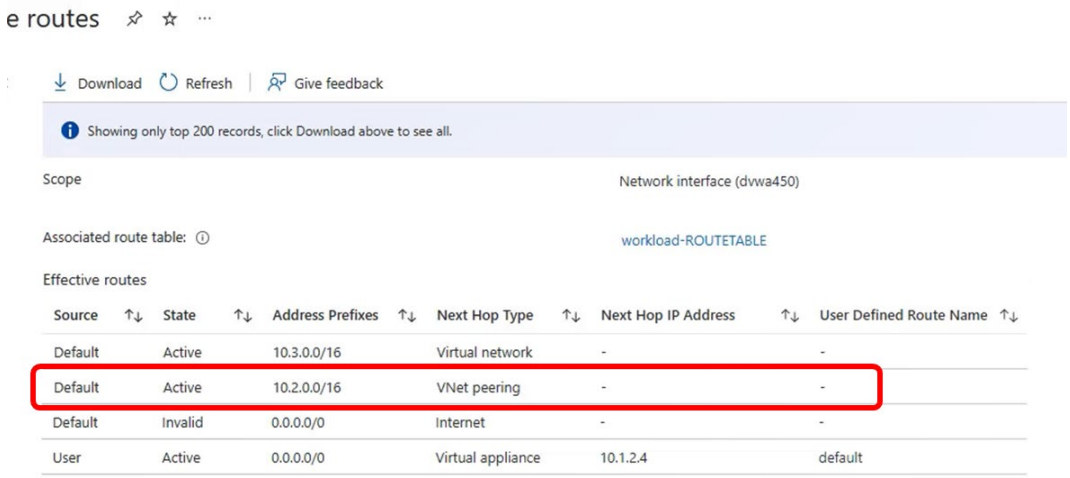
44. In the right pane, click on the name of the linuxssh Network interface



45. In the left Network interface menu, scroll all the way down and click on **Effective routes**



46. Confirm the routing entry for the VNET peering is showing as per below. This view is very useful for troubleshooting Azure routing issues.



Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address	User Defined Route Name
Default	Active	10.3.0.0/16	Virtual network	-	-
Default	Active	10.2.0.0/16	VNet peering	-	-
Default	Invalid	0.0.0.0/0	Internet	-	-
User	Active	0.0.0.0/0	Virtual appliance	10.1.2.4	default

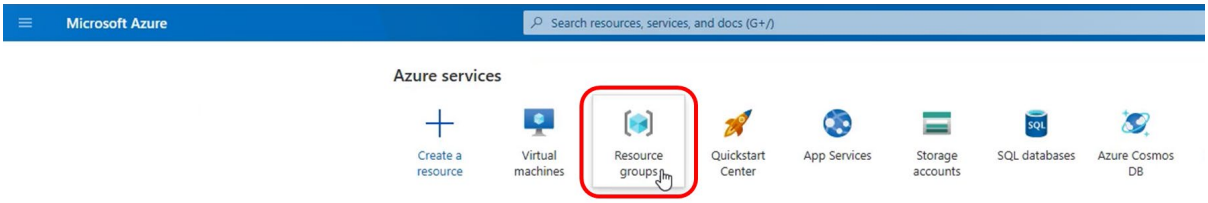
47. The VNET peering is complete

Task 11 - Configure Azure LB for inbound SSH

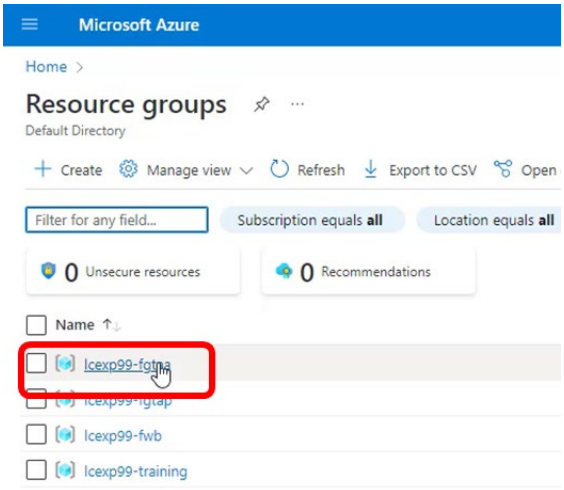
The next step is the creation of the appropriate Azure Load Balancer rules to permit inbound SSH traffic destined to the linuxssh VM.

Configuration steps

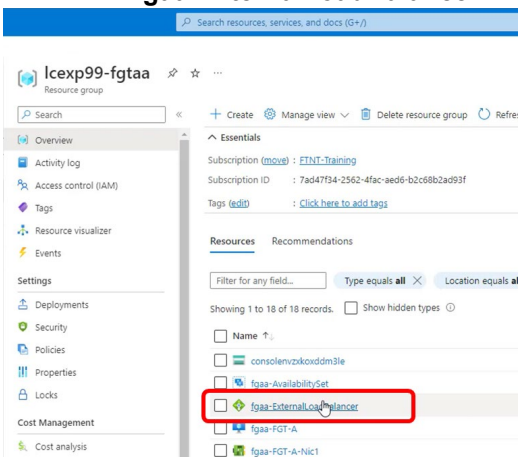
1. From the main Azure Portal, click on **Resource groups**



2. Click on the lcexp***<your student number>***-fgtaa resource group name itself to open a new pane on the right.

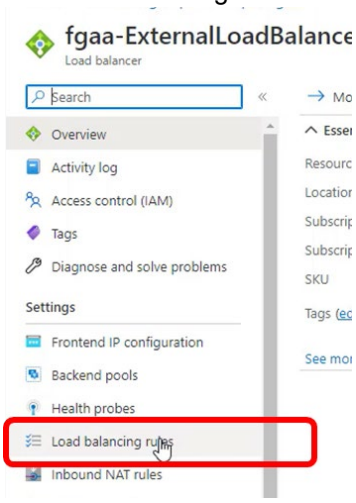


3. Click on the Load Balancer name of **fgaa-ExternalLoadBalancer** in the left pane

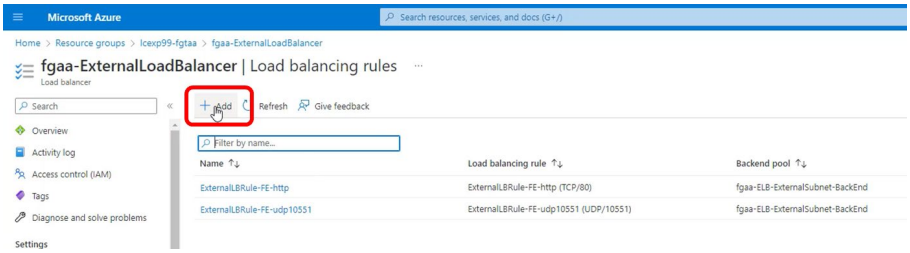


Task 11 - Configure Azure LB for inbound SSH

4. In left Load balancer menu, click on Load balancing rules



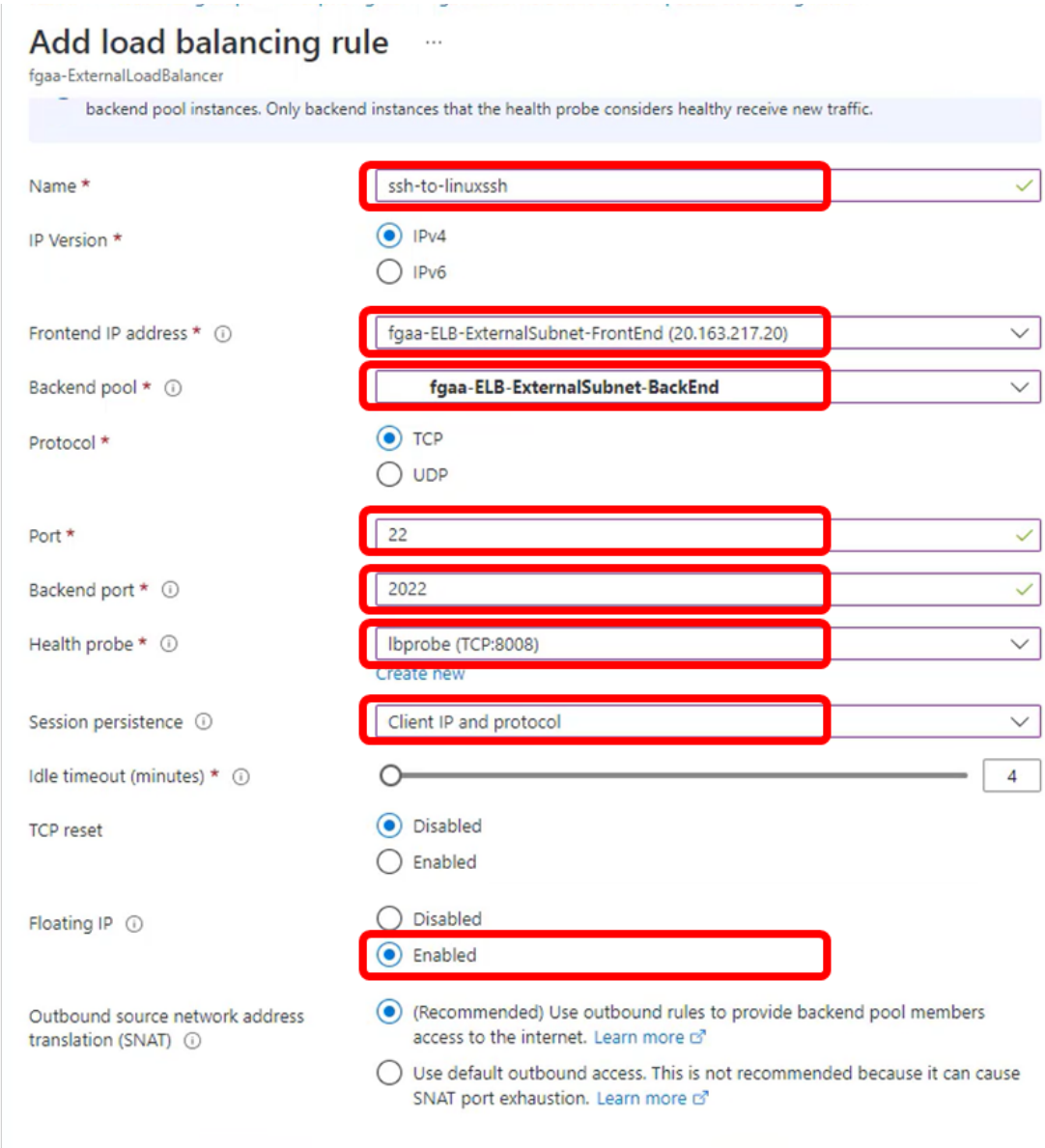
5. Click on **+ add** on the right pane to create a new load balancing rule



Task 11 - Configure Azure LB for inbound SSH

6. Use the following information from the table to fill out the page as showed in the image below

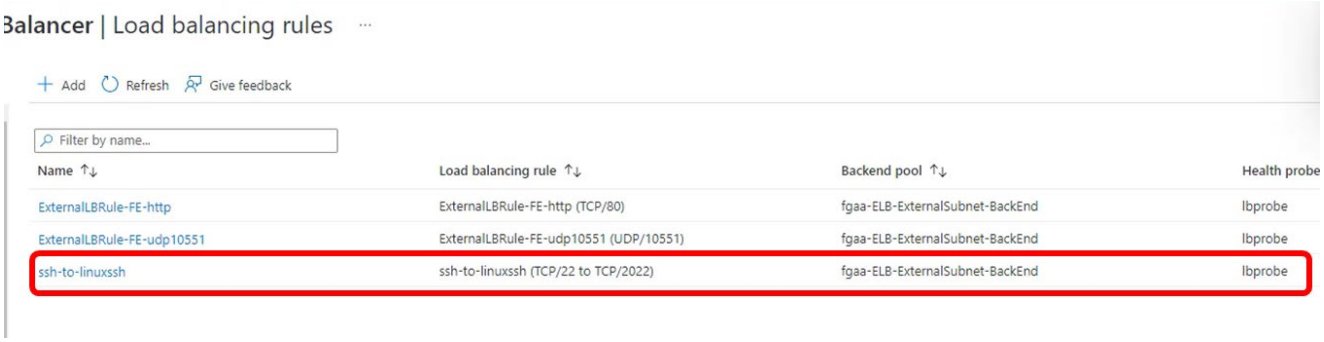
Name	ssh-to-linuxssh
Frontend IP address	fgaa-ELB-ExternalSubnet-FrontEnd
Backend pool	fgaa-ELB-ExternalSubnet-BackEnd
Port	22
Backend port	2022
Health probe	lbprobe (TCP:8008)
Session persistence	Client IP and protocol
Floating IP	Enable



7. Click on **Add** at the bottom of the pane

Task 11 - Configure Azure LB for inbound SSH

8. Confirm the load balancing rule added with the screen below



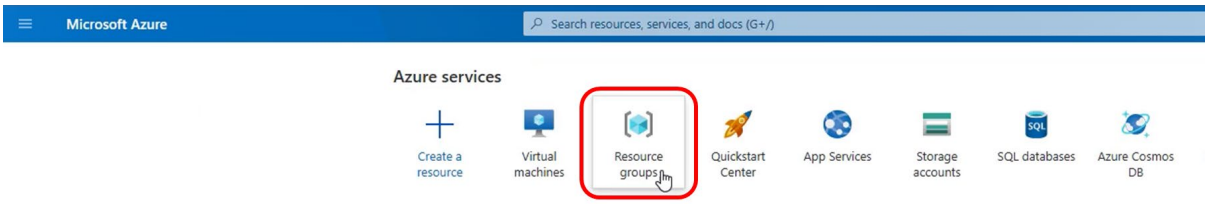
9. You have completed this task

Task 12 - Configure FortiGate Active-Active config synchronization

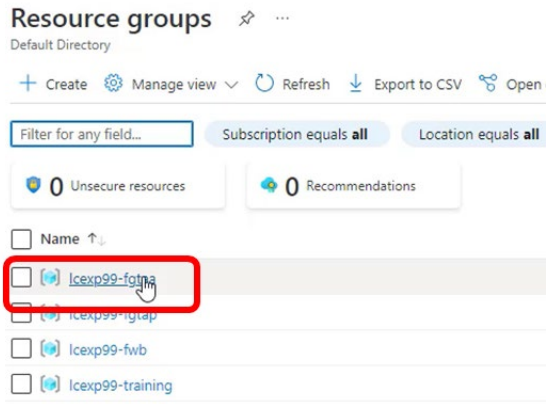
The next step is the configuration of the configuration synchronization of the FortiGate firewalls deployed in Active-Active mode located in the Inbound VNET by leveraging a FortiOS feature typically used in autoscaling groups or VM scale sets. The feature will work even though this deployment does not use autoscaling groups / VM scale sets.

Configuration steps

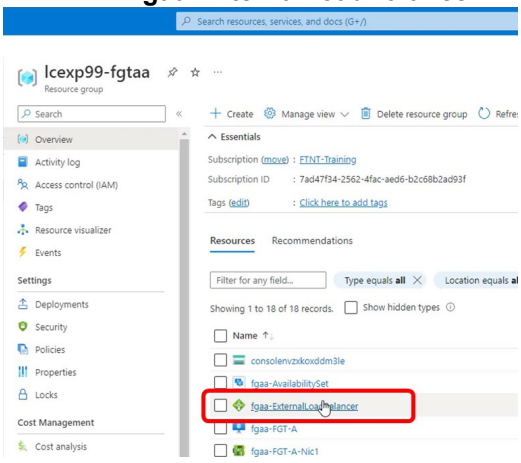
1. From the main Azure Portal, click on **Resource groups**



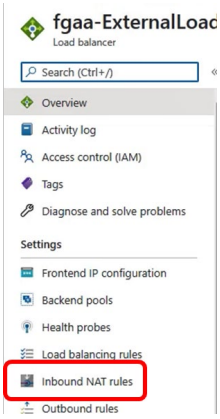
2. Click on the lcexp***<your student number>***-fgtaa resource group name itself to open a new pane on the right.



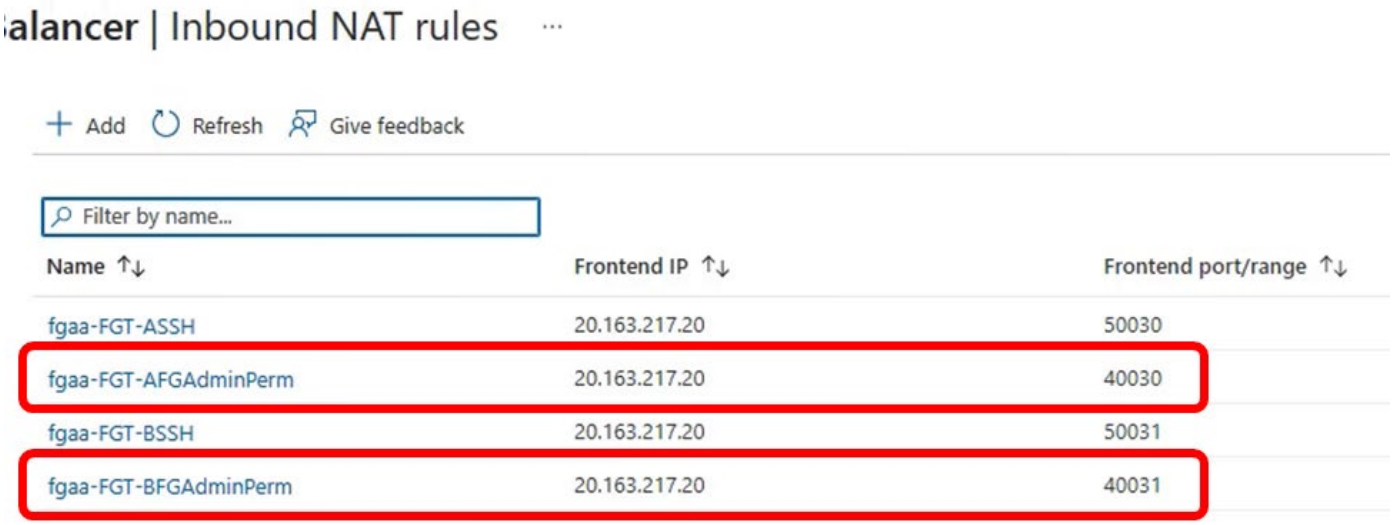
3. Click on the Load Balancer name of **fgaa-ExternalLoadBalancer** in the left pane



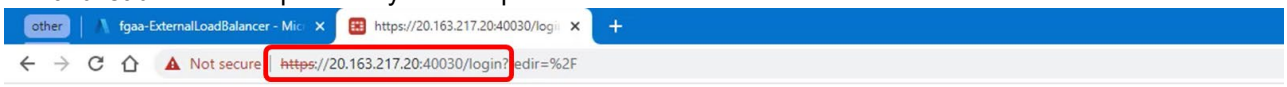
4. In left Load balancer menu, click on inbound NAT rules

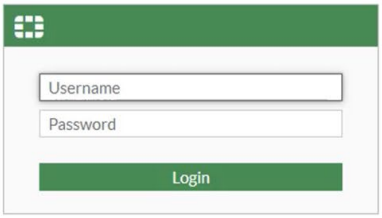


5. In the right pane, make note of the Frontend IP and Frontend port for both FortiGate fgaa-FGT-A and FortiGate fgaa-FGT-B for the HTTPS admin access

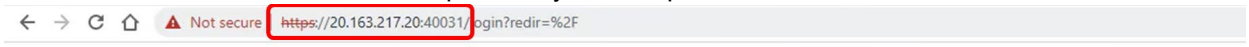


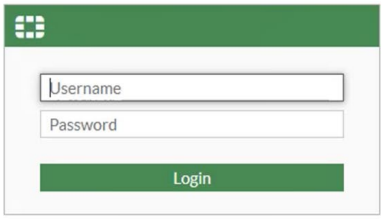
6. Open a new web browser tab to https of the FrontEnd IP address along with the port for FortiGate fgaa-FGT-A, https://20.163.217.20:40030 in this example, and log in using the credentials of **azureadm** and the previously chosen password.





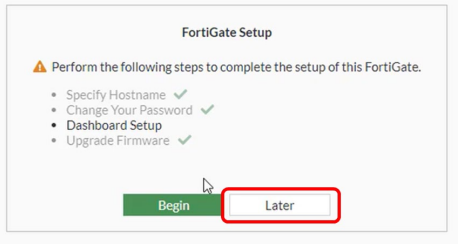
7. Open another web browser tab to https of the FrontEnd IP address along with the port for FortiGate fgaa-FGT-B, https://20.163.217.20:40031 in this example, and log in using the credentials of **azureadm** and the previously chosen password.



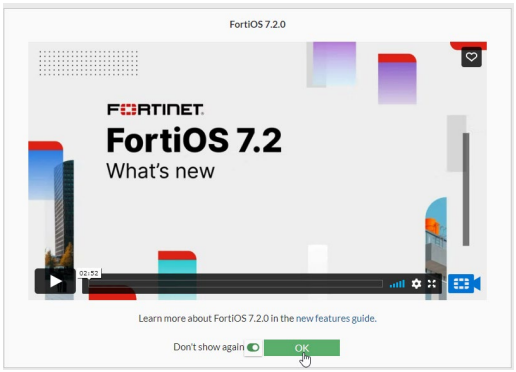


Task 12 - Configure FortiGate Active-Active config synchronization

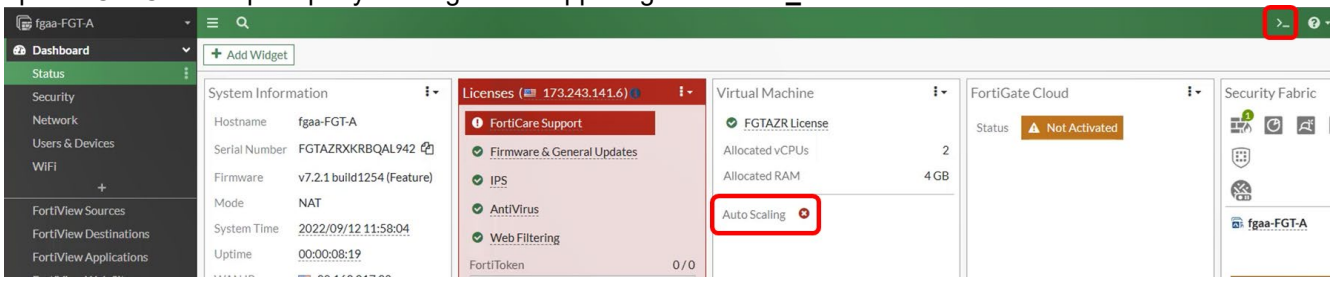
8. On both FortiGate web browser tabs dismiss the FortiGate Setup prompt by clicking **Later**



9. Dismiss the subsequent prompt as well by clicking **OK**

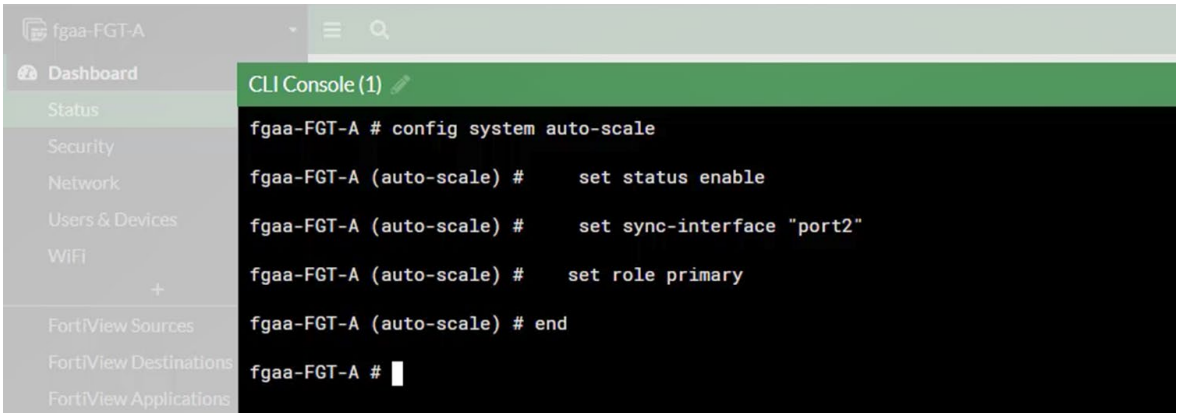


On the Dashboard Status of FortiGate fgaa-FGT-A, confirm Auto Scaling is not configured and then open a CLI Console prompt by clicking on the upper right icon of **>_**

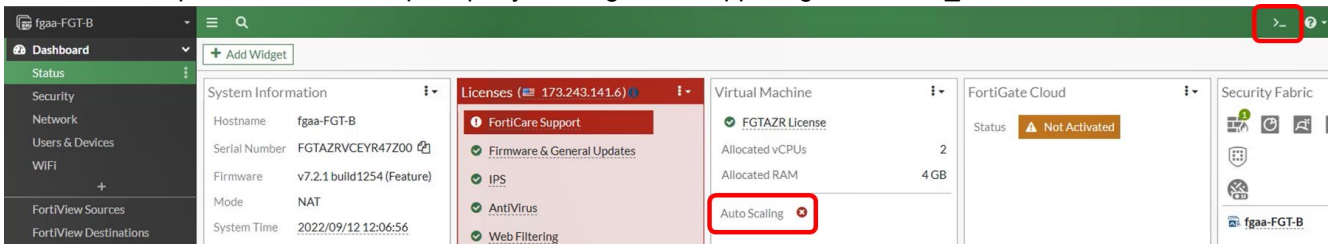


10. In the CLI Console enter the following commands:

```
config system auto-scale
   set status enable
   set sync-interface "port2"
   set role primary
end
```

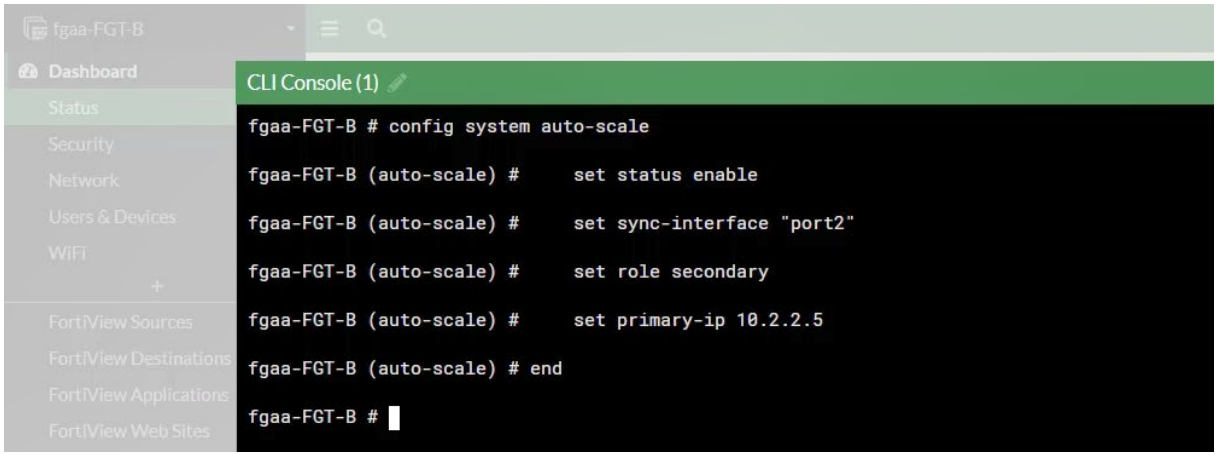


11. On the Dashboard Status of FortiGate fgaa-FGT-B, confirm Auto Scaling is also not configured and then open a CLI Console prompt by clicking on the upper right icon of **>_**

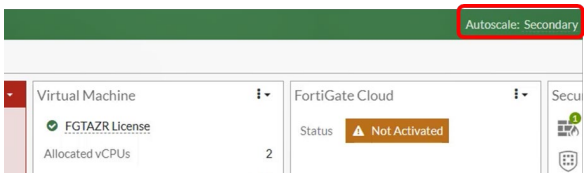


12. In the CLI Console enter the following commands:

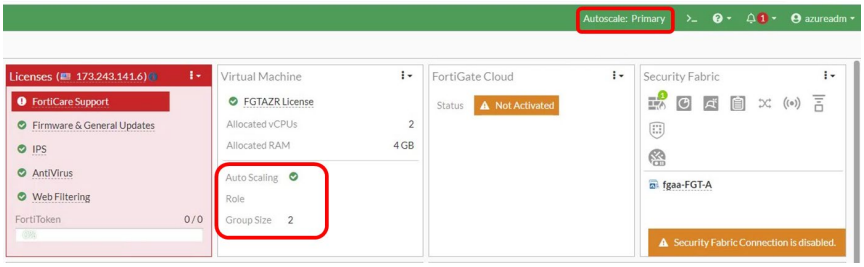
```
config system auto-scale
   set status enable
   set sync-interface "port2"
   set role secondary
   set primary-ip 10.2.2.5
end
```



13. Exit out of the CLI Console then confirm the secondary mode of Autoscale configuration of FortiGate fgaa-FGT-B on the upper right corner of the Dashboard Status. This might require a wait of approximately 5 minutes



14. On the web browser tab of FortiGate fgaa-FGT-A also exit out of the CLI console and confirm the Autoscale configuration



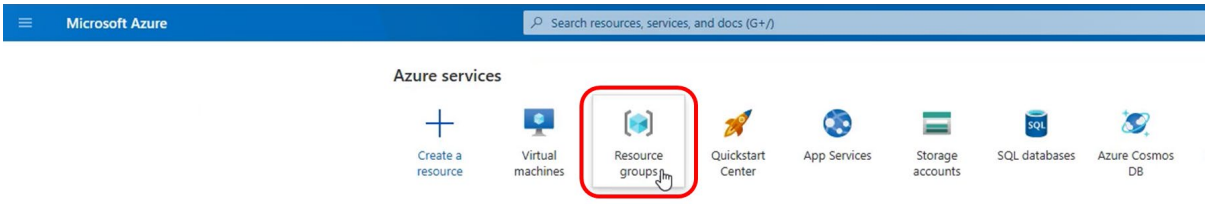
15. This task is now complete

Task 13 - Configure FortiGate Active-Active Routing and Security Policies

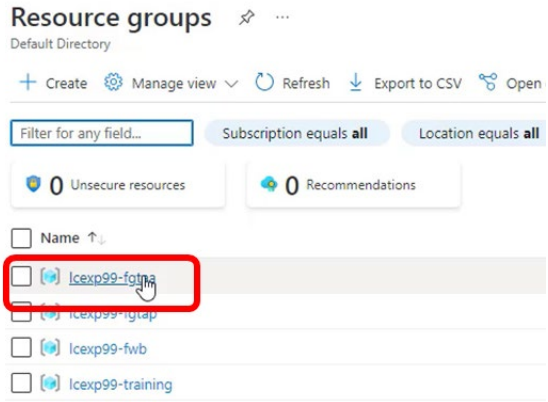
The next step is the configuration of the configuration the static routes and security policies of the FortiGate firewalls deployed in Active-Active mode located in the Inbound VNET. This will allow inbound traffic to the DMZ protected Subnet located in the workload VNET

Configuration steps

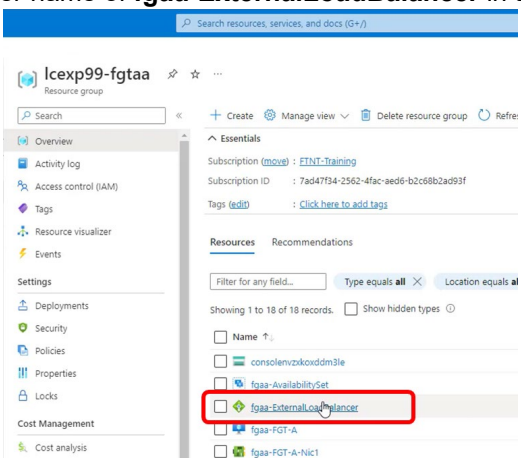
1. From the main Azure Portal, click on **Resource groups**



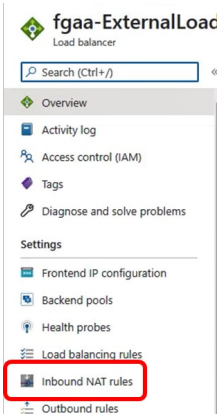
2. Click on the lcexp***<your student number>***-fgtaa resource group name itself to open a new pane on the right.



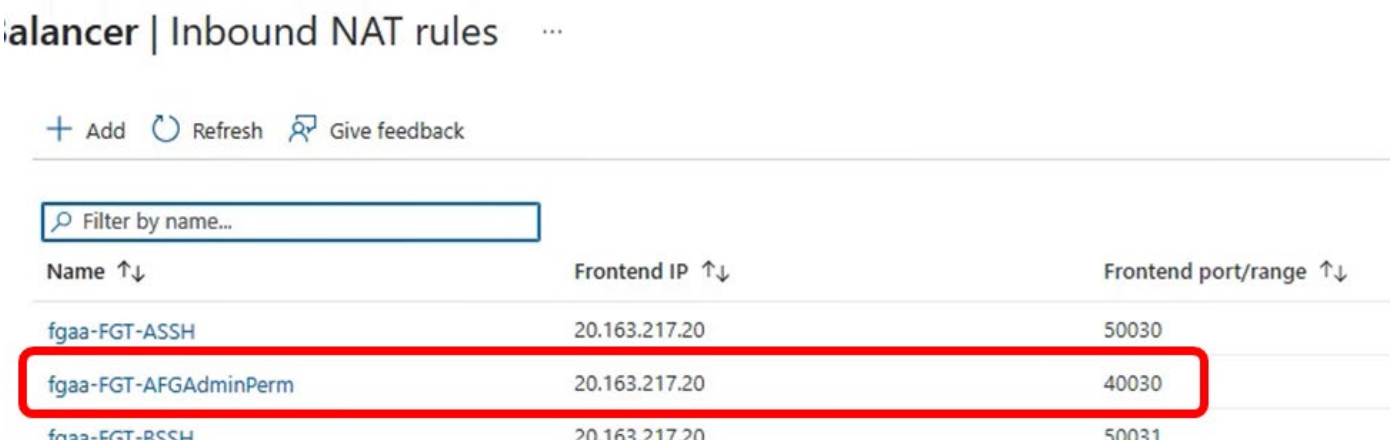
3. Click on the Load Balancer name of **fgaa-ExternalLoadBalancer** in the left pane



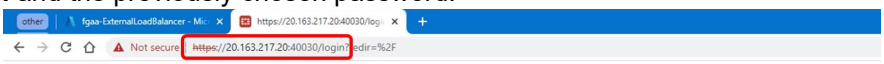
4. In left Load balancer menu, click on inbound NAT rules

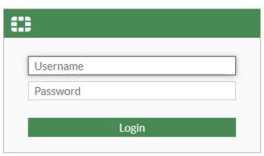


5. In the right pane, make note of the Frontend IP and Frontend port for FortiGate fgaa-FGT-A for the HTTPS admin access

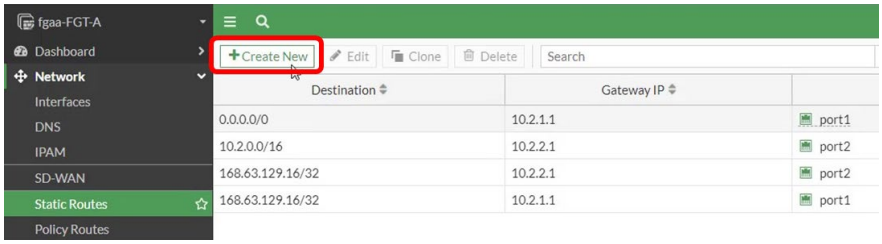


6. Open a new web browser tab to https of the FrontEnd IP address along with the port for FortiGate fgaa-FGT-A, https://20.163.217.20:40030 in this example, and log in using the credentials of **azureadm** and the previously chosen password.



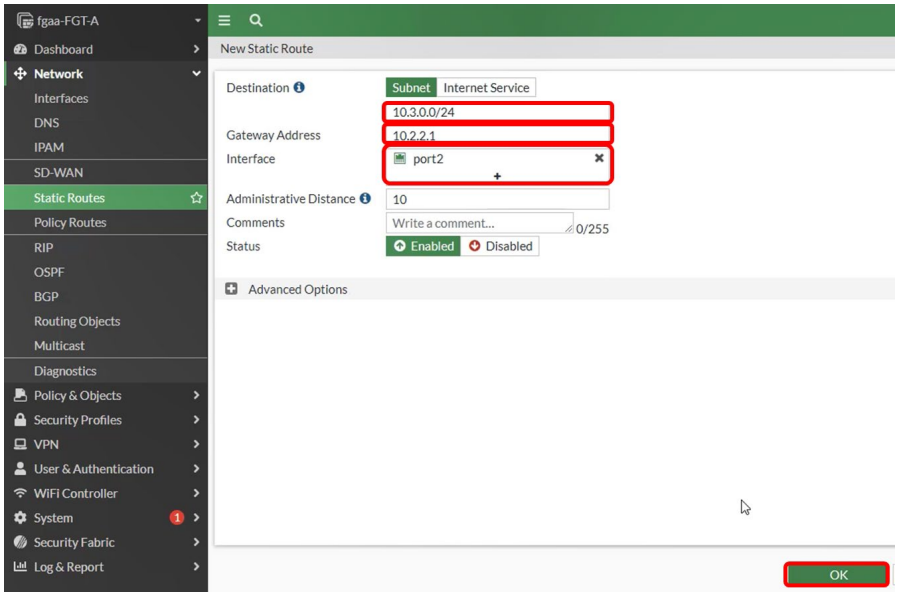


7. In the left FortiGate menu of fgaa-FGT-A click on **Network**, then **Static Routes**, then **+ Create New**

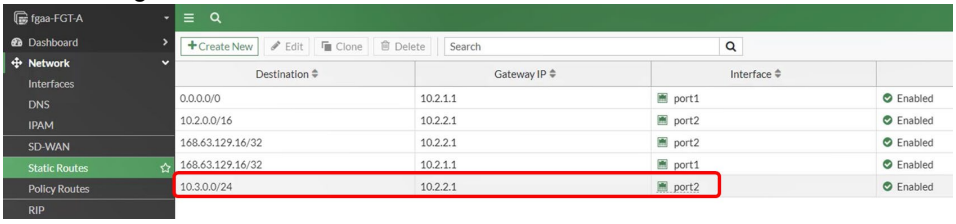


8. Use the following information from the tables to fill out the New Static Route as showed in the image below then click **OK**

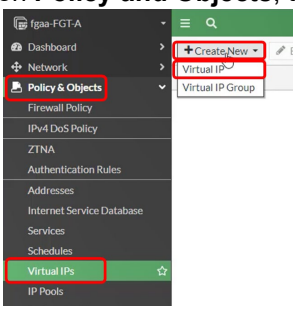
Destination	Subnet 10.3.0.0/24
Gateway Address	10.2.2.1
Interface	port2



9. Confirm the routing entries with the screen below

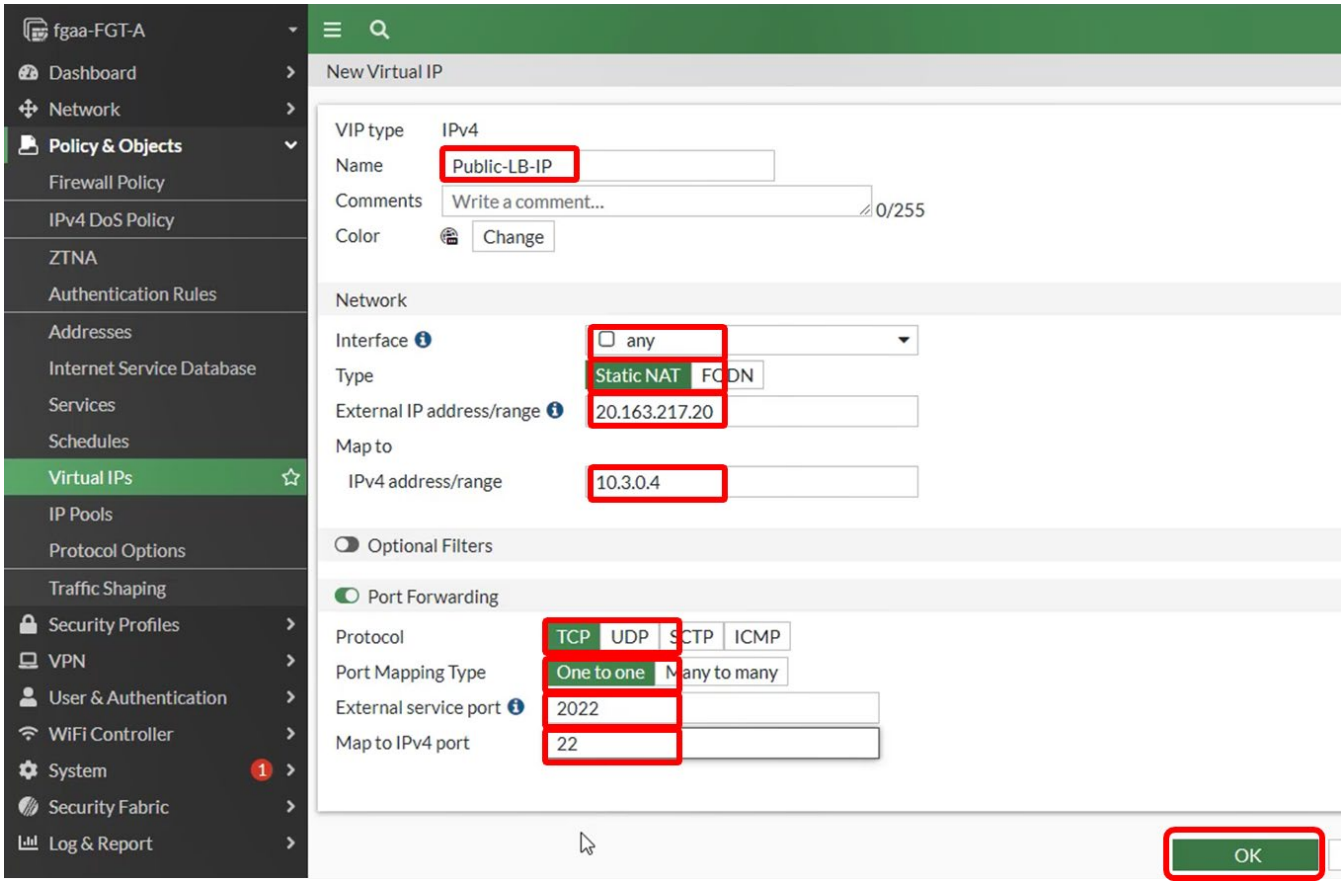


10. In the same FortiGate menu, click on **Policy and Objects**, then **Virtual IPs**, then **+ Create New**

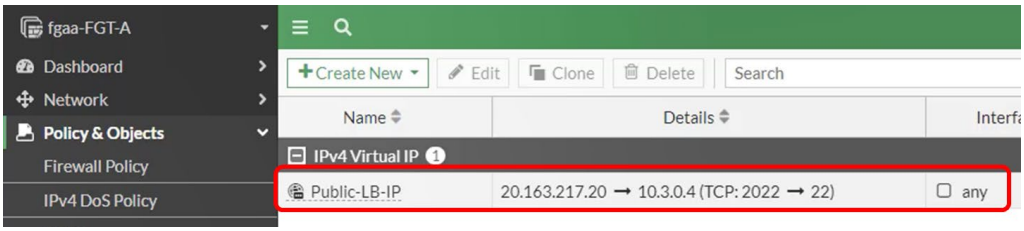


11. Use the following information from the table to fill out the New Virtual IP as showed in the image below then click **OK**

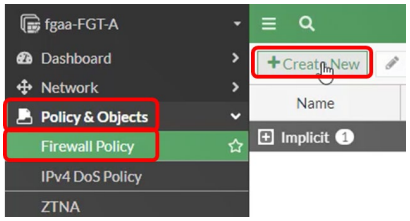
Name	Public-LB-IP
Interface	Any
Type	Static NAT
External IP address/range	FGAA LB Frontend IP (20.163.217.20 in this example from step 5)
Map to IPv4 address/range	10.3.0.4
Port Forwarding	TCP
Port Mapping Type	On to one
External service port	2022
Map to IPv4	22



12. Confirm the Virtual IP created with the screen below:

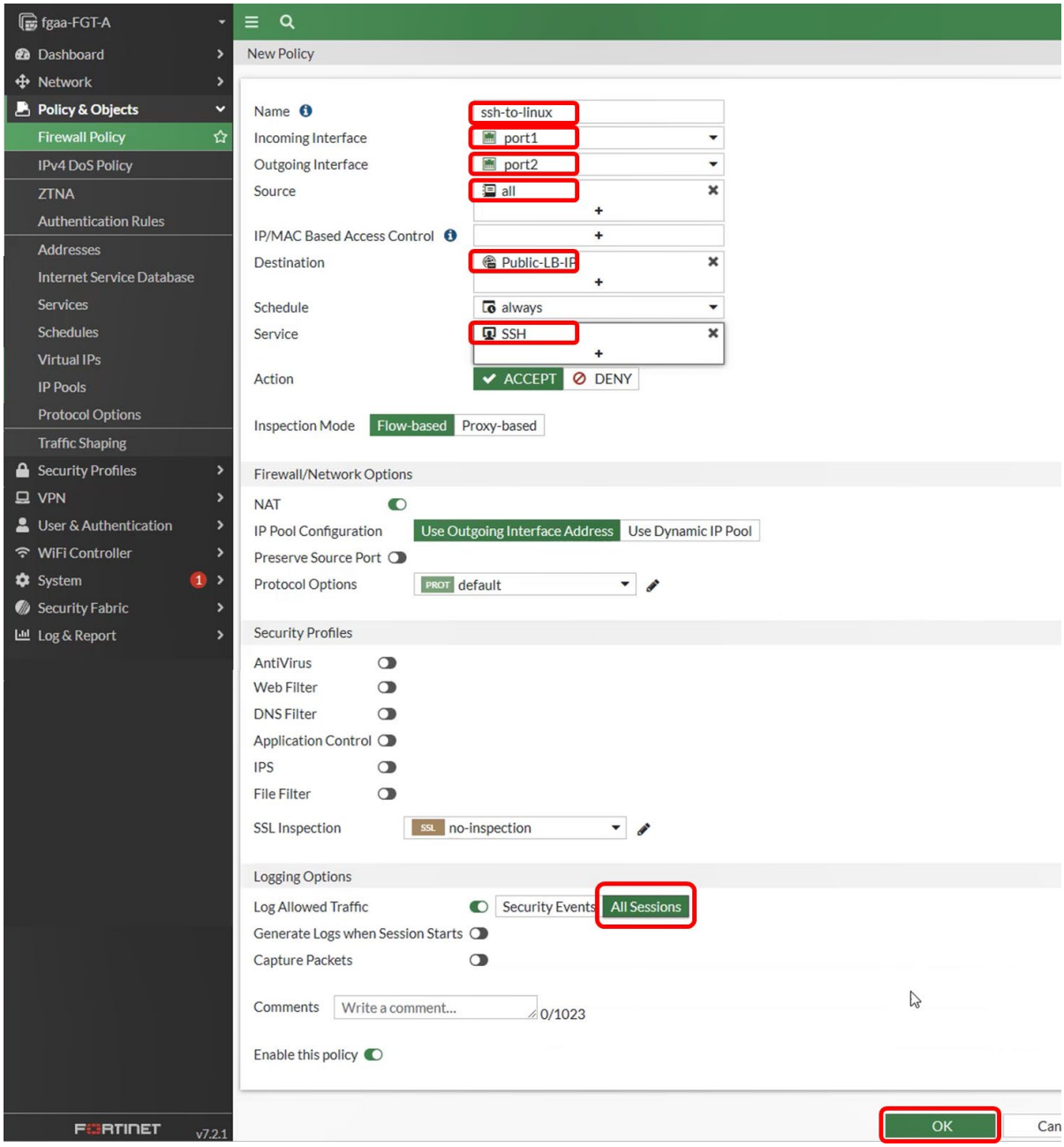


13. In the same FortiGate menu, click on **Policy and Objects**, then **Firewall Policy**, then **+ Create New**

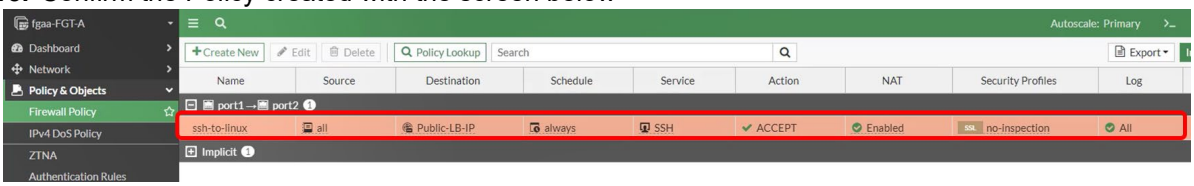


14. Use the following information from the table to fill out the Policy as showed in the image below then click **OK**

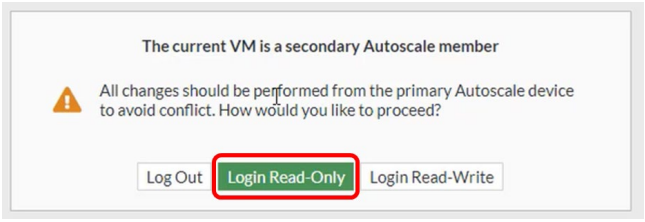
Name	ssh-to-linux
Incoming Interface	port1
Outgoing Interface	port2
Source	all
Destination	Public-LB-IP *(Virtual IP)*
Service	SSH
Log Allowed Traffic	All Sessions



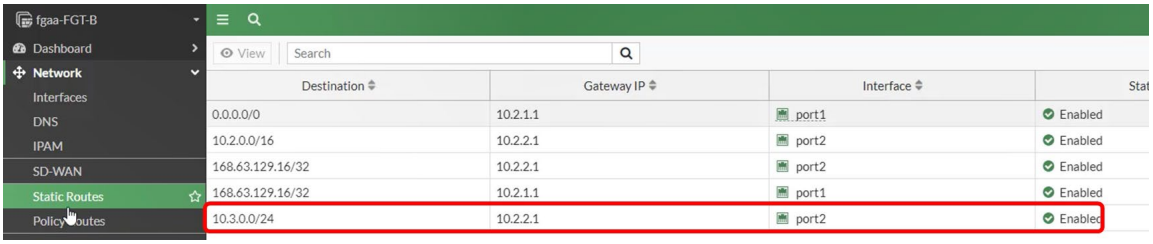
15. Confirm the Policy created with the screen below



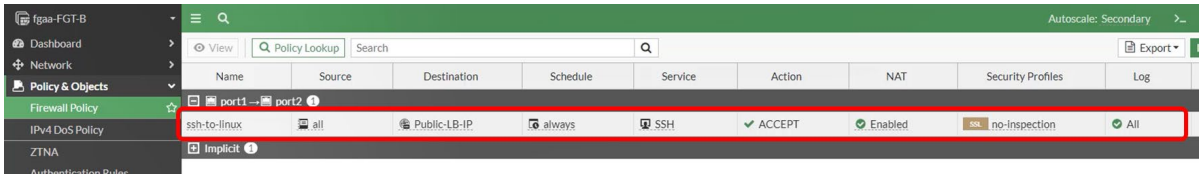
16. Open another web browser tab to https of the FrontEnd IP address along with the port for FortiGate fgaa-FGT-B, https://20.163.217.20:40031 in this example, and log in using the credentials of **azureadm** and the previously chosen password.
17. Click on **Log in Read-Only**



18. In the left FortiGate menu of fgaa-FGT-B click on **Network**, then **Static Routes**. Confirm the static route created on FortiGate fgaa-FGT-A is synchronized over to FortiGate fgaa-FGT-B



19. In the same FortiGate menu, click on **Policy and Objects**, then **Firewall Policy**. Confirm the Policy created on FortiGate fgaa-FGT-A synchronized over to FortiGate fgaa-FGT-B



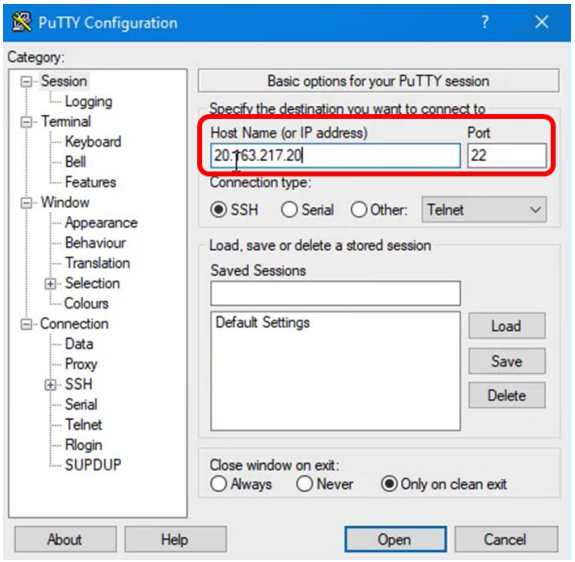
20. You have completed this task

Task 14 - Test inbound SSH to linuxssh

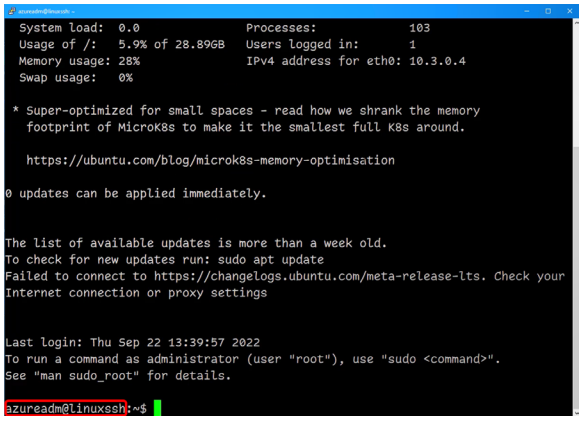
The next step is to test the entire configuration by confirming SSH access into linuxssh VM is permitted.

Task steps

1. Open an SSH connection from you own laptop to the FrontEnd IP address (20.163.217.20 in this example). The screenshot below show the popular PuTTY software, but any suitable SSH client can be used.



2. Confirm you can login as per below



3. This task is now complete