

Securing Hybrid Cloud in Azure

Student Lab Guide

version 1

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>

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Table of Contents

LAB ACCESS USING THE AZURE PORTAL.....	5
Lab Environment	5
Azure Portal Lab Access.....	5
LAB 1— SECURING HYBRID CLOUD IN AZURE	11
Objectives.....	11
Lab Diagrams	12

TASK 1 - CREATING A VIRTUAL NETWORK IN AZURE	13
TASK 2 - DEPLOY LINUXSSH VIRTUAL MACHINE	22
TASK 3 - DEPLOY DVWA VIRTUAL MACHINE.	26
TASK 4 - DEPLOY FORTIGATE ACTIVE-PASSIVE	36
TASK 5 - CONFIGURE VNET PEERING FGAP.....	50
TASK 6 - CONFIGURE WORKLOAD SUBNET UDR.....	55
TASK 7 - CONFIGURE FORTIGATE ACTIVE PASSIVE	67
TASK 8 – CONFIRM VM OUTBOUND ACCESS.....	74
TASK 9 - DEPLOY FORTIGATE ACTIVE-ACTIVE	79
TASK 10 - CONFIGURE VNET PEERING FGAA	92
TASK 11 - CONFIGURE AZURE LB FOR INBOUND SSH	97
TASK 12 - CONFIGURE FORTIGATE ACTIVE-ACTIVE CONFIG SYNCHRONIZATION.....	101
TASK 13 - CONFIGURE FORTIGATE ACTIVE-ACTIVE ROUTING AND SECURITY POLICIES	106
TASK 14 - TEST INBOUND SSH TO LINUXSSH.....	113

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

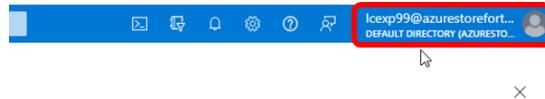
1. Open a browser, and then access the following URL:

<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

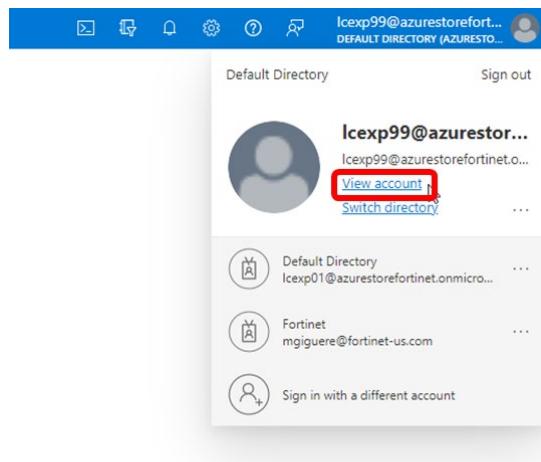
Username:	<user@domain received by email>
Password:	<password provided by email>

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



▶ Lab Access Using the Azure Portal

6. Click Change Password

The screenshot shows the 'My Account' overview page. On the left, there's a sidebar with links like Overview, Security info, Devices, Password, Organizations, Settings & Privacy, and My sign-ins. The main area has a profile card for 'Icexp99' with an email address 'Icexp99@azurerefortinet.onmicrosoft.com'. To the right are three cards: 'Security info' (with a link to 'UPDATE INFO'), 'Password' (with a link to 'CHANGE PASSWORD' which is highlighted with a red box), and 'Perso...' (partially visible). A mouse cursor is hovering over the 'CHANGE PASSWORD' button.

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

The screenshot shows the 'Change password' form. At the top, it says 'Change password'. Below that, a note states: 'Strong password required. Enter 8-256 characters. Do not include common words or names. Combine uppercase letters, lowercase letters, numbers, and symbols.' The 'User ID' field is pre-filled with 'Icexp99@azurerefortinet.onmicrosoft.com'. The 'Old password' field is filled with '*****'. The 'Create new password' field is filled with 'strong' (the first few characters are redacted). The 'Confirm new password' field is filled with '*****'. At the bottom, there are two buttons: 'Submit' (highlighted with a red box) and 'Cancel'. A cursor is pointing at the 'Submit' button.

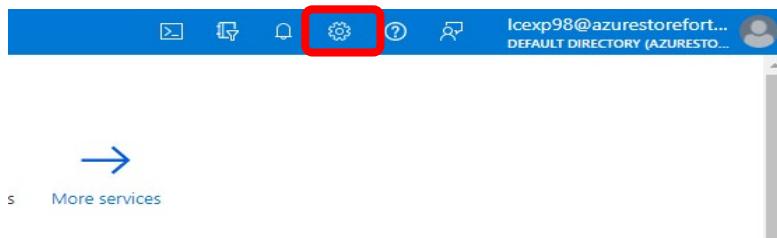
► Lab Access Using the Azure Portal

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

The screenshot shows the Microsoft Azure Profile page. At the top right, there is a user icon with the name 'lcexp99' and a 'DEFAULT DIRECTORY' label. Below the profile picture, the name 'lcexp99' is displayed. To the right of the name, there are links for 'Manage account', 'Change password', 'Set up self service password reset', 'Review terms of use', and 'Sign out everywhere'. The 'Change password' link is underlined, indicating it was recently used.

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 Then click on **Languaje + region**

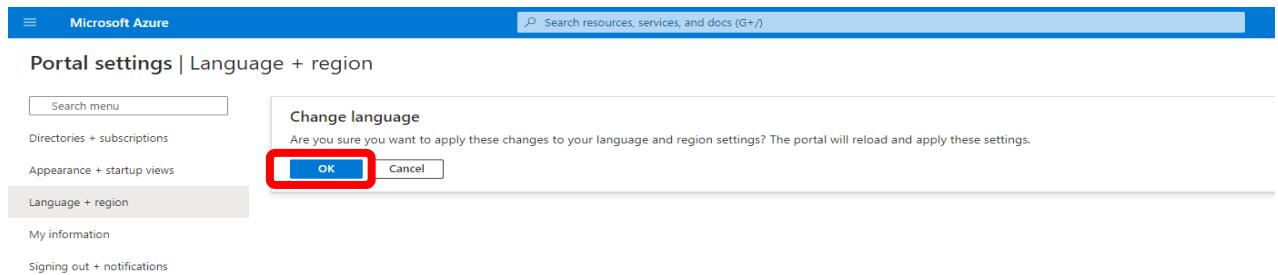
The screenshot shows the 'Portal settings | Directories + subscriptions' page. On the left, there is a sidebar with options like 'Directories + subscriptions', 'Appearance + startup views', and 'Language + region', which is highlighted with a red box. The main content area shows basic portal settings information and a search bar.

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.

The screenshot shows the 'Portal settings | Language + region' page. On the left, there is a sidebar with 'Language + region' highlighted. The main content area displays a message: 'Choose your language and the regional format that will influence how your date/time and currency will appear.' Below this, there are two dropdown menus: 'Language' set to 'Español' and 'Regional format' set to 'Español (México)', both of which are highlighted with a red box.

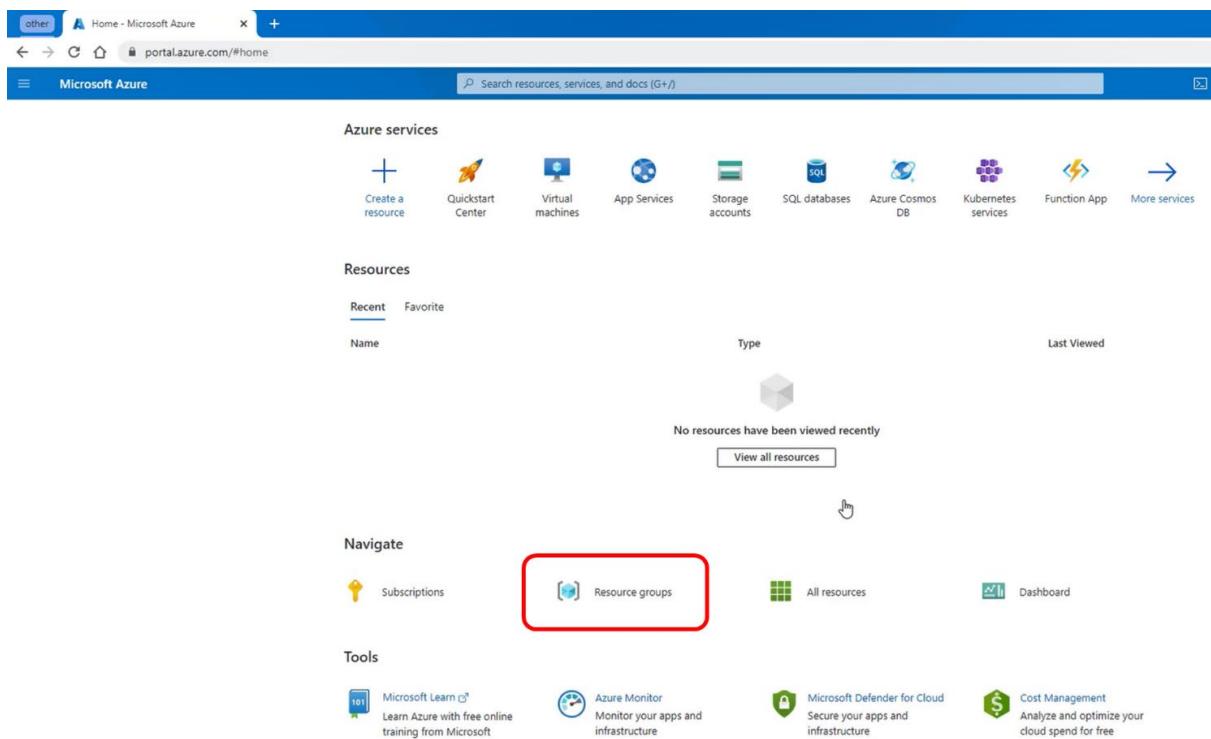
▶ Lab Access Using the Azure Portal

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.



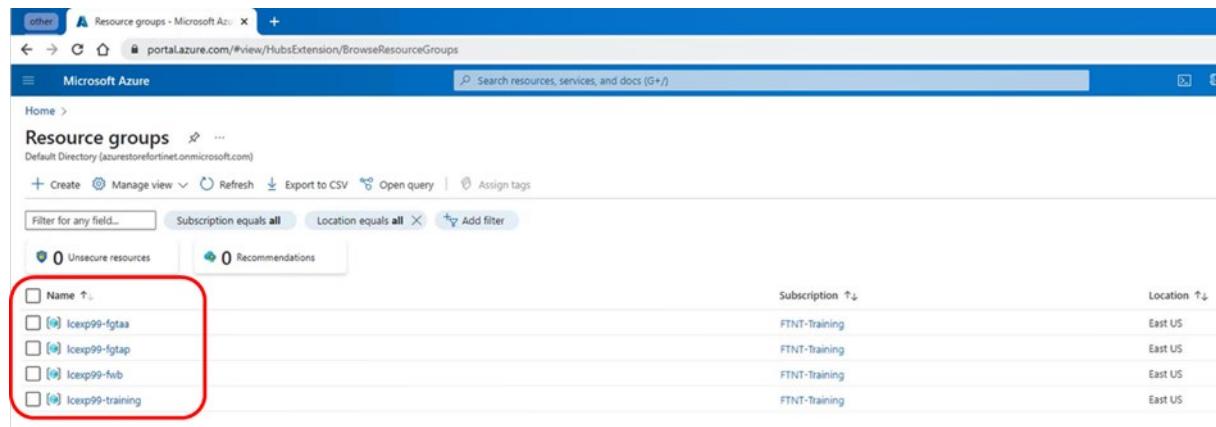
10. Of note, in the Azure account, which is a new Azure subscription, only four resource groups will be already there pre-created. All four will be used in this lab. No new ones can be created as resource groups are used as the basis of the individualization of the security in the lab environment

11. Click on Resource Groups in the main page.



▶ Lab Access Using the Azure Portal

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



The screenshot shows the Microsoft Azure Resource groups page. At the top, there's a navigation bar with links for Home, Resource groups, and other options. Below the navigation is a search bar labeled "Search resources, services, and docs (G+)".

The main area is titled "Resource groups" and shows a list of four resource groups:

Name	Subscription	Location
Icep99-fgtaa	FTNT-Training	East US
Icep99-fgtap	FTNT-Training	East US
Icep99-fwb	FTNT-Training	East US
Icep99-training	FTNT-Training	East US

A red box highlights the first item in the list, "Icep99-fgtaa".

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.

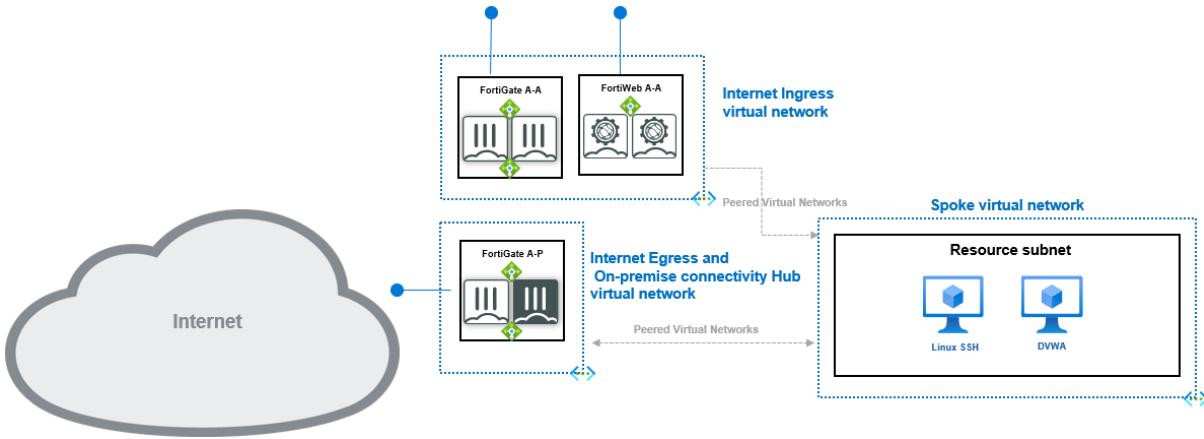
Objectives

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

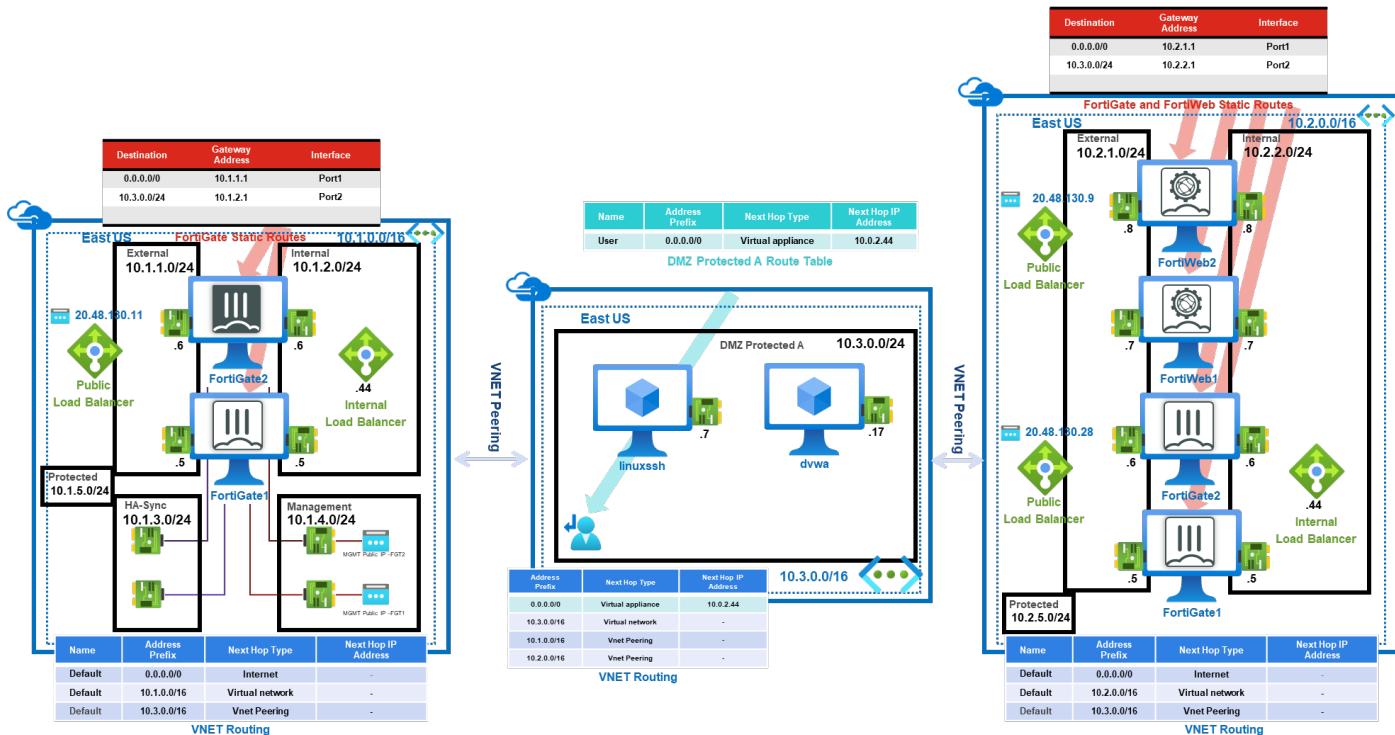
► Lab Access Using the Azure Portal

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**

The screenshot shows the Microsoft Azure portal homepage. At the top, there's a blue header bar with the 'Microsoft Azure' logo and a search bar that says 'Search resources, services, and docs (G+)'. Below the header, the main content area has a title 'Azure services' and a large button with a plus sign and the text 'Create a resource', which is circled in red. To the right of this button are icons for 'Resource groups', 'Virtual machines', 'Network security groups', and 'Route tables'. Below this section is a heading 'Resources' and two tabs: 'Recent' (which is underlined in blue) and 'Favorite'. At the bottom of the page, there are 'Recent' and 'Favorite' sections.

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

The screenshot shows the 'Create a resource' search results page. At the top, there's a blue header bar with the 'Microsoft Azure' logo and a search bar that says 'Search resources, services, and docs (G+)'. Below the header, the main content area has a heading 'Create a resource' and a search bar where 'virtual network' is typed in and highlighted with a red box. To the left, there's a sidebar with sections for 'Get Started', 'Recently created', and 'Categories' (which includes 'AI + Machine Learning', 'Analytics', 'Blockchain', 'Compute', and 'Containers'). In the center, there are cards for 'Virtual machine', 'Kubernetes Service', and 'Azure Cosmos DB', each with 'Create | Learn more' links. To the right, there are cards for 'Windows Server 2019 Datacenter', 'Ubuntu Server 20.04 LTS', and 'Windows 10 Pro, version 20H2', also with 'Create | Learn more' links. At the bottom, there's a 'Popular Azure services' section with a 'See more in All services' link.

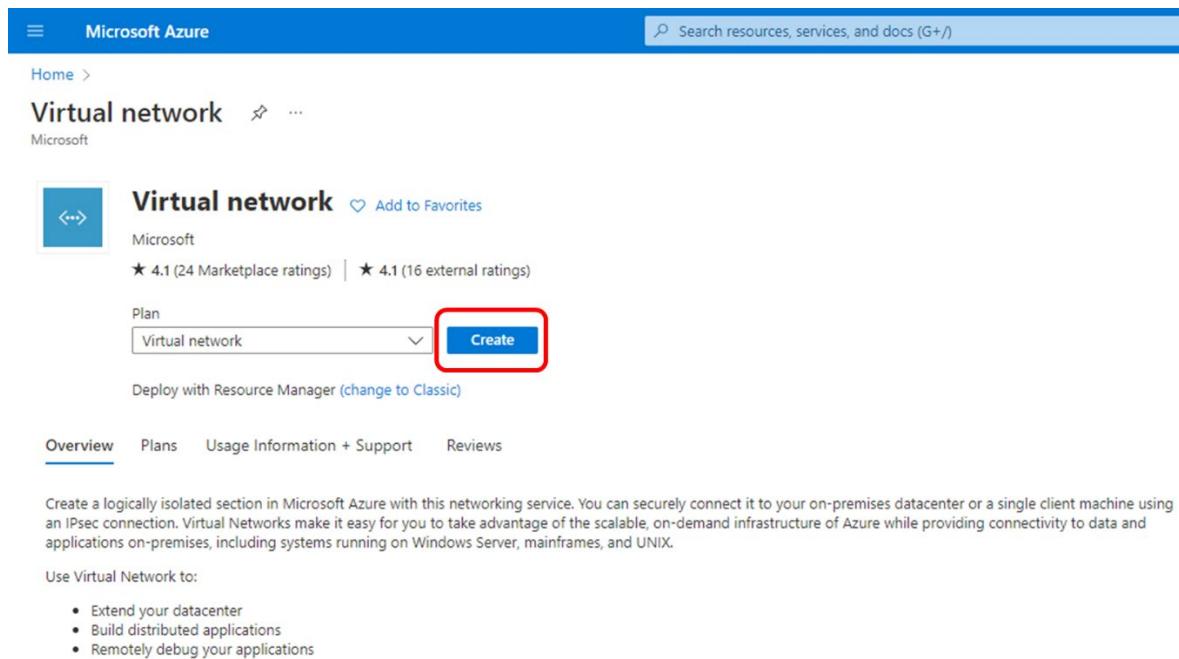
► Task 1 - Creating a Virtual Network in Azure

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

The screenshot shows the Microsoft Azure Marketplace interface. At the top, there's a search bar with the placeholder "Search resources, services, and docs (G+)" and a navigation bar with "Home > Create a resource > Marketplace". On the left, a sidebar includes sections for "Get Started", "Service Providers", "Management", "Private Marketplace", "Private Offer Management", "My Marketplace" (with "Favorites", "Recently created", and "Private products" listed), and "Categories" (with "Networking (186)", "Security (169)", "Compute (108)", and "IT & Management Tools"). The main area displays search results for "virtual network", showing 1 to 20 of 436 results. The first result, "Virtual network" by Microsoft, is highlighted with a red box. It has a blue icon with two arrows, the name "Virtual network", the provider "Microsoft", the category "Azure Service", and a description: "Create a logically isolated section in Microsoft Azure and securely connect it outward.". Below the description are "Create" and "Heart" buttons. Other results include "Virtual network gateway" by Microsoft, "Azure Virtual Network Endpoints Management" by KoçSistem, "Network Manager", "Network License Manager", and "Network security group". Each result card also has a "Create" button and a "Heart" button.

► Task 1 - Creating a Virtual Network in Azure

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



The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar. Below the header, the URL 'Virtual network' is visible. The main content area has a title 'Virtual network' with a 'Add to Favorites' link. It shows a rating of ★ 4.1 (24 Marketplace ratings) and ★ 4.1 (16 external ratings). A dropdown menu under 'Plan' is set to 'Virtual network'. A prominent blue 'Create' button is highlighted with a red rectangle. Below the button, there's a link 'Deploy with Resource Manager (change to Classic)'. At the bottom of the page, there are tabs for 'Overview' (which is selected), 'Plans', 'Usage Information + Support', and 'Reviews'.

► Task 1 - Creating a Virtual Network in Azure

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

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

The screenshot shows the Azure portal interface for creating a virtual network. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the breadcrumb navigation shows 'Home > Create a resource > Virtual network > Create virtual network'. The main content area has tabs for 'Basics', 'IP Addresses', 'Security', 'Tags', and 'Review + create'. The 'Basics' tab is selected. The 'Project details' section contains fields for 'Subscription' (set to 'FTNT-Training') and 'Resource group' (set to 'Icexp99-training'). Below that, the 'Instance details' section shows 'Name' (set to 'workload-VNET') and 'Region' (set to 'East US').

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



► Task 1 - Creating a Virtual Network in Azure

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

The screenshot shows the 'Create virtual network' interface in Microsoft Azure. The 'IP Addresses' tab is selected. In the 'IPv4 address space' section, the value '10.3.0.0/16' is entered, highlighted by a red box labeled '1'. Below this, there is a checkbox for 'Add IPv6 address space' which is unchecked. In the 'Subnet' section, a red box labeled '2' highlights the '+ Add subnet' button. To its right are 'Remove subnet' and 'Subnet name' fields. Below the subnet section, a message states 'This virtual network doesn't have any subnets.' At the bottom, there are two notifications: one with a red X icon stating 'This virtual network doesn't have any subnets.' and one with a blue info icon stating 'A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway.' Both notifications have a 'Learn more' link.

► Task 1 - Creating a Virtual Network in Azure

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

The screenshot shows the Azure portal interface for creating a virtual network. On the left, the 'Create virtual network' blade is visible with tabs for Basics, IP Addresses, Security, Tags, and Review + create. The IP Addresses tab is selected, showing an IPv4 address space of 10.3.0.0/16. Below this, there's a checkbox for 'Add IPv6 address space'. A note indicates that the subnet's address range must be contained within the virtual network's address space. The main area shows a table for subnets, which is currently empty. A tooltip message states: 'This virtual network doesn't have any subnets.' On the right, a modal dialog titled 'Add subnet' is open. It contains fields for 'Subnet name' (set to 'DMZ-Protected-A') and 'Subnet address range' (set to '10.3.0.0/24'). A note below the range specifies: '10.3.0.0 - 10.3.0.255 (251 + 5 Azure reserved addresses)'. This entire section is highlighted with a red rounded rectangle. The 'NAT GATEWAY' and 'SERVICE ENDPOINTS' sections of the modal are also visible but not highlighted.

9. Click on Add



► Task 1 - Creating a Virtual Network in Azure

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

The screenshot shows the 'Create virtual network' interface in Microsoft Azure, specifically the 'IP Addresses' tab. The 'IPv4 address space' is set to 10.3.0.0/16. A new subnet 'DMZ-Protected-A' has been added with the address range 10.3.0.0/24. This subnet entry is highlighted with a red box. A tooltip indicates that a NAT gateway is recommended for outbound internet access.

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

The screenshot shows the 'Review + create' page of the Azure virtual network creation wizard. The 'Next : Security >' button is highlighted with a red box. Other buttons visible include 'Review + create', '< Previous', and 'Download a template for automation'.

► Task 1 - Creating a Virtual Network in Azure

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**

Validation passed

Basics IP Addresses Security Tags Review + create

Basics

Subscription	FTNT-Training
Resource group	lcepx99-training
Name	workload-VNET
Region	East US

IP addresses

Address space	10.3.0.0/16
Subnet	DMZ-Protected-A (10.3.0.0/24)

Tags

None

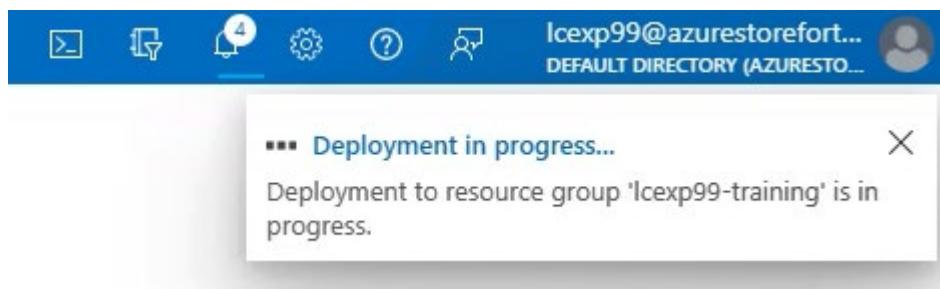
Security

BastionHost	Disabled
DDoS protection plan	Basic
Firewall	Disabled

< Previous Next > Download a template for automation

Create

14. The deployment of the VNET will start



► Task 1 - Creating a Virtual Network in Azure

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).

The screenshot shows the Microsoft Azure portal interface. The left sidebar lists 'Resource groups' with several items: 'Icexp99-fgtaa', 'Icexp99-fgtap', 'Icexp99-fwb', and 'Icexp99-training'. The 'Icexp99-training' item is selected and highlighted with a red box. The main content area shows the details for the 'Icexp99-training' resource group. It includes sections for 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Resource visualizer', and 'Events'. On the right, there is an 'Essentials' section with information about the subscription (move to FINT-Training), subscription ID (7ad47f34-2562-4fac-aed6-b2c68b2ad93f), and tags. Below this is a 'Resources' section with a table showing two records: 'Icexp999b6048c2training' and 'workload-VNET'. The 'workload-VNET' row is also highlighted with a red box.

16. The Workload VNET was successfully created

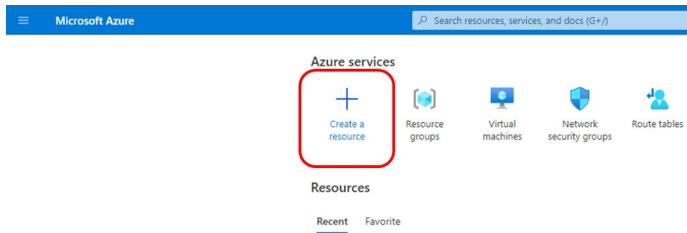
- ▶ Task 2 - Deploy linuxssh virtual machine

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

The screenshot shows the 'Create a resource' page. On the left, there's a sidebar with categories like 'Get Started', 'Recently created', and 'Categories'. Under 'Categories', there are links for 'AI + Machine Learning', 'Analytics', 'Blockchain', 'Compute', 'Containers', 'Databases', and 'Developer Tools'. The main area has sections for 'Popular Azure services' (with 'Virtual machine' highlighted), 'Popular Marketplace products' (listing 'Windows Server 2019 Datacenter', 'Ubuntu Server 20.04 LTS', 'Windows 10 Pro, version 20H2', and 'Ubuntu Server 18.04 LTS'), and a 'Getting Started?' link.

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	Icexp<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

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

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20220912155340 | Overview > Icexp99-training > Marketplace > Ubuntu Server 20.04 LTS > Create a virtual machine ...

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

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

Subscription * FTNT-Training

Resource group * Icexp99-training [Create new](#)

Instance details

Virtual machine name * linuxssh

Region * (US) East US

Availability options No infrastructure redundancy required

Security type Standard

Image * Ubuntu Server 20.04 LTS - Gen1 [See all images](#) | [Configure VM generation](#)

VM architecture Arm64 x64 Arm64 is not supported with the selected image.

Run with Azure Spot discount

Size * Standard_B1s - 1 vcpu, 1 GiB memory (\$7.59/month) [See all sizes](#)

Administrator account

Authentication type SSH public key Password

Username * azureadm

Password * *****

Confirm password * *****

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * None Allow selected ports

Select inbound ports * SSH (22)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

[Review + create](#) [< Previous](#) [Next : Disks >](#)

► 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

The screenshot shows the Microsoft Azure 'Create a virtual machine' interface. The 'Networking' tab is selected. The 'Public IP' dropdown is set to 'None' and is highlighted with a red box. A tooltip below the dropdown reads: '⚠️ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.' Other settings visible include 'Virtual network' (workload-VNET), 'Subnet' (DMZ-Protected-A (10.3.0.0/24)), and 'NIC network security group' (Basic selected).

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

▶ Task 2 - Deploy linuxssh virtual machine

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.

Microsoft Azure

Search resources, services, and docs (G+)

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20220912155340 | Overview > Icexp99-training > Marketplace > Ubuntu Server 20.04 LTS >

Create a virtual machine

Basics Disks Networking Management **Monitoring** Advanced Tags Review + create

Configure monitoring options for your VM.

Diagnostics

Boot diagnostics Enable with managed storage account (recommended) **1** Enable with custom storage account Disable

Enable OS guest diagnostics

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**

Microsoft Azure

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20220912155340 | Overview > lcxp99-training > Marketplace > Ubuntu Server 20.04 LTS

Create a virtual machine

Validation passed

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.

PRODUCT DETAILS

1 X Standard B1s by Microsoft Terms of use | Privacy policy Subscription credits apply ⓘ 0.0104 USD/hr Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name

Preferred e-mail address

Preferred phone number

⚠ You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

Create < Previous Next > Download a template for automation

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.

Task 3 - Deploy dvwa virtual machine.

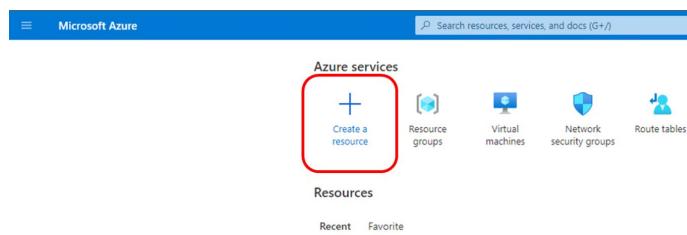
Our next step is going to be creation of the next VM (Virtual Machine) into the workload VNET. This VM will be running the software DVWA.

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

Category	Service	Action
Get Started	Getting Started? Try our Quickstart center	
Recently created		
Categories	Virtual machine	Create Learn more
AI + Machine Learning	Kubernetes Service	Create Docs MS Learn
Analytics	Azure Cosmos DB	Create Docs MS Learn
Blockchain	Function App	Create Docs
Compute		
Containers		
Databases		
Developer Tools		
...+...		
Popular Marketplace products	Windows Server 2019 Datacenter	Create Learn more
	Ubuntu Server 20.04 LTS	Create Learn more
	Windows 10 Pro, version 20H2	Create Learn more
	Ubuntu Server 18.04 LTS	Create Learn more

- ▶ 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	Icexp< <i>your student number</i> >-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	< <i>choose your own</i> >
Public inbound ports	Allow selected ports
Select inbound ports	SSH (22), HTTP (80), HTTPS (443)

► Task 3 - Deploy dvwa virtual machine.

Microsoft Azure

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20220912160857 | Overview > Icexp99-training > Marketplace > Create a virtual machine ...

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

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

Subscription * ⓘ FTNT-Training

Resource group * ⓘ Icexp99-training

Instance details

Virtual machine name * ⓘ dvwa

Region * ⓘ (US) East US

Availability options ⓘ No infrastructure redundancy required

Security type ⓘ Standard

Image * ⓘ Ubuntu Server 20.04 LTS - Gen1

VM architecture ⓘ x64

Run with Azure Spot discount ⓘ

Size * ⓘ Standard_B2s - 2 vcpus, 4 GiB memory (\$30.37/month)

Administrator account

Authentication type ⓘ Password

Username * ⓘ azureadadm

Password * ⓘ
Confirm password * ⓘ

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ Allow selected ports

Select inbound ports * ⓘ HTTP (80), HTTPS (443), SSH (22)

Warning: This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

► 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

The screenshot shows the Microsoft Azure 'Create a virtual machine' interface. The 'Networking' tab is selected. The 'Public IP' dropdown is set to 'None' and is highlighted with a red box. Other settings include a 'Virtual network' of 'workload-VNET', a 'Subnet' of 'DMZ-Protected-A (10.3.0.0/24)', and 'NIC network security group' set to 'Basic'. A warning message at the bottom states: '⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.' There are also checkboxes for 'Delete NIC when VM is deleted' and 'Enable accelerated networking'.

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.

The screenshot shows the 'Create a virtual machine' wizard in Microsoft Azure, specifically the 'Monitoring' step. The 'Monitoring' tab is selected in the top navigation bar. Below it, a sub-header says 'Configure monitoring options for your VM.' Under the 'Diagnostics' section, there are three options:

- Enable with managed storage account (recommended)
- Enable with custom storage account** (highlighted with a red box labeled '1')
- Disable

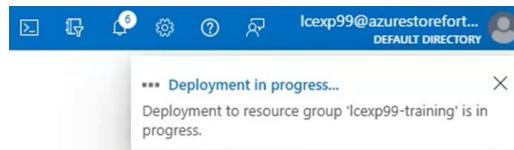
Below these options is a checkbox for 'Enable OS guest diagnostics'. Further down, a dropdown menu for 'Diagnostics storage account' is shown, containing the value 'Icexp999b6048c2training' (highlighted with a red box labeled '2'). A 'Create new' button is visible next to the dropdown. At the bottom of the screen, there are navigation buttons: 'Review + create' (highlighted in blue), '< Previous', 'Next : Advanced >', and 'Next : Tags'.

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.

The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The top navigation bar includes 'Microsoft Azure', a search bar, and a breadcrumb trail: Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20220912160857 | Overview > lcexp99-training > Marketplace > Create a virtual machine. Below the navigation is a green validation message: 'Validation passed'. The 'Review + create' tab is selected in the top navigation bar. A note below states: 'Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.' The 'PRODUCT DETAILS' section shows '1 X Standard B2s by Microsoft' with a price of '0.0416 USD/hr'. It also links to 'Subscription credits apply', 'Terms of use', and 'Privacy policy'. The 'Pricing for other VM sizes' link is highlighted with a blue border. The 'TERMS' section contains a detailed legal agreement. Below it, form fields are filled with 'Name: lcexp99 undefined', 'Preferred e-mail address: (empty)', and 'Preferred phone number: (empty)'. A warning message at the bottom left says: '⚠ You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.' At the bottom, the 'Basics' tab is selected, and the 'Create' button is highlighted with a red box. Navigation buttons include '< Previous', 'Next >', and 'Download a template for automation'.

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**

The screenshot shows the Microsoft Azure 'Overview' page for a deployment named 'CreateVm-canonical.0001-com-ubuntu-server-focal-2-20220912161852'. The deployment status is 'complete'. Key details include:

- Deployment name: CreateVm-canonical.0001-com-ubuntu-server-focal-2-20220912161852
- Subscription: FTNT-Training
- Resource group: Icexp99-training
- Start time: 9/12/2022, 4:20:41 PM
- Correlation ID: 881dbce6-724c-4df1-a585-64492214d52c

Below the deployment summary, there are sections for 'Deployment details' and 'Next steps'. Under 'Next steps', three options are listed: 'Setup auto-shutdown' (Recommended), 'Monitor VM health, performance and network dependencies' (Recommended), and 'Run a script inside the virtual machine' (Recommended). A red box highlights the 'Go to resource' button, which is located at the bottom of the 'Next steps' section.

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

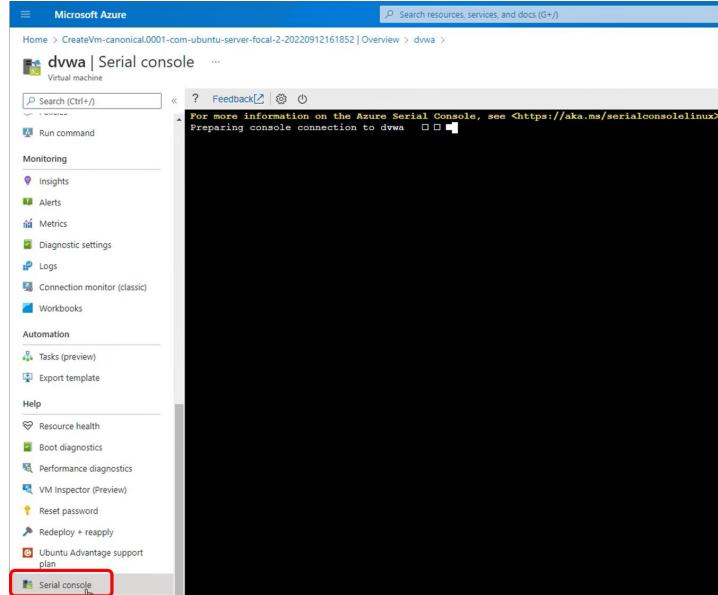
The screenshot shows the Microsoft Azure 'Virtual machine' overview page for the 'dvwa' VM. The VM is running in the 'East US' location. Key details include:

- Resource group: Icexp99-training
- Status: Running
- Location: East US
- Subscription: FTNT-Training
- Subscription ID: 7ad47f34-2562-4fac-aed6-b2c68b2ad93f
- Tags: Click here to add tags

The left sidebar lists navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Disks, and Size. The 'Virtual machine' tab is selected. A red box highlights the 'dvwa' VM thumbnail in the top navigation bar.

► 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 (**azureadadm** and the chosen password)

```

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

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20220912161852 | Overview > dvwa

dvwa | Serial console ...
```

The screenshot shows the Microsoft Azure portal interface for a virtual machine named 'dvwa'. The left sidebar contains a list of management options, with 'Serial console' highlighted by a red box. The main pane displays a terminal session titled 'Serial console'. The terminal output shows the following sequence of events:

```

<14>Sep 12 20:21:48 cloud-init: 256 SHA256:A/KPVoLXGKsZ3xBdUj35DhUnTwwgf+YNLjQRIsjG0LE root@dsvwa (ECDSA)
<14>Sep 12 20:21:48 cloud-init: 256 SHA256:Uyxla3ayWx1wS220ndgpy88Lyvv3akvMF9XoSMeWI root@dsvwa (ED25519)
<14>Sep 12 20:21:48 cloud-init: 3072 SHA256:R6Kkib5qf72ConnGQlBzkkgiDFYl5lOcgGzT6pF5tWc root@dsvwa (RSA)
<14>Sep 12 20:21:48 cloud-init: -----END SSH HOST KEY FINGERPRINTS-----
-----BEGIN SSH HOST KEY KEYS-----
ecdsa-sha2-nistp256 AAAAE2VjZHNhLKNoYTItbmlzdHAyNTYAAAIBmlzdHAyNTYAAAIBBEOMxeqxCCDjP9YHsS+UBCendaN4w2zyaK/1A6Z2PnPcxFHO
ssh-ed25519 AAAAC3NzaC1lZDI1TE5AAAAIN5UrAtuyy24fNGON56LGe356/MDiD0eiGJc29/Hj root@dsvwa
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAABgQDWKtR6u58gevx9b1hBdKM+Gv3TospwqhTwH7RMNpNDNmPjbDd8Yd4xCCWJXb2juzXp6j1vVxuggGBtDFo7
sempC0c9N+kp2khzF6JDBln0uEHFy1Xbjqhr6xYnmuFnFrtAvEso/ln4W94WE9mvxehDcrIRNHYmemhA2jmUFHeeVv4ScmpqfQarX3XV29RE5BXs/wTi
bx8KPNRUI7TOE8eKFf3NjJLKFB9MPN67C2Ivb3XEP+xDDL3hkteN2KvC+f7zeBeu1p0SW3FbB4iwrCSyjmhW3ElR8Uta15RCImcCizJJnt0jb4fydkPMztW/s
54j4ox4E= root@dsvwa
-----END SSH HOST KEY KEYS-----
[ 39.824074] cloud-init[1642]: Cloud-init v. 22.2-0ubuntu1-20.04.3 running 'modules:final' at Mon, 12 Sep 2022 20:21:47
[ 39.829382] cloud-init[1642]: Cloud-init v. 22.2-0ubuntu1-20.04.3 finished at Mon, 12 Sep 2022 20:21:48 +0000. Datasource
2022-09-12T20:36:39.719461Z INFO Daemon Agent WALinuxAgent-2.8.0.11 launched with command 'python3 -u bin/WALinuxAgent-2.

dvwa login: azureadadm
Password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-1019-azure x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Mon Sep 12 20:38:25 UTC 2022

System load: 0.01           Processes:          109
Usage of /: 4.9% of 28.89GB   Users logged in:      0
Memory usage: 7%             IPv4 address for eth0: 10.3.0.5
Swap usage: 0%              

0 updates can be applied immediately.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

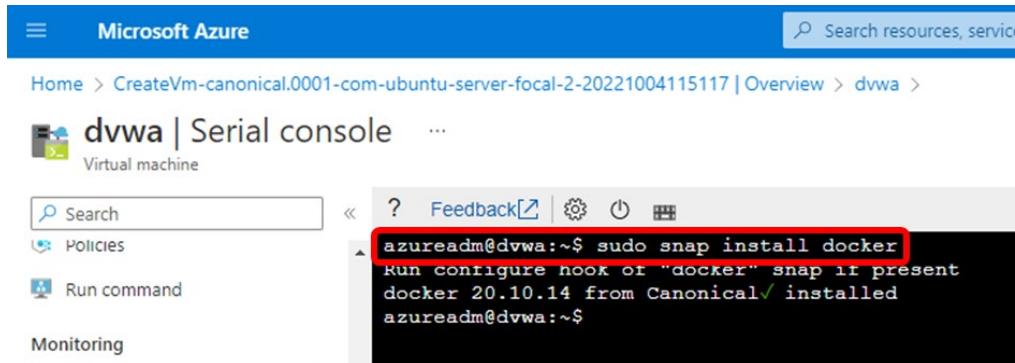
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureadadm@dsvwa:~$
```

► Task 3 - Deploy dvwa virtual machine.

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

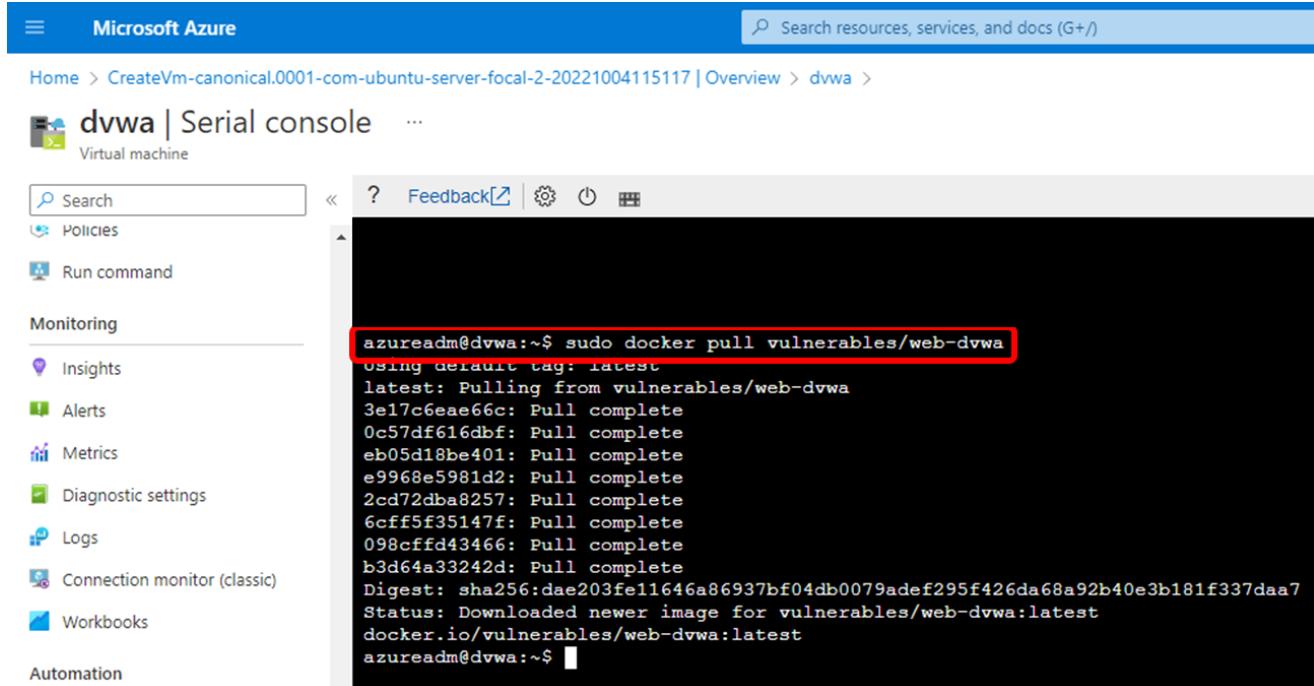
```
sudo snap install docker
```



The screenshot shows the Microsoft Azure portal interface. In the center, there's a terminal window titled "dvwa | Serial console". The command "sudo snap install docker" is entered and its output is displayed: "azureadm@dvwa:~\$ sudo snap install docker", "Run configure hook of "docker" snap if present", "docker 20.10.14 from Canonical✓ installed", and "azureadm@dvwa:~\$". The entire command line is highlighted with a red box.

18. Next install DVWA by entering the following command:

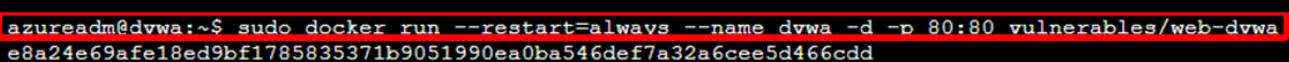
```
sudo docker pull vulnerables/web-dvwa
```



The screenshot shows the Microsoft Azure portal interface. In the center, there's a terminal window titled "dvwa | Serial console". The command "sudo docker pull vulnerables/web-dvwa" is entered and its output is displayed: "azureadm@dvwa:~\$ sudo docker pull vulnerables/web-dvwa", "Using default tag: latest", "latest: Pulling from vulnerables/web-dvwa", "3e17c6aae66c: Pull complete", "0c57df616dbf: Pull complete", "eb05d18be401: Pull complete", "e9968e5981d2: Pull complete", "2cd72dba8257: Pull complete", "6cff5f35147f: Pull complete", "098cffd43466: Pull complete", "b3d64a33242d: Pull complete", "Digest: sha256:dae203fe11646a86937bf04db0079adef295f426da68a92b40e3b181f337daa7", "Status: Downloaded newer image for vulnerables/web-dvwa:latest", and "docker.io/vulnerables/web-dvwa:latest". The entire command line is highlighted with a red box.

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
```



The screenshot shows the Microsoft Azure portal interface. In the center, there's a terminal window titled "dvwa | Serial console". The command "sudo docker run --restart=always --name dvwa -d -p 80:80 vulnerables/web-dvwa" is entered and its output is displayed: "azureadm@dvwa:~\$ sudo docker run --restart=always --name dvwa -d -p 80:80 vulnerables/web-dvwa" and "e8a24e69afe18ed9bf1785835371b9051990ea0ba546def7a32a6cee5d466cdd". The entire command line is highlighted with a red box.

- ▶ Task 3 - Deploy dvwa virtual machine.

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

```
sudo docker container ls
```

```
azureadm@dvwa:~$ sudo docker container ls
CONTAINER ID        IMAGE               COMMAND       CREATED          STATUS          PORTS          NAMES
e8a24e69afe1        vulnerables/web-dvwa   "/main.sh"   39 seconds ago   Up 37 seconds   0.0.0.0:80->80/tcp, :::80->80/tcp   dvwa
azureadm@dvwa:~$
```

21. The DVWA VM was successfully deployed

▶ Task 4 - Deploy FortiGate Active-Passive

Task 4 - Deploy FortiGate Active-Passive

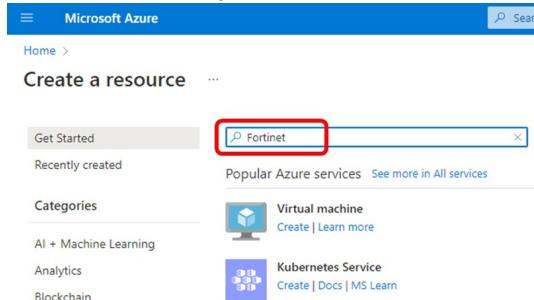
The next step is the deployment of the of the FortiGate firewalls (in Active-Passive mode) along with associated network resources including the virtual network for the Internet Egress Hub.

Creation steps

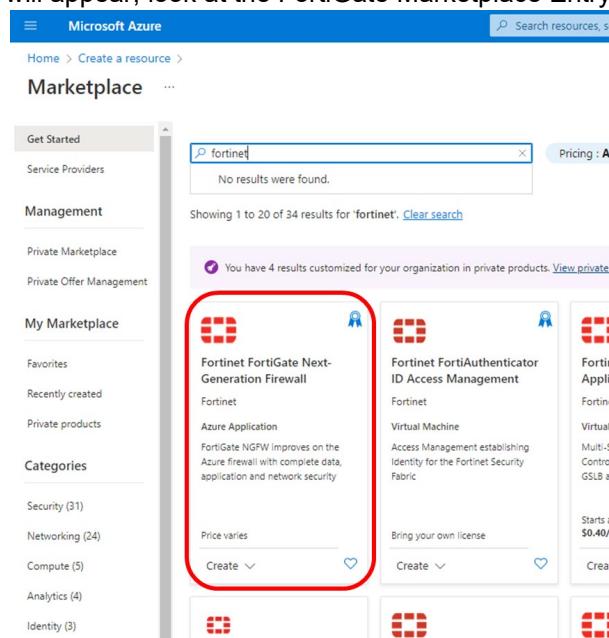
1. From the main Azure Portal, click on **Create a resource**



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

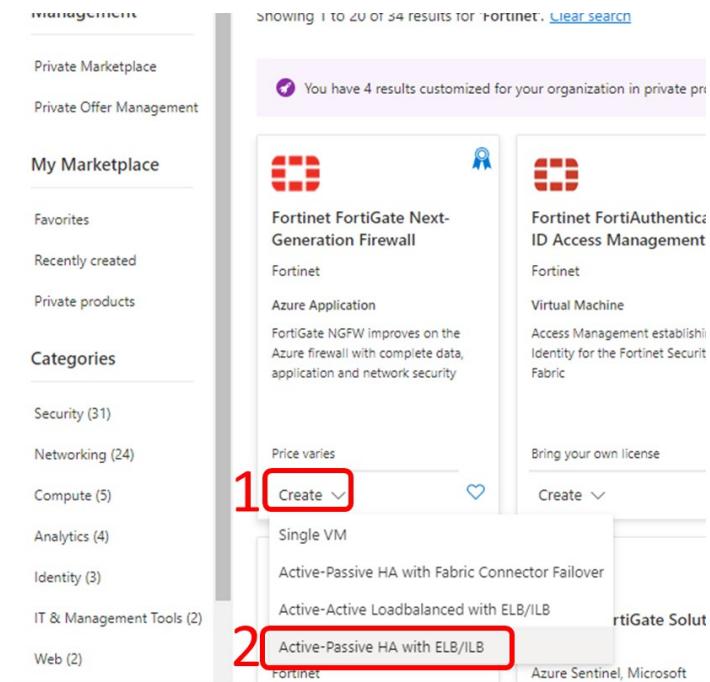


3. The following results will appear, look at the FortiGate Marketplace Entry



► Task 4 - Deploy FortiGate Active-Passive

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



► Task 4 - Deploy FortiGate Active-Passive

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

Subscription	FTNT-Training
Resource group	Icexp<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

Microsoft Azure Search resources, services

Home > Create a resource > Marketplace > **Create Fortinet FortiGate Next-Generation Firewall** ...

Basics Instance Networking Public IP Public IP Verification Advanced Review + create

Project details

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

Subscription * ⓘ FTNT-Training

Resource group * ⓘ Icexp99-fgtap Create new

Instance details

Region * ⓘ East US

FortiGate Deployment Type - Active/Passive - External and Internal Load Balancers - Availability Set or Availability Zones ⓘ

FortiGate administrative username * ⓘ azureadm

FortiGate password * ⓘ Hide

Confirm password * ⓘ

FortiGate Name Prefix * ⓘ fgap

FortiGate Image SKU ⓘ Pay As You Go

FortiGate Image Version ⓘ Latest

► Task 4 - Deploy FortiGate Active-Passive

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

Microsoft Azure

Search resources, services, and docs (G+)

Home > Create a resource > Marketplace >

Create Fortinet FortiGate Next-Generation Firewall

Basics **Instance** Networking Public IP Public IP Verification Advanced Review + create

Instance Type

For this FortiGate deployment, it is recommended to use the general purpose or compute optimized virtual machines. A selection of supported instances sizes is listed in our documentation. FortiGate Active/Passive HA uses the FGCP protocol for configuration sync and HA failover. This requires dedicated sync and management ports. A minimum of 4 NICs is required for the instance type.

[Learn more](#)

Size * ⓘ	2x Standard F4s
	4 vcpus, 8 GB memory
	Change size

Availability Options

Deploy FortiGate VMs in an Availability Set or Availability Zones.

[Learn more](#)

Availability Option ⓘ	Availability Set
-----------------------	-------------------------

FortiGate License

FortiGate A Flex-VM ⓘ

FortiGate B Flex-VM ⓘ

Pay As You Go licenses was selected in the basics blade and provisioned automatically during deployment. Registration of the PAYG license is required to receive support.

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

► Task 4 - Deploy FortiGate Active-Passive

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

Microsoft Azure

Home > Create a resource > Marketplace > Create Fortinet FortiGate Next-Generation Firewall

Networking

Configure Internal Networking

Create a new or select an existing virtual network with the required subnets.

Configure virtual networks

Virtual network * (new) fgap-VNET
Create new

External Subnet * (new) ExternalSubnet (10.0.0.0/26)

Internal subnet * (new) InternalSubnet (10.0.1.0/26)

HA Sync subnet * (new) HASyncSubnet (10.0.2.0/26)

HA Management subnet * (new) HAMGMTSubnet (10.0.3.0/26)

Protected A subnet * (new) ProtectedASubnet (10.0.4.0/24)

ⓘ The selected subnets should be empty and will only be used by the FortiGate VMs network interfaces. The internal subnet is a transit subnet containing only the FortiGate interfaces for traffic to and from the internal networks. Internal systems should be installed in a protected subnet with user defined route configuration.

Accelerated networking

Enables SR-IOV support allowing the FortiOS to bypass the hypervisor and talk directly with the PCIe hardware.

Learn more

Enabled Disabled

► Task 4 - Deploy FortiGate Active-Passive

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

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network which is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or your on-premises network.

2 Name * hub-VNET

3 ADDRESS SPACE
The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

Address range	Addresses
10.1.0.0/16	10.1.0 - 10.1.255.255 (65536 addresses)

4 SUBNETS
The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.

Subnet name	Address range	Addresses
ExternalSubnet	10.1.1.0/24	10.1.1.0 - 10.1.1.255 (256 addresses)
InternalSubnet	10.1.2.0/24	10.1.2.0 - 10.1.2.255 (256 addresses)
HASyncSubnet	10.1.3.0/24	10.1.3.0 - 10.1.3.255 (256 addresses)
HAMGMTSubnet	10.1.4.0/24	10.1.4.0 - 10.1.4.255 (256 addresses)
ProtectedASubnet	10.1.5.0/24	10.1.5.0 - 10.1.5.255 (256 addresses)

5 OK Discard

11. Click OK to return to the networking pane

▶ Task 4 - Deploy FortiGate Active-Passive

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

Microsoft Azure

Home > Create a resource > Marketplace >

Create Fortinet FortiGate Next-Generation Firewall

Basics Instance **Networking** Public IP Public IP Verification Advanced Review + create

Configure Internal Networking

Create a new or select an existing virtual network with the required subnets.

Configure virtual networks

Virtual network * ⓘ (new) hub-VNET

External Subnet * ⓘ (new) ExternalSubnet (10.1.1.0/24)

Internal subnet * ⓘ (new) InternalSubnet (10.1.2.0/24)

HA Sync subnet * ⓘ (new) HASyncSubnet (10.1.3.0/24)

HA Management subnet * ⓘ (new) HAMGMTSubnet (10.1.4.0/24)

Protected A subnet * ⓘ (new) ProtectedASubnet (10.1.5.0/24)

Note: ⓘ The selected subnets should be empty and will only be used by the FortiGate VMs network interfaces. The internal subnet is a transit subnet containing only the FortiGate interfaces for traffic to and from the internal networks. Internal systems should be installed in a protected subnet with user defined route configuration.

Accelerated networking

Enables SR-IOV support allowing the FortiOS to bypass the hypervisor and talk directly with the PCIe hardware.
Learn more

Accelerated Networking ⓘ Enabled Disabled

Review + create **< Previous** **Next : Public IP >**

► Task 4 - Deploy FortiGate Active-Passive

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

The screenshot shows the 'Create Fortinet FortiGate Next-Generation Firewall' wizard in the Microsoft Azure portal. The current step is 'Public IP'. The 'External Load Balancer' dropdown is highlighted with a red box labeled '1'. A tooltip indicates it contains '(new) fgap-FGT-PIP'. Below it are dropdowns for 'FortiGate A management' and 'FortiGate B management', both showing '(new)' and 'Create new' options.

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

The screenshot shows the 'Create public IP address' pane. It includes fields for 'Name' (set to 'fgap-FGT-PIP'), 'SKU' (radio button selected for 'Standard', indicated by a red box labeled '2'), and 'Routing preference' (radio button selected for 'Microsoft network').

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

The screenshot shows the 'Create Fortinet FortiGate Next-Generation Firewall' wizard again. The 'Public IP' step is shown. Three 'Create new' buttons for 'External Load Balancer', 'FortiGate A management', and 'FortiGate B management' are highlighted with red boxes.

16. Click on **Next: Public IP Verification** at the bottom

17. Confirm the Public IP have been validated

The screenshot shows the 'Public IP Verification' step. It displays three validation messages: 'The External Load Balancer Public IP is Standard SKU. Proceed.', 'The FortiGate A management Public IP is Standard SKU or none selected. Proceed.', and 'The FortiGate B management Public IP is Standard SKU or none selected. Proceed.'.

► Task 4 - Deploy FortiGate Active-Passive

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**

Validation Passed

Basics Instance Networking Public IP Public IP Verification Advanced Review + create

PRODUCT DETAILS

Fortinet FortiGate Next-Generation Firewall
by Fortinet

Terms of use | Privacy policy

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name Icexp99 undefined

Preferred e-mail address

Preferred phone number

Basics

Subscription	FTNT-Training
Resource group	Icexp99-fgtap
Region	East US
FortiGate administrative username	azureadm
FortiGate password	*****
FortiGate Name Prefix	fngn

Create < Previous Next Download a template for automation

20. A notification of the deployment start will display



► Task 4 - Deploy FortiGate Active-Passive

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

The screenshot shows the Microsoft Azure Deployment Overview page for a completed deployment. The deployment name is 'fortinet.fortinet-fortigate-20220912142528'. It was deployed by 'FTNT-Training' under the resource group 'Icexp99-fgtap'. The deployment started at 9/12/2022, 2:33:00 PM and has a correlation ID of c66d5d04-f196-4dca-b0d1-241c13d01be8. A green checkmark indicates the deployment is complete. There are links for 'Deployment details', 'Next steps', and 'Go to resource group'.

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**

The screenshot shows the Microsoft Azure Resource groups page. The 'Resource groups' button is highlighted with a red box. Other buttons include 'Create a resource', 'Virtual machines', 'Quickstart Center', 'App Services', 'Storage accounts', 'SQL databases', and 'Azure Cosmos DB'.

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

The screenshot shows the Microsoft Azure Resource groups list page. The 'Icexp99-fgtap' resource group is selected and highlighted with a red box. Other visible resource groups include 'Icexp99-fgtaa', 'Icexp99-fwb', and 'Icexp99-training'. There are filters for 'Name' and 'Subscription equals all'.

► Task 4 - Deploy FortiGate Active-Passive

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

The screenshot shows the Azure portal interface for the resource group 'Icexp99-fgtap'. On the left, there's a navigation menu with sections like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings (Deployments, Security, Policies, Properties, Locks), Cost Management (Cost analysis, Cost alerts (preview), Budgets, Advisor recommendations), Monitoring (Insights (preview), Alerts, Metrics), and a hub-VNET section. The main pane displays a list of resources under the 'Resources' tab. A search bar at the top allows filtering by name, type, and location. The results show 24 records, including network interfaces, disks, a PIP, and the route table. The resource 'fgap-RouteTable-ProtectedASubnet' is specifically highlighted with a red box and a cursor pointing to it.

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

The screenshot shows the 'fgap-RouteTable-ProtectedASubnet' route table settings page. The left sidebar has a 'Subnets' menu item highlighted with a red box. The main area shows a table with one subnet entry: 'ProtectedASubnet' with an address range of '10.1.5.0/24' and associated with 'hub-VNET'. There are also tabs for Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems.

▶ Task 4 - Deploy FortiGate Active-Passive

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

fgap-RouteTable-ProtectedASubnet | Subnets

Route table

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

+ Associate

Search subnets

Name ↑ Address range ↑ Virtual network ↑

ProtectedASubnet 10.1.5.0/24 hub-VNET

28. Confirm by clicking on **Yes**

Dissociate subnet

Do you want to dissociate the subnet 'ProtectedASubnet'?

Yes No

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

fgap-RouteTable-ProtectedASubnet | Subnets

Route table

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

+ Associate

Search subnets

Name ↑

No results.

► Task 4 - Deploy FortiGate Active-Passive

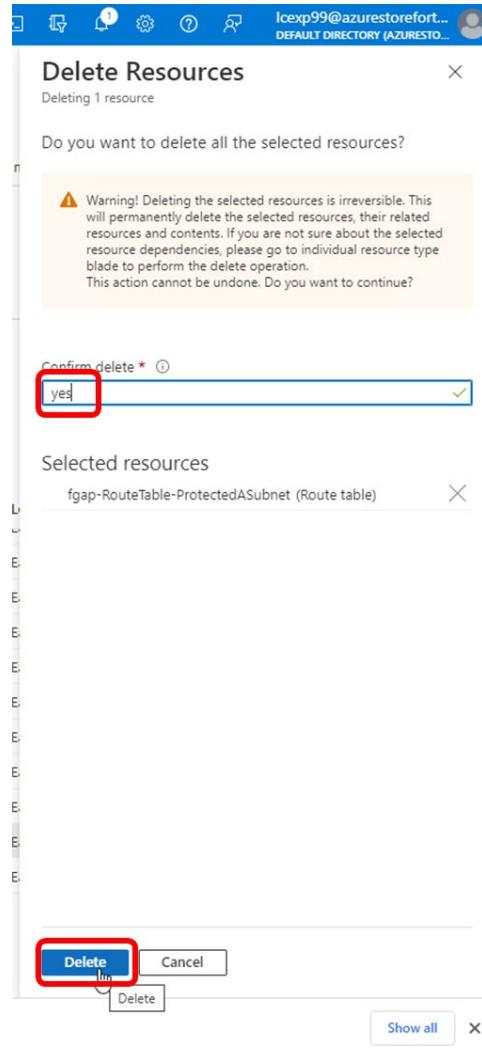
30. Go back to on the Icexp<*your student number*>-fgtaa resource group and then scroll all the way down and select the route table named **fgap-RouteTable-ProtectedASubnet**

Name	Type	Location
fgap-FGT-B_disk2_e0fea5d8f7a14304a877f7774e...	Disk	East US
fgap-FGT-B_OsDisk_1_dce6f1b731b64be5aef3fb...	Disk	East US
fgap-FGT-PIP	Public IP address	East US
fgap-InternalLoadBalancer	Load balancer	East US
fgap-RouteTable-ProtectedASubnet	Route table	East US
hub-VNET	Virtual network	East US

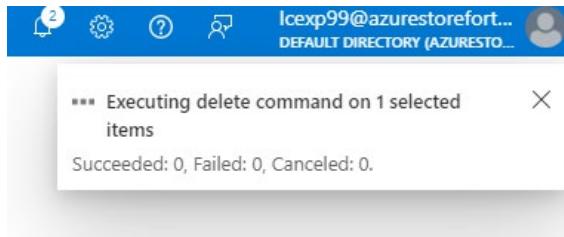
31. Click on Delete on the top menu

▶ Task 4 - Deploy FortiGate Active-Passive

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

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**

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it is a section for 'Azure services' with various icons like 'Create a resource', 'Quickstart Center', 'Virtual machines', etc. The main area is titled 'Resources' with tabs for 'Recent' and 'Favorite'. It shows a message 'No resources have been viewed recently' and a 'View all resources' button. In the 'Tools' section, there are links for 'Subscriptions', 'Resource groups' (which is highlighted with a red box), 'All resources', and 'Dashboard'. There are also links for 'Microsoft Learn', 'Azure Monitor', 'Microsoft Defender for Cloud', and 'Cost Management'.

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

This screenshot shows the 'Resource groups' page in the Azure portal. The URL in the browser bar is 'portal.azure.com/#view/HubsExtension/BrowseResourceGroups'. The page lists several resource groups: 'Icexp99-fgtaa' (selected and highlighted with a red box), 'Icexp99-fgtap', 'Icexp99-fwb', and 'Icexp99-training'. Each group has a checkbox next to its name. To the right, there are columns for 'Subscription' (FTNT-Training) and 'Location' (East US). At the bottom, there are buttons for 'Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'.

► Task 5 - Configure VNET Peering FGAP

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

The screenshot shows the Microsoft Azure Resource Groups interface. In the left sidebar, under 'Resource groups', the 'hub-VNET' entry is highlighted. The main pane displays the 'Essentials' section for the 'Icexp99-fgtap' resource group. It includes details like Subscription ID, Deployment count, and Location. Below this, the 'Resources' section lists various Azure resources, including several Network interfaces and a Disk, all associated with the 'hub-VNET'. A red box highlights the 'hub-VNET' entry in the list.

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

The screenshot shows the 'hub-VNET' settings page in the Microsoft Azure portal. The left sidebar lists various settings like Address space, Connected devices, Subnets, and DNS servers. The 'Peerings' tab is highlighted with a red box and a large number '1' above it. Other tabs include Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems.

- In the right pane, click **+ Add**

The screenshot shows the 'Peering' list page for the 'hub-VNET'. The top navigation bar shows the path 'Icexp99-fgtap > hub-VNET'. The main area displays a table of existing peerings. At the top of the table, there is a red box around the '+ Add' button, which is highlighted with a large number '2'.

► Task 5 - Configure VNET Peering FGAP

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

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

The screenshot shows the 'Add peering' configuration page in the Microsoft Azure portal. The page has two main sections: 'This virtual network' and 'Remote virtual network'.

- This virtual network:**
 - Peering link name ***: outbound-to-workload (highlighted with a red box and labeled 1)
 - Traffic to remote virtual network: Allow (default) (radio button selected)
 - Traffic forwarded from remote virtual network: Allow (default) (radio button selected)
 - Virtual network gateway or Route Server: None (default) (radio button selected)
- Remote virtual network:**
 - Peering link name ***: workload-to-outbound (highlighted with a red box and labeled 2)
 - Virtual network deployment model: Resource manager (radio button selected)
 - I know my resource ID:
 - Subscription: FTNT-Training (dropdown menu)
 - Virtual network ***: workload-VNET (highlighted with a red box and labeled 3)
 - Traffic to remote virtual network: Allow (default) (radio button selected)
 - Traffic forwarded from remote virtual network: Allow (default) (radio button selected)
 - Virtual network gateway or Route Server: None (radio button selected)

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

► Task 5 - Configure VNET Peering FGAP

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:

A screenshot of the Microsoft Azure portal showing the 'Peerings' blade. The table lists one peering entry: 'outbound-to-workload'. The 'Peering status' column shows 'Connected' and the 'Peer' column shows 'workload-VNET'. A red box highlights this row.

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

A screenshot of the Microsoft Azure portal navigation bar. The 'Resource groups' link is highlighted with a red box. The full path shown is Home > Resource groups > Icexp99-fgtap > hub-VNET.

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

A screenshot of the Microsoft Azure portal 'Resource groups' blade. The 'Icexp99-training' resource group is highlighted with a red box. The blade shows basic information like 'Default Directory (azurestorefortinet.onmicrosoft.com)', 'Subscription (move) : FINT-Training', and 'Deployments : 5 Succeeded'.

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

A screenshot of the Microsoft Azure portal 'Resources' blade for the 'Icexp99-training' resource group. The 'linuxssh645' network interface is highlighted with a red box. The blade lists various resources including virtual machines, network security groups, and disks.

► Task 5 - Configure VNET Peering FGAP

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

The screenshot shows the Azure portal interface for a network interface named 'linuxssh645'. The left sidebar contains several sections: Overview, Activity log, Access control (IAM), Tags, Settings (with IP configurations, DNS servers, Network security group, Properties, Locks), Monitoring (with Insights, Alerts, Metrics, Diagnostic settings), Automation (with Tasks (preview) and Export template), Help, and a bottom section with Effective security rules and Effective routes. The 'Effective routes' item is highlighted with a red box and labeled '1'.

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

The screenshot shows the 'Effective routes' table for the 'linuxssh645' network interface. The table has columns: Source, State, Address Prefixes, Next Hop Type, and User Defined Route Name. There are eight rows listed. The second row, which corresponds to the 'VNet peering' entry, is highlighted with a red box and labeled '2'.

Source	State	Address Prefixes	Next Hop Type	User Defined Route Name
Default	Active	10.3.0.0/16	Virtual network	-
Default	Active	10.1.0.0/16	VNet peering	2
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	-

14. The VNET peering is complete

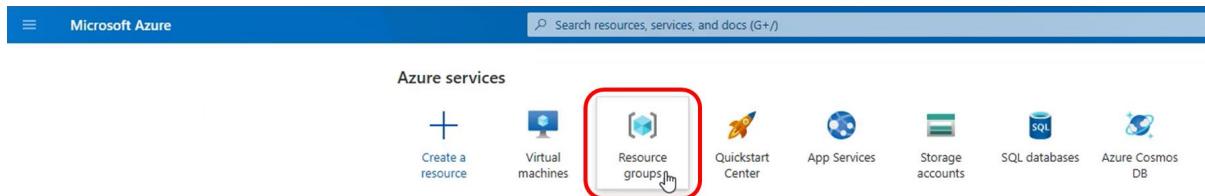
- ▶ Task 6 - Configure Workload subnet UDR

Task 6 - Configure Workload subnet UDR

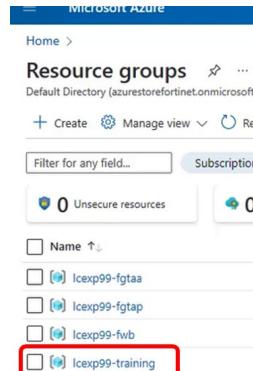
The next step is the creation and configuration of the user defined route to force the traffic destined to the Internet from the workload DMZ subnet to go out via the FortiGate firewalls.

Creation and configuration steps

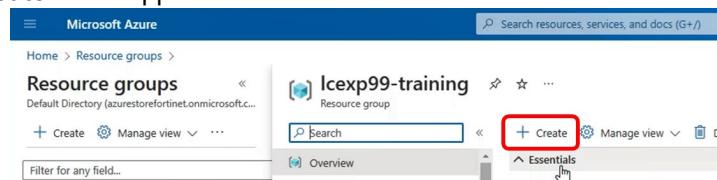
1. From the main Azure Portal, click on **Resource groups**



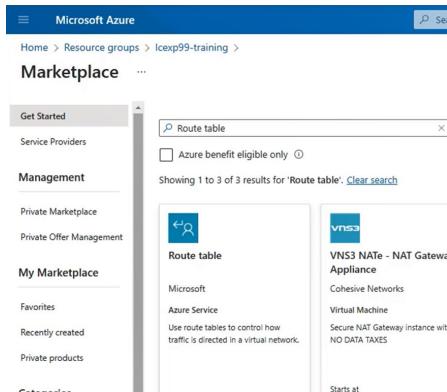
2. Click on the **Icexp<your student number>-training** resource group name itself to open a new pane on the right.



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

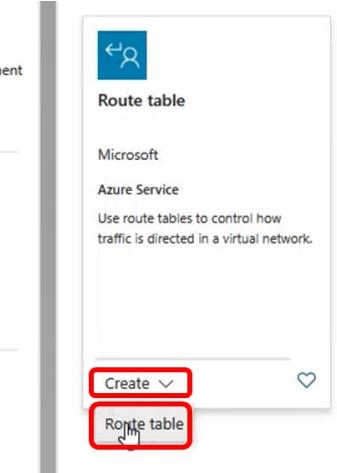


4. In the Marketplace pane, search for **Route Table**



▶ Task 6 - Configure Workload subnet UDR

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

The screenshot shows the 'Create Route table' wizard in the Azure portal. The 'Name' field (containing 'workload-ROUTETABLE') and the 'Propagate gateway routes' field (set to 'No') are both highlighted with a red box.

Microsoft Azure

Home > Resource groups > Icexp99-training > Marketplace > Create Route table

Basics Tags Review + create

Project details

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

Subscription * FTNT-Training

Resource group * Icexp99-training

Instance details

Region * East US

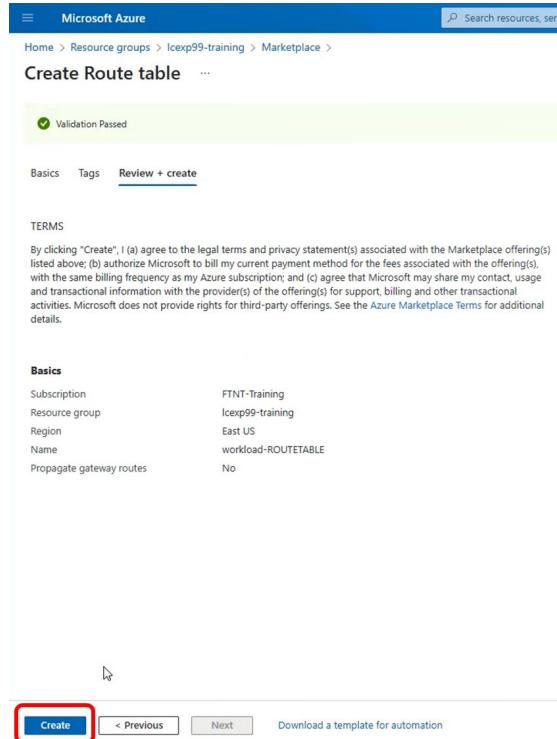
Name * workload-ROUTETABLE

Propagate gateway routes * Yes 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

► Task 6 - Configure Workload subnet UDR

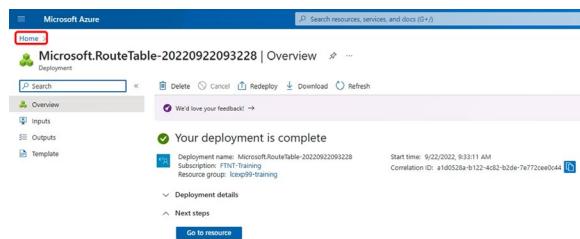
9. Click on **Create** after confirming the information entered.



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

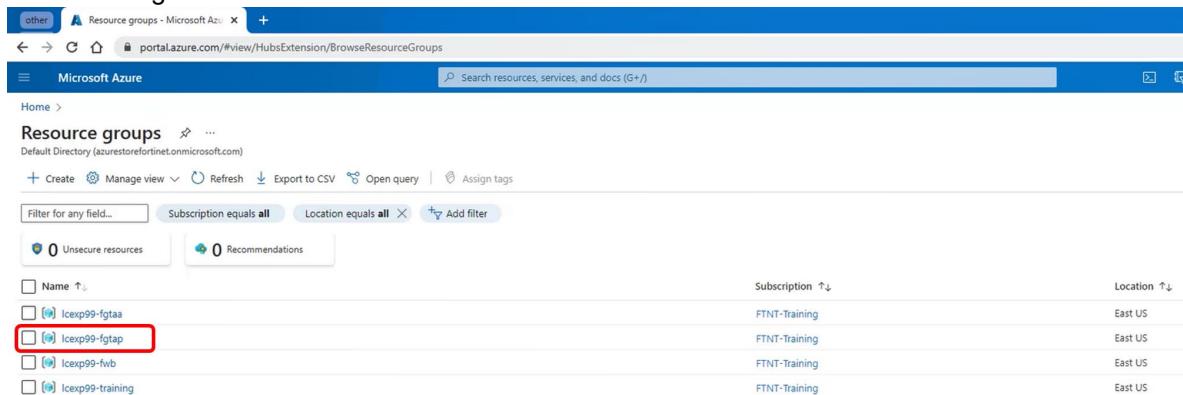


12. Click on **Resource groups**



► Task 6 - Configure Workload subnet UDR

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



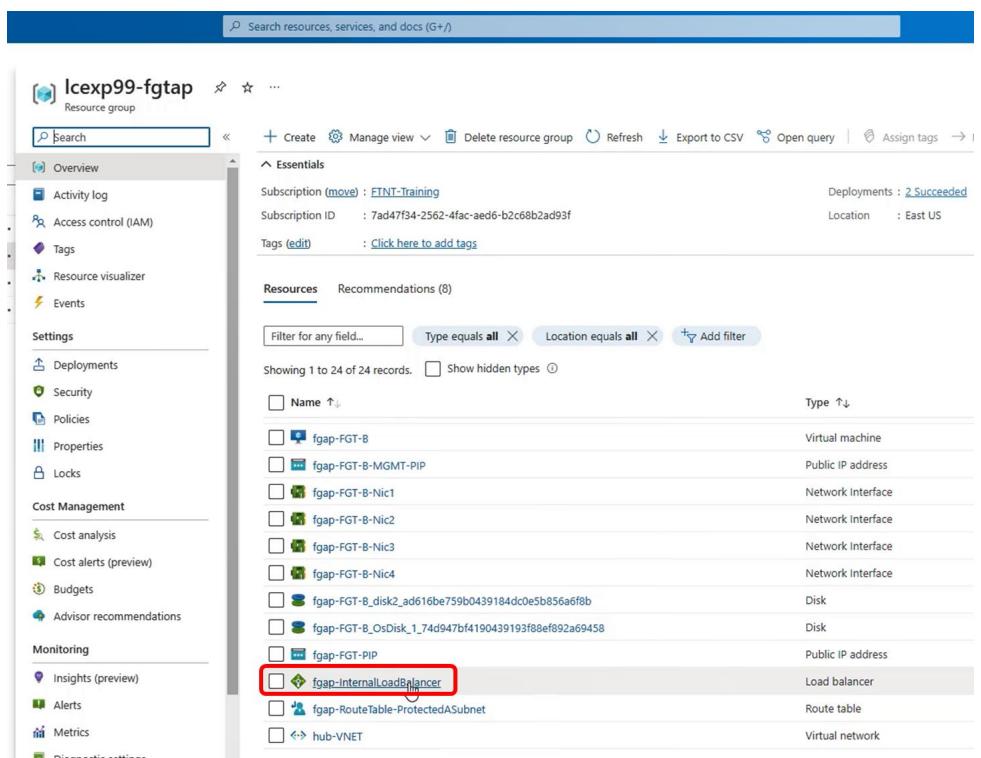
The screenshot shows the Microsoft Azure Resource groups page. The URL is <https://portal.azure.com/#view/HubsExtension/BrowseResourceGroups>. The search bar at the top contains "Search resources, services, and docs (G+)".

The main area displays a table of resource groups:

	Subscription	Location
Icexp99-fgtap	FTNT-Training	East US
Icexp99-fgtap	FTNT-Training	East US
Icexp99-fwb	FTNT-Training	East US
Icexp99-training	FTNT-Training	East US

A red box highlights the "Icexp99-fgtap" row, indicating it is selected.

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



The screenshot shows the Microsoft Azure Resource group "Icexp99-fgtap" overview page. The URL is <https://portal.azure.com/#resource/Icexp99-fgtap>. The search bar at the top contains "Search resources, services, and docs (G+)".

The left sidebar shows the navigation menu for the resource group:

- Overview
- Activity log
- Access control (IAM)
- Tags
- Resource visualizer
- Events
- Settings

 - Deployments
 - Security
 - Policies
 - Properties
 - Locks

- Cost Management

 - Cost analysis
 - Cost alerts (preview)
 - Budgets
 - Advisor recommendations

- Monitoring

 - Insights (preview)
 - Alerts
 - Metrics

- Diagnostic settings

The main content area shows the "Resources" section. A red box highlights the "fgap-internalLoadBalancer" item in the list of resources.

Name	Type
fgap-FGT-B	Virtual machine
fgap-FGT-B-MGMT-PIP	Public IP address
fgap-FGT-B-Nic1	Network interface
fgap-FGT-B-Nic2	Network interface
fgap-FGT-B-Nic3	Network interface
fgap-FGT-B-Nic4	Network interface
fgap-FGT_B_disk2_ada16be759b0439184dc0e5b856a6f8b	Disk
fgap-FGT_B_OsDisk_1_74d947bf4190439193f88ef892a69458	Disk
fgap-FGT-PIP	Public IP address
fgap-internalLoadBalancer	Load balancer
fgap-RouteTable-ProtectedASubnet	Route table
hub-VNET	Virtual network

► Task 6 - Configure Workload subnet UDR

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

The screenshot shows the 'Settings' section of the load balancer's configuration. The 'Frontend IP configuration' option is highlighted with a red box and labeled '1'.

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

The screenshot shows the 'Frontend IP configuration' details page. The assigned IP address '10.1.2.4' is highlighted with a red box and labeled '2'.

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

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

The screenshot shows the 'Resource groups' page. The 'Icxp99-training' resource group is selected and highlighted with a red box.

► Task 6 - Configure Workload subnet UDR

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

The screenshot shows the Azure Resource Group Overview page for the 'Icexp99-training' group. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings (Deployments, Security, Policies, Properties, Locks), Cost Management (Cost analysis, Cost alerts (preview), Budgets, Advisor recommendations), Monitoring (Insights (preview), Alerts, Metrics), and Metrics. The right pane displays a list of resources with a search bar at the top. A route table named 'workload-ROUTETABLE' is visible in the list, with its name highlighted by a red box.

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

The screenshot shows the 'workload-ROUTE' Route table page. The left sidebar includes Overview, Activity log, Access control (IAM), Tags, and a 'Routes' link, which is highlighted with a red box. The main pane features a search bar and a list of routes.

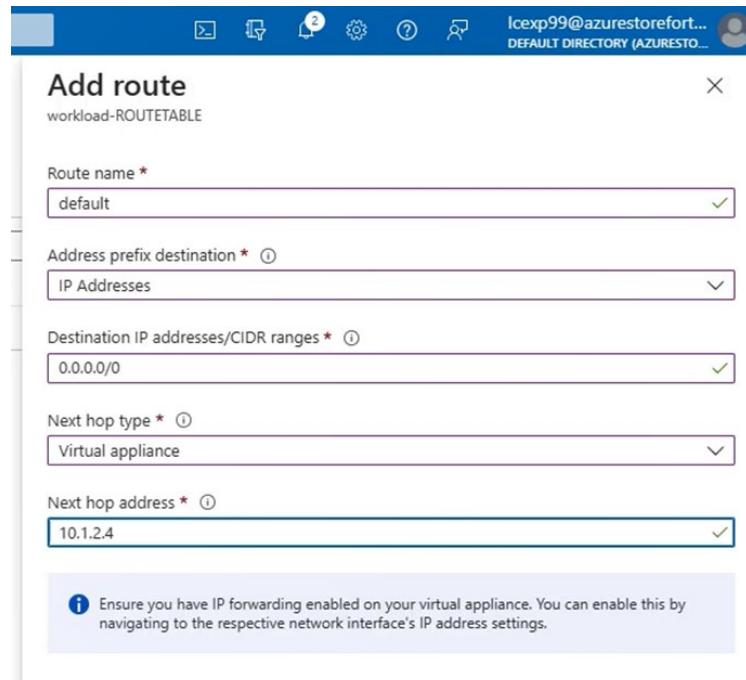
21. In the right pane, click on + Add

The screenshot shows the 'workload-ROUTETABLE | Routes' page. The top navigation bar includes a search bar and a '+ Add' button, which is highlighted with a red box. The main pane contains a search bar for routes and a table with one row.

▶ 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**

The screenshot shows the 'workload-ROUTETABLE | Subnets' blade. On the right side, there is a section titled '+ Associate' with a red box around it. Below it is a search bar labeled 'Search subnets' and a table with one row showing 'No results.'

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

The screenshot shows the 'Associate subnet' dialog box. It has two dropdown menus: 'Virtual network' set to 'workload-VNET' and 'Subnet' set to 'DMZ-Protected-A'. Both dropdowns are highlighted with a red box.

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

The screenshot shows the 'Associate' blade again. It lists a single subnet entry: 'Name' is 'DMZ-Protected-A', 'Address range' is '10.3.0.0/24', and 'Virtual network' is 'workload-VNET'. The 'Subnets' tab is currently selected.

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



30. Click on **Resource groups**

The screenshot shows the 'Resources' page in the Azure portal. In the center, there is a grid of icons for various services. The 'Resource groups' icon, which looks like a folder with a question mark, is highlighted with a red box.

► Task 6 - Configure Workload subnet UDR

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

The screenshot shows the Microsoft Azure Resource Groups page. At the top, there's a blue header bar with the Microsoft Azure logo. Below it, the URL 'https://portal.azure.com/#blade/HubsBlade/resourceType/resourceGroups/resourceGroup/Icexp99-training' is visible. The main title is 'Resource groups'. Underneath, it says 'Default Directory (azurerestoreforinet.onmicrosoft.com)'. There are buttons for '+ Create', 'Manage view', and 'Ref'. A search bar says 'Filter for any field...' and a dropdown says 'Subscription'. Below that, there are two boxes: 'Unsecure resources' (0) and 'Secure resources' (0). A table lists four resources: 'Icexp99-fgtaa', 'Icexp99-fgtap', 'Icexp99-fwb', and 'Icexp99-training'. The last item, 'Icexp99-training', is highlighted with a red rectangle.

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.

The screenshot shows the 'Icexp99-training' resource group details page. On the left, there's a sidebar with 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Resource visualizer', and 'Events'. Under 'Settings', there are 'Deployments', 'Security', 'Policies', 'Properties', 'Locks', and 'Cost Management'. The main area has tabs for 'Essentials' and 'Resources'. The 'Resources' tab is selected, showing 'Recommendations (9)'. A filter bar at the top of the list allows filtering by 'Name', 'Type', and 'Location'. The list shows 11 items, with 'dvwa450' highlighted with a red rectangle. The details for 'dvwa450' are shown on the right: Type is 'Network interface', and it's associated with 'Virtual machine' 'dvwa' and 'Network security group' 'dvwa-nsg'.

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

This screenshot shows the 'dvwa450' network interface settings page. The left sidebar has sections for 'Monitoring' (Insights, Alerts, Metrics, Diagnostic settings), 'Automation' (Tasks (preview), Export template), and 'Help' (Effective security rules, Effective routes, New Support Request). The 'Effective routes' link is highlighted with a red box and the number '1'.

▶ Task 6 - Configure Workload subnet UDR

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

routes ⚡ ⭐ ...

Download Refresh Give feedback

Showing only top 200 records, click Download above to see all.

Scope	Network interface (dvwa450)									
Associated route table: ⓘ	workload-ROUTETABLE									
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		Invalid		0.0.0.0/0		Internet		-		-
User		Active		0.0.0.0/0		Virtual appliance		10.1.2.4		default

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



36. Click on **Resource groups**



► Task 6 - Configure Workload subnet UDR

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

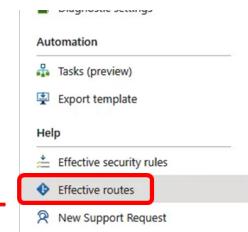
The screenshot shows the Microsoft Azure Resource Groups page. At the top, there's a navigation bar with 'Microsoft Azure' and a 'Home' link. Below it is a 'Resource groups' section with a 'Default Directory (azurerestorefortinet.onmicrosoft.com)' dropdown, a 'Create' button, and a 'Manage view' dropdown. There are also 'Subscription' and 'Filter for any field...' buttons. Under the 'Resource groups' heading, there are two sections: 'Unsecure resources' (0) and 'Secure resources' (0). A red box highlights the 'Icexp99-training' entry under the 'Secure resources' section.

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

The screenshot shows the Microsoft Azure Resource Groups page with the 'linuxssh' resource group selected. The left sidebar has 'Essentials' expanded, showing 'Subscription (move) : FTNT-Training', 'Subscription ID : 7ad47f34-2562-4fac-aed6-b2c68b2ad93f', and 'Tags (edit) : Click here to add tags'. The main pane shows a list of resources under 'Resources' with 'Recommendations (9)' below it. A filter bar at the top of the list allows filtering by 'Name', 'Type', and 'Location'. The list shows 11 records, with the 'linuxssh' entry highlighted in grey. A red box highlights the 'linuxssh645' entry in the list, which is the specific network interface being referred to in the task.

▶ 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

routes ⚡ ⭐ ...

The screenshot shows a table titled 'Effective routes' with the following columns: Source, ↑↓, State, ↑↓, Address Prefixes, ↑↓, Next Hop Type, ↑↓, Next Hop IP Address, ↑↓, User Defined Route Name, and ↑↓. The rows are:

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		Invalid		0.0.0.0/0		Internet		-		-	
User		Active		0.0.0.0/0		Virtual appliance		10.1.2.4		default	

41. The user defined route has been deployed successfully

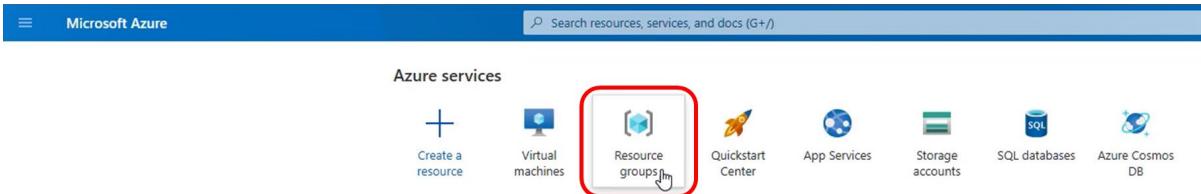
► Task 7 - Configure FortiGate Active Passive

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.

A screenshot of the "Resource groups" page in the Azure portal. The title bar says "Resource groups". Below it, there are buttons for "+ Create", "Manage view", "Refresh", and "Subscription equals all". A search bar says "Filter for any field...". There are two sections: "Unsecure resources" (0) and "Recommen" (0). The main list shows three resource groups: "lcexp99-fgtap" (selected and highlighted with a red box), "lcexp99-fvb", and "lcexp99-training".

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

A screenshot of the "Resource groups" page for the "lcexp99-fgtap" group. The title bar says "lcexp99-fgtap". The main content area shows the "Essentials" section with "Subscription (move)" set to "FTNT-Training", "Subscription ID" as "7ad47f34-2562-4fac-aed6-b2c68b2ad93f", "Tags (edit)" as "Click here to add tags", "Deployments" as "2 Succeeded", and "Location" as "East US". Below this is a "Resources" table with a filter bar at the top. The table lists 24 records, including "consoleafzgbv44lhvo4", "fgap-afzgbv44lhvo4-NSG", "fgap-AvailabilitySet", "fgap-ExternalLoadBalancer", "fgap-FGT-A" (selected and highlighted with a red box), and "fgap-FGT-A-Nic1". The columns show the resource name, type (e.g., Storage account, Network security group, Availability set, Load balancer, Virtual machine, Public IP address, Network interface), and status.

► Task 7 - Configure FortiGate Active Passive

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

Resource group (move) : lcexp99-fgtap

Location : East US

Subscription (move) : FTNT-Training

Subscription ID : 7ad47f34-2562-4fac-aed6-b2c68b2ad93f

SKU : Standard

Tier : Regional

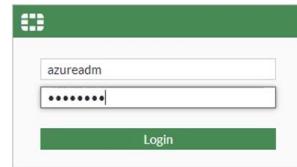
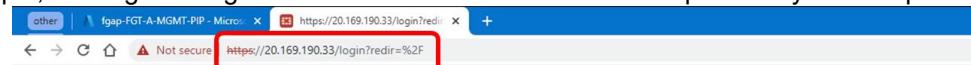
IP address : 20.169.190.33

DNS name : -

Associated to : fgap-FGT-A-Nic4

Tags (edit) : provider : 6EB3B02F-50E5-4A3E-8CB8-2E12925831AP

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

Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags

Subscription (move) : FTNT-Training

Subscription ID : 7ad47f34-2562-4fac-aed6-b2c68b2ad93f

Location : East US

Tags (edit) : Click here to add tags

Resources Recommendations (8)

Name Type

- fgap-FGT-B Virtual machine
- fgpa-FGT-B-MGMT-PIP Public IP address
- fgap-FGT-B-Nic1 Network Interface
- fgap-FGT-B-Nic2 Network Interface

► Task 7 - Configure FortiGate Active Passive

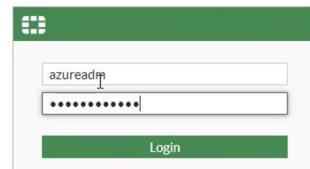
8. Make note of the public IP address of the management interface of FortiGate fgap-FGT-B, 20.169.207.186 in this example

The screenshot shows the FortiGate Management interface. At the top, there are buttons for Associate, Dissociate, Move, Delete, and Refresh. Below that is a section titled 'Essentials' with the following details:

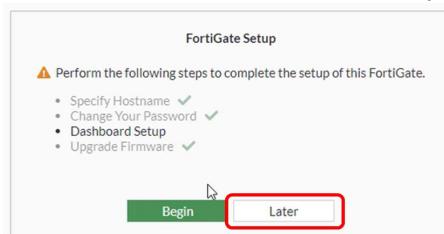
- Resource group (move) : lcepx99-fotap
- Location : East US
- Subscription (move) : FTNT-Training
- Subscription ID : 7ad47f34-2562-4fac-aed6-b2c68b2ad93f
- SKU : Standard
- Tier : Regional
- IP address : 20.169.207.186 (highlighted with a red box)
- DNS name : -
- Associated to : fgap-FGT-B-Nic4

At the bottom, there is a 'Tags (edit)' section with a provider tag: 6EB3B02F-50E5-4A3E-8CB8-2E12925831AP.

9. Open another new web browser tab to 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**

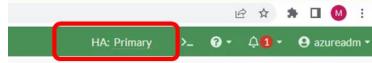


11. Dismiss the subsequent prompt as well by clicking **OK**

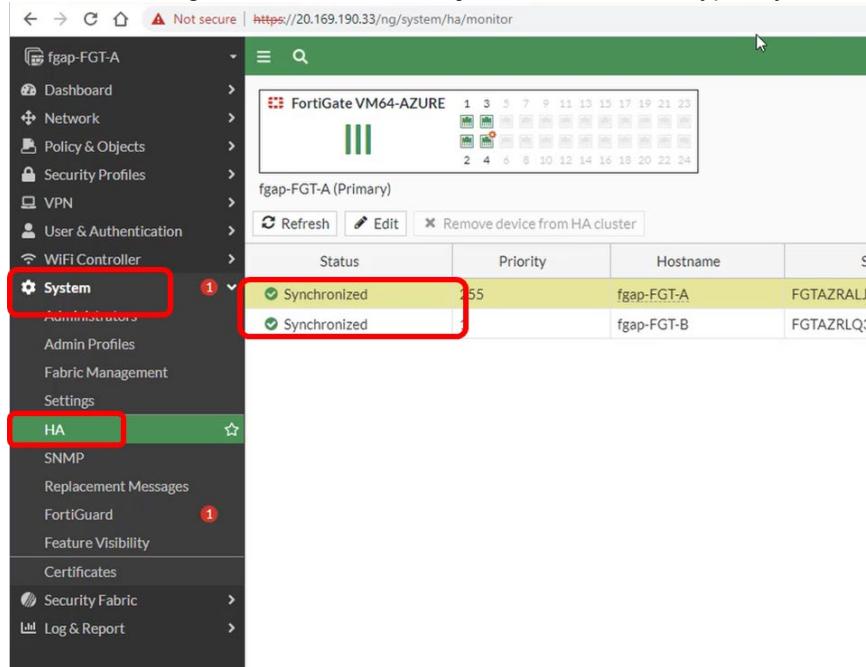


► Task 7 - Configure FortiGate Active Passive

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

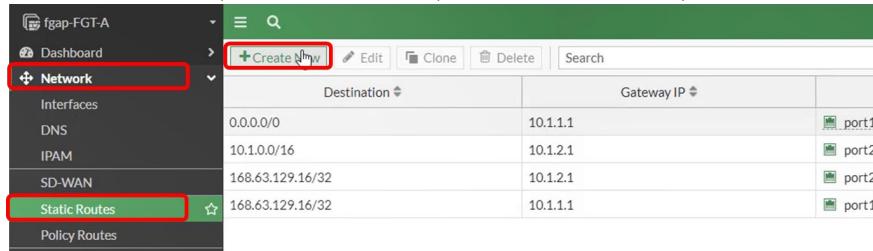


13. In the left FortiGate menu of the primary FortiGate, click on **System** and then on **HA**, ensure that both FortiGate are showing under the status of **Synchronized**. This typically takes 5 minutes.



Status	Priority	Hostname	
Synchronized	255	fgap-FGT-A	FGTAZRALJ
Synchronized	255	fgap-FGT-B	FGTAZRLQ;

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

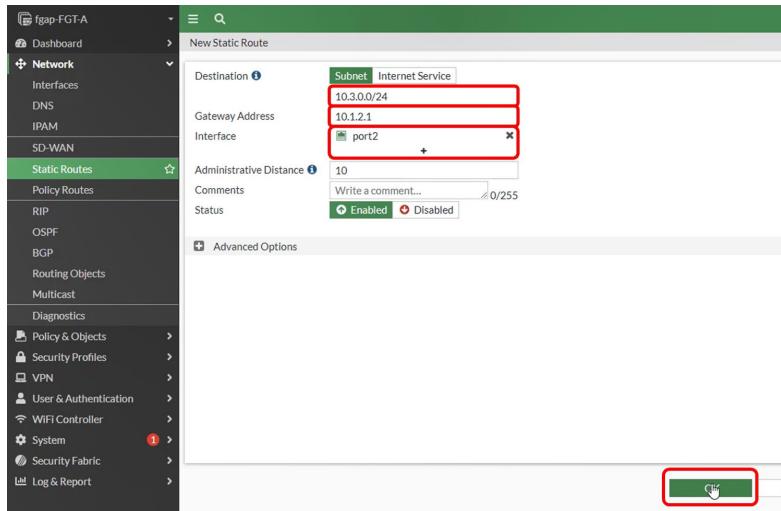


Destination	Gateway IP	
0.0.0.0/0	10.1.1.1	port1
10.1.0.0/16	10.1.2.1	port2
168.63.129.16/32	10.1.2.1	port2
168.63.129.16/32	10.1.1.1	port1

► Task 7 - Configure FortiGate Active Passive

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

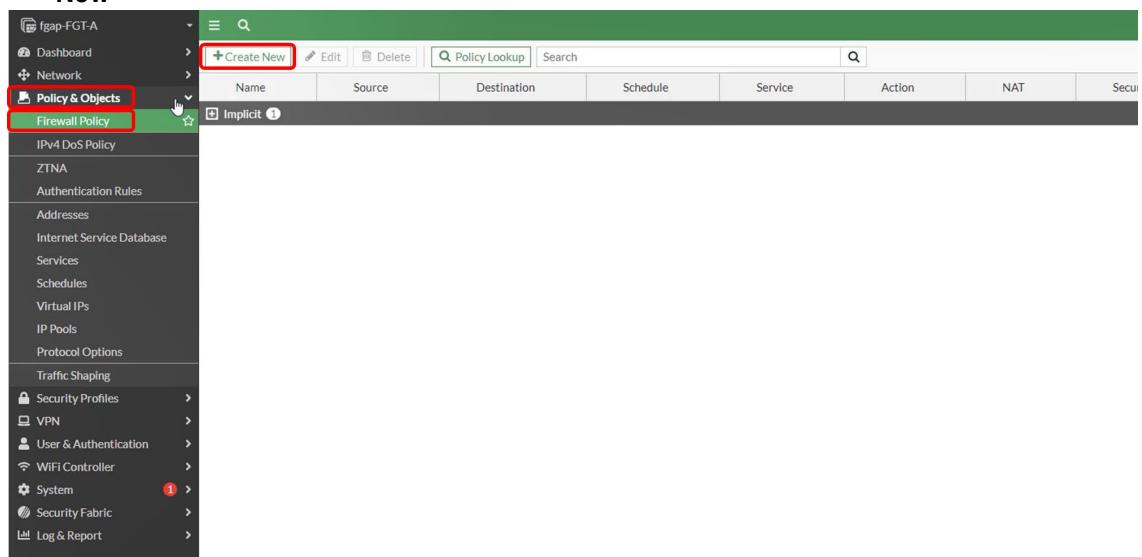
Destination	Subnet 10.3.0.0/24
Gateway Address	10.1.2.1
Interface	port2



16. Confirm the routing entries with the screen below

Destination	Gateway IP	Interface	Status
0.0.0.0/0	10.1.1.1	port1	Enabled
10.1.0.0/16	10.1.2.1	port2	Enabled
168.63.129.16/32	10.1.2.1	port2	Enabled
168.63.129.16/32	10.1.1.1	port1	Enabled
10.3.0.0/24	10.1.2.1	port2	Enabled

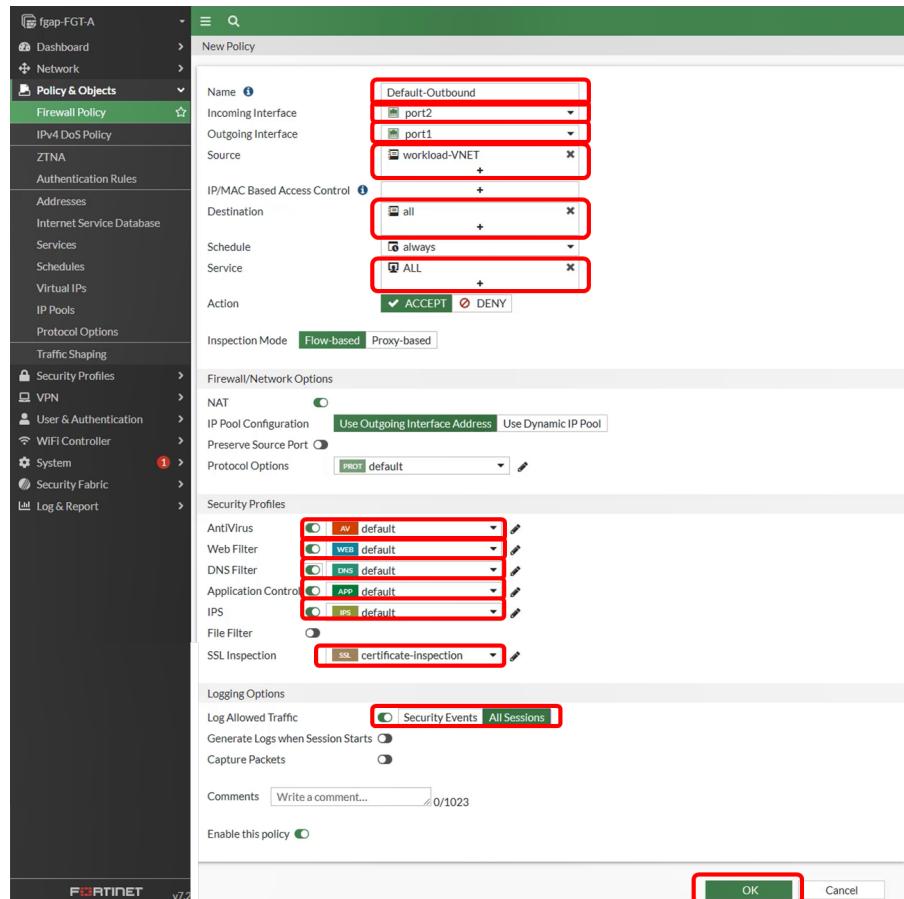
17. In the same FortiGate menu, click on **Policy and Objects**, then **Firewall Policy**, then **+ Create New**



► Task 7 - Configure FortiGate Active Passive

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

The screenshot shows the FortiGate management interface under the 'Policy & Objects' section, specifically the 'Firewall Policy' tab. A policy named 'Default-Outbound' is selected. A tooltip is displayed over the 'Source' field, which contains the value 'workload-VNET'. The tooltip details the source configuration: Address 'workload-VNET', Type 'Subnet', Subnet '10.30.0/24', and Interface 'any'. The policy itself has the following settings: Source 'workload-VNET', Destination 'all', Schedule 'always', Service 'ALL', Action 'ACCEPT', NAT 'Enabled', Security Profiles (AV default, WEB default, DNS default, APP default, IPS default, SSL certificate-inspection), Log 'All', and Bytes '0 B'. The policy is marked as 'Implicit'.

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

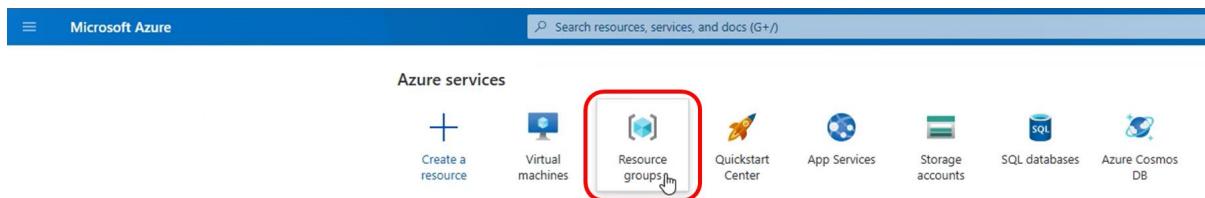
- ▶ Task 8 – Confirm VM outbound access

Task 8 – Confirm VM outbound access

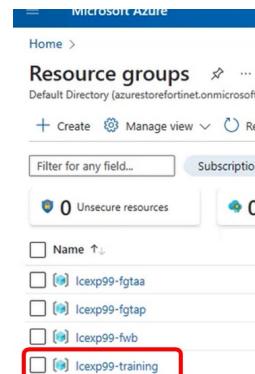
The next step is the confirmation of the traffic destined to the Internet from the VMs in the workload DMZ subnet to go out via the FortiGate FGAP firewalls located in the outbound VNET.

Creation and configuration steps

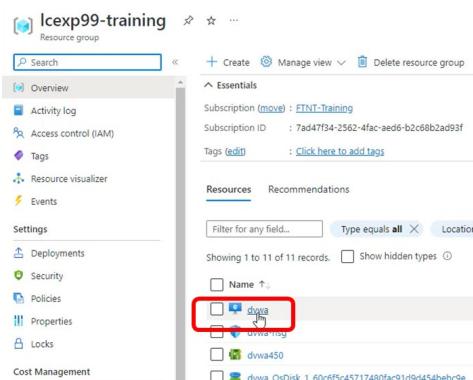
1. From the main Azure Portal, click on **Resource groups**



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

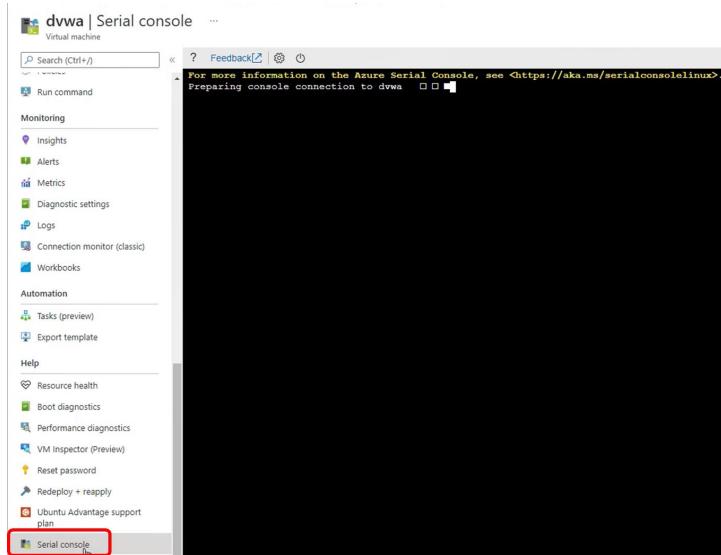


3. In the right pane, click on the name of the dvwa Virtual Machine



► 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 (**azureadadm** and the chosen password)

```
[ OK ] Started Snap Daemon.  
Starting Wait until snapd is fully seeded...  
Starting Time & Date Service.  
[ OK ] Started Time & Date Service.  
[ OK ] Finished Wait until snapd is fully seeded.  
Starting Apply the settings specified in cloud-config...  
[ OK ] Finished Service for snap application lxd.activate.  
[ 24.857292] cloud-init[1108]: Cloud-init v. 22.2-0ubuntu1~20.04.3 running 'modules:config'  
[ 25.357785] cloud-init[1122]: Cloud-init v. 22.2-0ubuntu1~20.04.3 running 'modules:final'  
[ 25.357944] cloud-init[1122]: Cloud-init v. 22.2-0ubuntu1~20.04.3 finished at Thu, 22 Sep  
ds  
Ubuntu 20.04.5 LTS dwww ttyS0  
2022-09-22T13:26:00.236652Z INFO Daemon Agent WSLinuxAgent-2.0.0.11 launched with command '  
dwww login:  
dwww login:  
dwww login:  
dwww login: azureadadm  
Password:
```

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

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

```
Last login: Mon Sep 12 20:38:27 UTC 2022 on ttys0  
root@dot:~$ azureadadm@dvwa:~$  
azureadadm@dvwa:~$ curl http://www.fortinet.com  
<head><title>Object moved</title></head><body><h1>Object Moved</h1></body>azureadadm@dvwa:~$
```

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

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
2022/10/13 10:15:55	10.3.0.4		44.199.160.6	HTTPBROWSER	✓ Accept (UTM Allowed)	Default-Outbound
2022/10/13 10:15:29	10.3.0.4		91.189.91.49	HTTPS.BROWSER	✓ Accept (UTM Allowed)	Default-Outbound
2022/10/13 10:14:48	10.3.0.4		54.247.62.1	HTTPS.BROWSER	✓ Accept (UTM Allowed)	Default-Outbound
2022/10/13 10:14:36	10.3.0.5		3.91.211.14	HTTPBROWSER	✓ Accept (UTM Allowed)	Default-Outbound

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

Default-Outbound	workload-VNET	all	always	ALL	ACCEPT	Enabled	default	WEB	DNS	APP	IPS	SSE	certificate-inspection	All	21.94 KB

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 Icexp<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

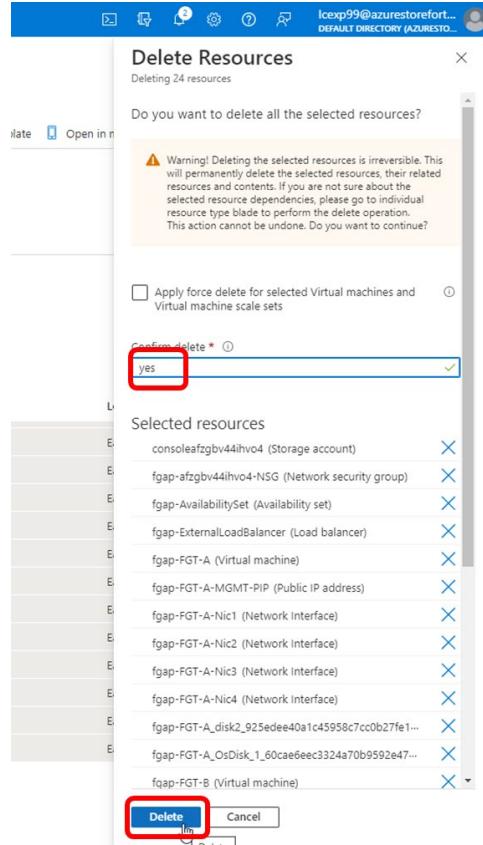
The screenshot shows the Azure Resource Group Overview page for 'Icexp99-fgtap'. On the left, there's a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Deployments, Security, Policies, Properties, and Logs. The main area displays a table of resources under the 'Resources' tab. The first column is 'Name', which has a red box around its header. Below the table, there are filters and a message saying 'Showing 1 to 24 of 24 records.' At the top right, there are buttons for Create, Manage view, Delete reso, and other actions.

14. Click on Delete on the top menu

The screenshot shows the same Azure Resource Group Overview page as the previous one, but now the 'Delete' button in the top right menu bar is highlighted with a red box. A tooltip above the button says 'Run the 'Delete' command on the selected resources'. Other buttons in the top menu include Create, Manage view, Refresh, Export to CSV, Open query, Assign tags, Move, and Export template.

► 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

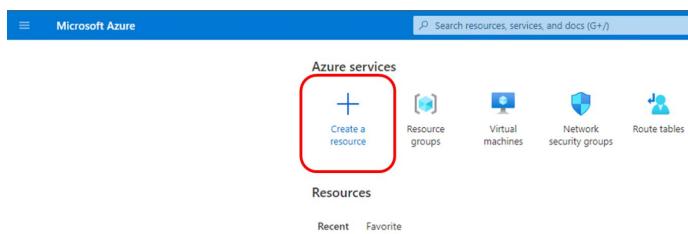
► Task 9 - Deploy FortiGate Active-Active

Task 9 - Deploy FortiGate Active-Active

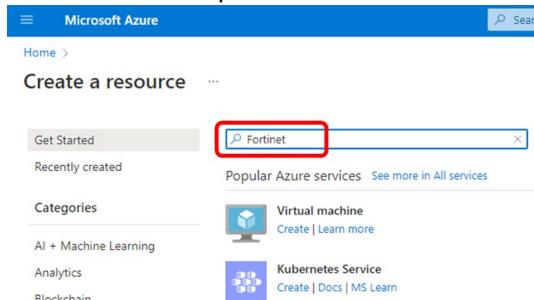
The next step is the deployment of the of the FortiGate firewalls (in Active-Active) along with associated network resources including the virtual network for the Internet Ingress Hub.

Deployment steps

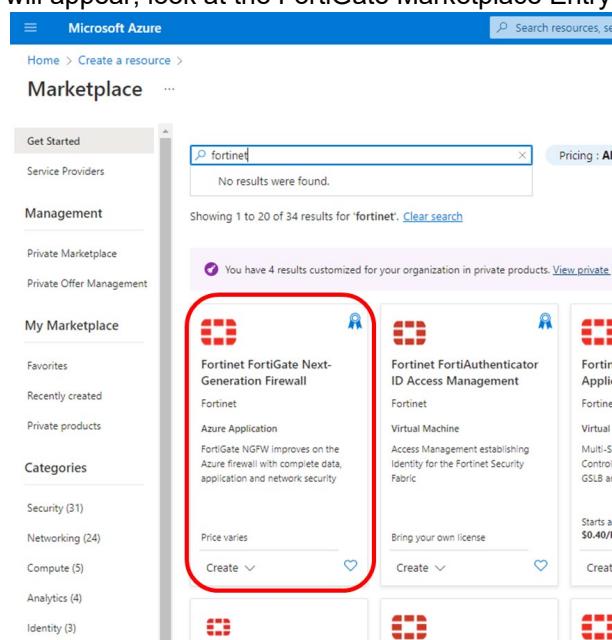
1. From the main Azure Portal, click on **Create a resource**



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



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



► Task 9 - Deploy FortiGate Active-Active

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

The screenshot shows the Microsoft Azure Marketplace interface. The search bar at the top contains the text "fortinet". Below the search bar, there is a checkbox labeled "Azure benefit eligible only". The results section displays 20 of 34 items found for "fortinet". The first item listed is "Fortinet FortiGate Next-Generation Firewall" by Fortinet, categorized as an "Azure Application". The second item is "Fortinet FortiAuthenticator ID Access Management" by Fortinet, categorized as a "Virtual Machine". The third item, which is highlighted with a red box, is "Active-Active Loadbalanced with ELB/ILB" by Fortinet, categorized as a "Web Web". This item has a "Create" button, also highlighted with a red box. Other visible items include "Active-Passive HA with Fabric Connector Failover" and "FortiWeb Web". The left sidebar contains navigation links for "Get Started", "Service Providers", "Management", "Private Marketplace", "Private Offer Management", "My Marketplace", "Favorites", "Recently created", "Private products", and "Categories" (Security, Networking, Compute, Analytics, Identity, IT & Management Tools, Web, Developer Tools, Internet of Things, Monitoring & Diagnostics, AI + Machine Learning).

▶ Task 9 - Deploy FortiGate Active-Active

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

Subscription	FTNT-Training
Resource group	Icexp<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

Create Fortinet FortiGate Next-Generation Firewall ...

Basics Instance Type Networking Public IP Public IP Verification Advanced Review + create

Project details

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

Subscription * ⓘ FTNT-Training

Resource group * ⓘ Icexp99-fgtaa

Create new

Instance details

Region * ⓘ East US

FortiGate Deployment Type - Active/Active - External and Internal Load Balancers - Availability Set or Availability Zones ⓘ

FortiGate administrative username * ⓘ azureadm ✓

FortiGate password * ⓘ ✓

Confirm password * ⓘ ✓

FortiGate Name Prefix * ⓘ fgaa ✓

FortiGate Image SKU ⓘ Pay As You Go ✓

FortiGate Image Version ⓘ Latest ✓

FortiGate Availability Options ⓘ Availability Set ✓

► Task 9 - Deploy FortiGate Active-Active

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
-------------	------------------------

Create Fortinet FortiGate Next-Generation Firewall ...

Basics Instance Type Networking Public IP Public IP Verification Advanced Review + create

For this FortiGate deployment, it is recommended to use the general purpose or compute optimized virtual machines. A selection of supported instances sizes is listed in our documentation.
[Learn more](#)

Size * ⓘ **2x Standard F2s**
2 vcpus, 4 GB memory
[Change size](#)



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

Create Fortinet FortiGate Next-Generation Firewall ...

Basics Instance Type **Networking** Public IP Public IP Verification Advanced Review + create

Configure Internal Networking

Create a new or select an existing virtual network with the required subnets. The internal subnet is a transit subnet containing only the FortiGate interfaces. Servers can be installed in a protected subnet with user defined routing configuration.

Configure virtual networks

Virtual network * ⓘ **(new) fortigateVNET**

External Subnet * ⓘ **(new) ExternalSubnet (10.0.0.0/26)**

Internal subnet * ⓘ **(new) InternalSubnet (10.0.1.0/26)**

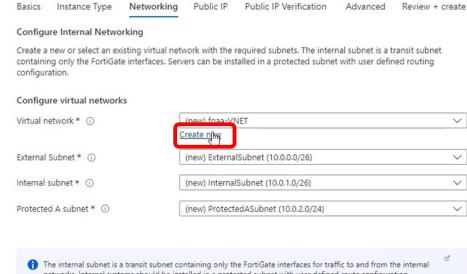
Protected A subnet * ⓘ **(new) ProtectedASubnet (10.0.2.0/24)**

ⓘ The internal subnet is a transit subnet containing only the FortiGate interfaces for traffic to and from the internal networks. Internal systems should be installed in a protected subnet with user defined route configuration.

Accelerated networking

Enables SR-IOV support allowing direct access from the NIC in the Azure infrastructure to the FortiGate VM.
[Learn more](#)

Accelerated Networking ⓘ Enabled Disabled



▶ Task 9 - Deploy FortiGate Active-Active

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

Create virtual network

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network which is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or your on-premises network.

Name * inbound-VNET

ADDRESS SPACE

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

Address range Addresses
10.2.0.0/16 10.2.0.0 - 10.2.255.255 (65536 addresses)

SUBNETS

The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.

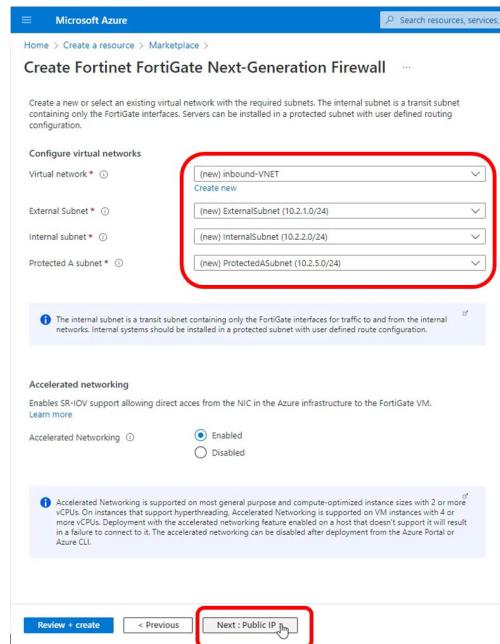
Subnet name	Address range	Addresses
ExternalSubnet	10.2.1.0/24	10.2.1.0 - 10.2.1.255 (256 addresses)
InternalSubnet	10.2.2.0/24	10.2.2.0 - 10.2.2.255 (256 addresses)
ProtectedASubnet	10.2.5.0/24	10.2.5.0 - 10.2.5.255 (256 addresses)

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



► Task 9 - Deploy FortiGate Active-Active

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



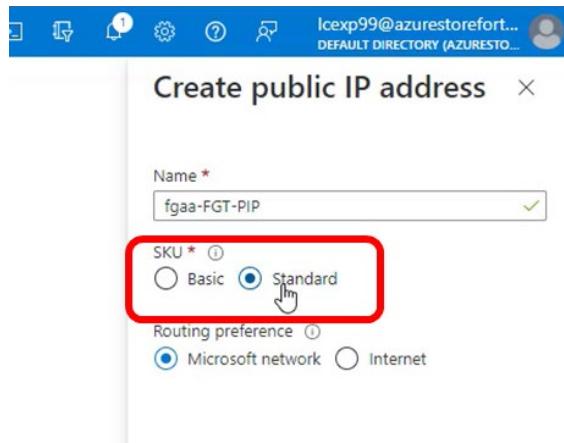
► Task 9 - Deploy FortiGate Active-Active

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

Create Fortinet FortiGate Next-Generation Firewall ...



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

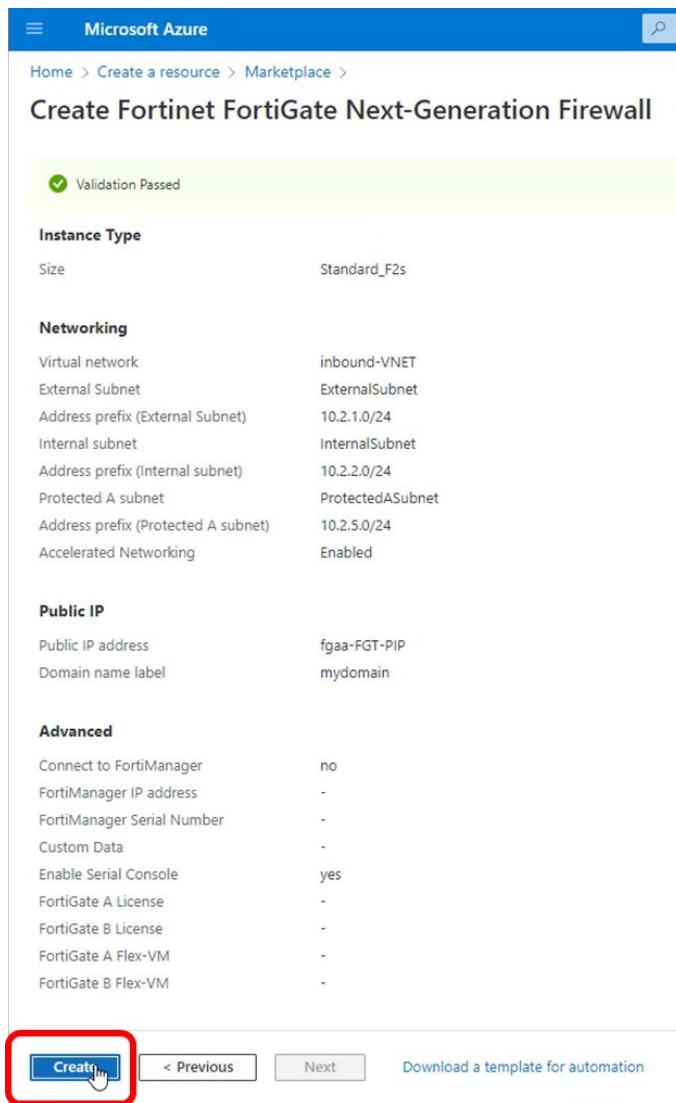


17. Click on **Next: Advanced** at the bottom, there is nothing to change in the Advanced pane

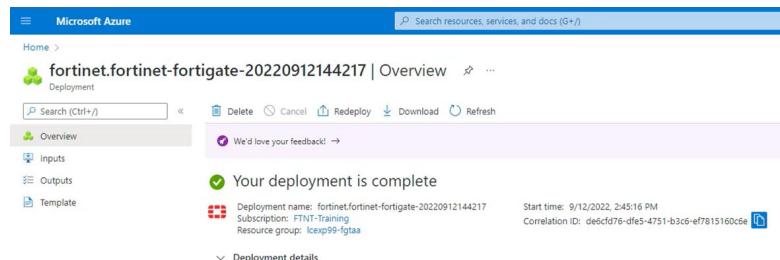
18. Click on **Next: Review + create** at the bottom

► Task 9 - Deploy FortiGate Active-Active

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



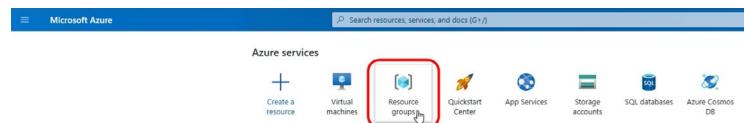
20. This template deploys several resources, expect 5 minutes for the deployment to complete



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.

► Task 9 - Deploy FortiGate Active-Active

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.

Resource groups

Default Directory

+ Create Manage view ↗

Filter for any field... Si

0 Unsecure resources

Name ↑↓

[?] lcexp99-fgtaa

[?] lcexp99-fw

[?] lcexp99-training

► Task 9 - Deploy FortiGate Active-Active

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

The screenshot shows the Azure portal interface for the resource group 'Icexp99-fgtaa'. On the left, there's a navigation menu with sections like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, and Metrics. The main area displays a list of resources under the 'Resources' tab. A red box highlights the entry 'fgaa-RouteTable-ProtectedASubnet' in the list.

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

The screenshot shows the 'fgaa-RouteTable-ProtectedASubnet' blade in the Azure portal. The left sidebar has links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration, Routes, Subnets (which is highlighted with a red box), Properties, and Locks. The main content area shows a table with columns for Name, IP address range, and Subnet ID. A search bar at the top right says 'Search subnets'.

► Task 9 - Deploy FortiGate Active-Active

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

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

fgaa > fgaa-RouteTable-ProtectedASubnet

RouteTable-ProtectedASubnet | Subnets ⚡ ⋮

Associate

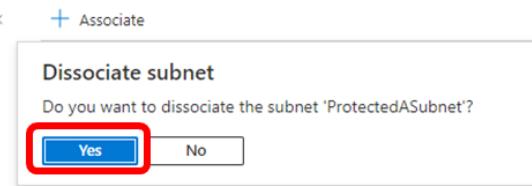
Search subnets

Name ↑↓	Address range ↑↓	Virtual network ↑↓
ProtectedASubnet	10.2.5.0/24	inbound-VNET

Live problems

27. Confirm by clicking on Yes

fgaa-ProtectedASubnet | Subnets ⚡ ⋮



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

Microsoft Azure Search resources, services, and docs

Home > Icexp99-fgaa > fgaa-RouteTable-ProtectedASubnet

fgaa-RouteTable-ProtectedASubnet | Subnets ⚡ ⋮

Route table

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

Associate

Search subnets

Name ↑↓	Address range ↑↓
No results.	

► Task 9 - Deploy FortiGate Active-Active

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

The screenshot shows the Azure Resource Group 'Icexp99-fgtaa' overview. The 'Resources' tab is selected, displaying a list of 18 resources. A red box highlights the 'fgaa-RouteTable-ProtectedASubnet' route table, which is listed as a Route table under Type, located in East US.

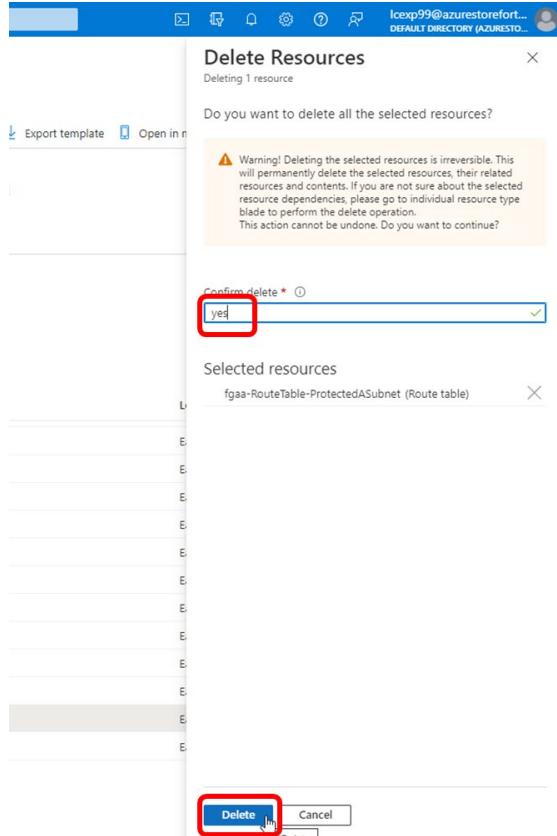
Name	Type	Location
fgaa-FGT-B	Virtual machine	East US
fgaa-FGT-B-Nic1	Network Interface	East US
fgaa-FGT-B-Nic2	Network Interface	East US
fgaa-FGT-B_disk2_baf239b790c243b381c...	Disk	East US
fgaa-FGT-B_OsDisk_1_8118a567158e4ccf...	Disk	East US
fgaa-FGT-PIP	Public IP address	East US
fgaa-InternalLoadBalancer	Load balancer	East US
fgaa-NSG-Allow-All	Network security group	East US
fgaa-RouteTable-ProtectedASubnet	Route table	East US
inbound-VNET	Virtual network	East US

30. Click on Delete on the top menu

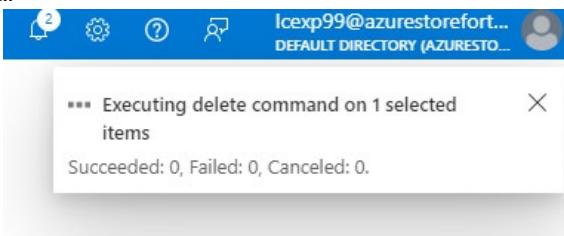
The screenshot shows the 'Delete' button highlighted in the top navigation bar of the Azure Resource Group 'Icexp99-fgtaa'. A tooltip indicates that clicking the 'Delete' button will run the 'Delete' command on the selected resources.

► Task 9 - Deploy FortiGate Active-Active

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



32. A notification will appear



33. Upon completion, the deployment is now complete

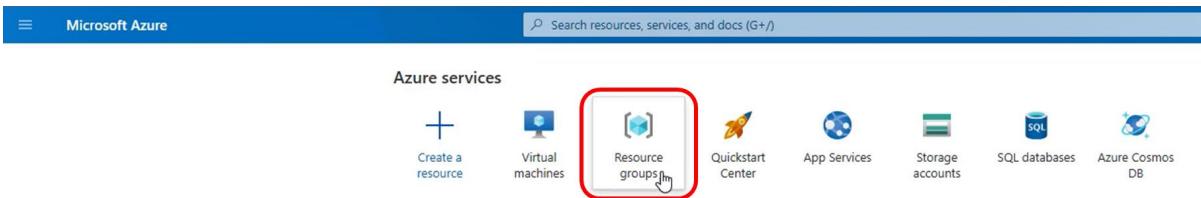
► Task 10 - Configure VNET Peering FGAA

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.

A screenshot of the Microsoft Azure portal showing the "Resource groups" page. The title bar says "Microsoft Azure" and "Home > Resource groups". There are filters for "Subscription equals all" and "Location equals all". The main list shows five resource groups: "lcexp99-fgtaa" (selected and highlighted with a red box and a cursor click), "lcexp99-iglap", "lcexp99-fwba", "lcexp99-training", and "lcexp99-fwba". Each item has a checkbox to its left.

► Task 10 - Configure VNET Peering FGAA

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

The screenshot shows the Azure Resource Group 'Icexp99-fgtaa' overview page. The 'Resources' tab is selected. A search bar at the top right contains the placeholder 'Search resources, services, and docs (G+ /)'. Below the search bar are buttons for '+ Create', 'Manage view', 'Delete resource group', 'Refresh', 'Export to CSV', 'Open query', and a help icon. The main area displays a list of resources with columns for Name, Type, and Status. The 'inbound-VNET' resource is highlighted with a red box.

Name	Type
fgaa-FGT-A_disk2_007821e80862436bab609138affb67a	Disk
fgaa-FGT-A_OsDisk_1_94a35b3296a54358a35e92c1eddef0bf	Disk
fgaa-FGT-B	Virtual machine
fgaa-FGT-B-Nic1	Network Interface
fgaa-FGT-B-Nic2	Network Interface
fgaa-FGT-B_disk2_6a2d0944feac408c8cadde6c45d9426c	Disk
fgaa-FGT-B_OsDisk_1_5076865bd8dc41c984e657836d6b7c94	Disk
fgaa-FGT-PIP	Public IP address
fgaa-InternalLoadBalancer	Load balancer
fgaa-NSG-Allow-All	Network security group
fgaa-RouteTable-ProtectedASubnet	Route table
inbound-VNET	Virtual network

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

The screenshot shows the 'Peering' section in the Virtual Network settings. The left sidebar lists various network-related features: Address space, Connected devices, Subnets, Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, Network manager, DNS servers, Peering (highlighted with a red box), Service endpoints, and Private endpoints. The right pane shows the 'Peering' configuration interface.

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

The screenshot shows the 'Peering' configuration page for the 'inbound-VNET' virtual network. The top navigation bar includes 'Home', 'Resource groups', 'Icexp99-fgtaa', and 'inbound-VNET'. The left sidebar has links for Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main area has a search bar and a '+ Add' button highlighted with a red box. Below the search bar are buttons for 'Refresh' and 'Sync'. A filter bar allows filtering by name and peering status. The bottom section has a message: 'Add a peering to get started'.

▶ Task 10 - Configure VNET Peering FGAA

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

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

Add peering ...

inbound-VNET

For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.

This virtual network

Peering link name * ✓

Traffic to remote virtual network ⓘ
 Allow (default)
 Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ
 Allow (default)
 Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ
 Use this virtual network's gateway or Route Server
 Use the remote virtual network's gateway or Route Server
 None (default)

Remote virtual network

Peering link name * ✓

Virtual network deployment model ⓘ
 Resource manager
 Classic

I know my resource ID ⓘ

Subscription * ⓘ ✓

Virtual network * ✓

Traffic to remote virtual network ⓘ
 Allow (default)
 Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ
 Allow (default)
 Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ
 Use this virtual network's gateway or Route Server
 Use the remote virtual network's gateway or Route Server
 None (default)

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:

	Peer	Peering status	Gateway transit
inbound-to-workload	workload-VNET	Connected	Disabled

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

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

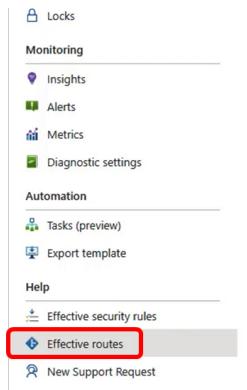
Name
Icexp99-fgtaa
Icexp99-fgtap
Icexp99-fwb
Icexp99-training

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

Name	Type
dvwa	Virtual machine
dvwa-nsg	Network security group
dvwa450	Network Interface
dvwa_OsDisk_1_60c6f5c45717480fac51d9d454beb9e	Disk
Icexp99b6048c2taining	Storage account
linuxssh	Virtual machine
linuxssh-nsg	Network security group
linuxssh645	Network Interface
linuxssh_disk1_ad01d2b5776342a5a527d5df92d9c86c	Disk
workload-VNET	Virtual network

▶ Task 10 - Configure VNET Peering FGAA

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.

The screenshot shows the 'Effective routes' table for the network interface 'Network interface (dvwa450)'. The table has columns for Source, State, Address Prefixes, Next Hop Type, and User Defined Route Name. A row for 'Default' with 'Address Prefixes' 10.2.0.0/16 and 'Next Hop Type' 'VNet peering' is highlighted with a red box. The table also includes rows for Default (10.3.0.0/16, Virtual network), Default (0.0.0.0/0, Internet), and User (0.0.0.0/0, Virtual appliance).

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

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

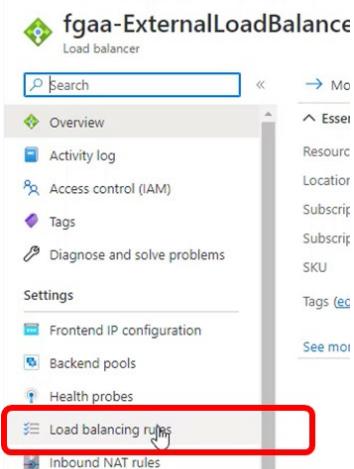
A screenshot of the Microsoft Azure portal's 'Resource groups' page. The title bar says 'Microsoft Azure' and 'Home >'. Below it is a 'Resource groups' section with a sub-section 'Default Directory'. There are buttons for '+ Create', 'Manage view', 'Refresh', 'Export to CSV', and 'Open'. Below these are filters for 'Subscription equals all' and 'Location equals all'. A list of resource groups is shown, with 'Icexp99-fgtaa' highlighted with a red box and a cursor pointing at it. Other listed groups include 'Icexp99-fgtap', 'Icexp99-fwb', and 'Icexp99-training'.

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

A screenshot of the Microsoft Azure portal's 'Icexp99-fgtaa' resource group details page. The title bar says 'Icexp99-fgtaa > Resource group'. On the left is a navigation sidebar with links like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Resource visualizer', 'Events', 'Settings' (with 'Deployments', 'Security', 'Policies', 'Properties', 'Locks', 'Cost Management', and 'Cost analysis' sub-links), and 'Cost analysis'. The main pane shows 'Essentials' information: Subscription (moved) to 'FNT-Training', Subscription ID, and Tags. Below this is a 'Resources' section with a list of resources, including 'consolenvzkoddm3le', 'fgaa-AvailabilitySet', 'fgaa-ExternalLoadBalancer' (which is highlighted with a red box and has a cursor over it), 'fgaa-FGT-A', and 'fgaa-FGT-A-Nic1'. There are also filters for 'Type equals all' and 'Location equals all'.

► 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

The screenshot shows the 'Load balancing rules' page for the 'fgaa-ExternalLoadBalancer'. It displays a table of existing load balancing rules. A red box highlights the '+ Add' button located at the top left of the table area. The table columns are Name, Load balancing rule, and Backend pool. The data in the table is as follows:

Name	Load balancing rule	Backend pool
ExternalLBRule-FE-Http	ExternalLBRule-FE-Http (TCP/80)	fgaa-ELB-ExternalSubnet-BackEnd
ExternalLBRule-FE-udp10551	ExternalLBRule-FE-udp10551 (UDP/10551)	fgaa-ELB-ExternalSubnet-BackEnd

► 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	lbpulse (TCP:8008)
Session persistence	Client IP and protocol
Floating IP	Enable

Add load balancing rule

fgaa-ExternalLoadBalancer

backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name * ✓

IP Version * IPv4 IPv6

Frontend IP address *

Backend pool *

Protocol * TCP UDP

Port * ✓

Backend port * ✓

Health probe * ✓
Create new

Session persistence

Idle timeout (minutes) * ✓

TCP reset Disabled Enabled

Floating IP ✓

Outbound source network address translation (SNAT) (Recommended) Use outbound rules to provide backend pool members access to the internet. [Learn more](#) ↗

Use default outbound access. This is not recommended because it can cause SNAT port exhaustion. [Learn more](#) ↗

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

Balancer | Load balancing rules ...

The screenshot shows a table of load balancing rules. The columns are: Name (sorted by name), Load balancing rule (sorted by name), Backend pool (sorted by name), and Health probe. A red box highlights the last row, which corresponds to the task requirement.

Name ↑↓	Load balancing rule ↑↓	Backend pool ↑↓	Health probe
ExternalLBRule-FE-http	ExternalLBRule-FE-http (TCP/80)	fgaa-ELB-ExternalSubnet-BackEnd	lbprobe
ExternalLBRule-FE-udp10551	ExternalLBRule-FE-udp10551 (UDP/10551)	fgaa-ELB-ExternalSubnet-BackEnd	lbprobe
ssh-to-linuxssh	ssh-to-linuxssh (TCP/22 to TCP/222)	fgaa-ELB-ExternalSubnet-BackEnd	lbprobe

9. You have completed this task

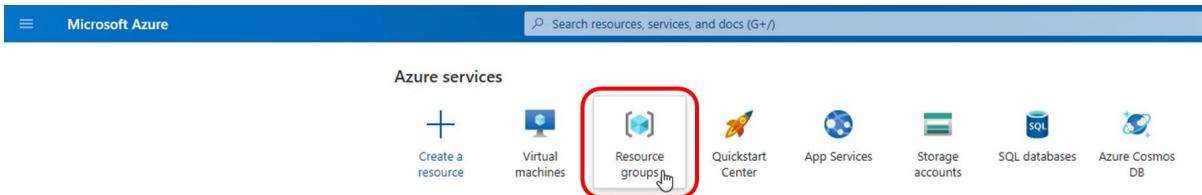
- ▶ Task 12 - Configure FortiGate Active-Active config synchronization

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**

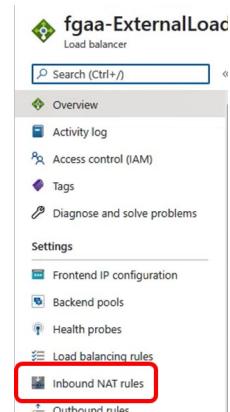


2. Click on the **lcepx99-fgtaa** resource group name itself to open a new pane on the right.

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

▶ Task 12 - Configure FortiGate Active-Active config synchronization

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 fgt-A and FortiGate fgt-B for the HTTPS admin access

Load balancer | Inbound NAT rules

+ Add ⏪ Refresh ⌂ Give feedback

Filter by name...

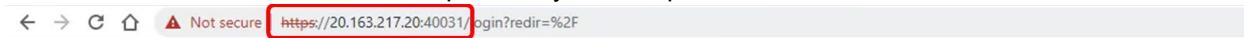
Name ↑↓	Frontend IP ↑↓	Frontend port/range ↑↓
fgaa-FGT-ASSH	20.163.217.20	50030
fgaa-FGT-AFGAdminPerm	20.163.217.20	40030
fgaa-FGT-BSSH	20.163.217.20	50031
fgaa-FGT-BFGAdminPerm	20.163.217.20	40031

► Task 12 - Configure FortiGate Active-Active config synchronization

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

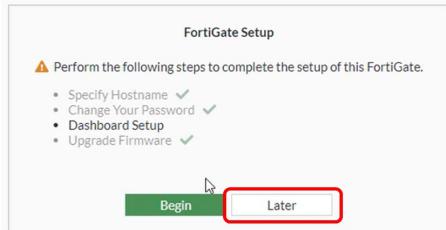
A screenshot of a FortiGate login interface. It has a green header with a circular logo. Below it are two input fields: one for 'Username' and one for 'Password'. At the bottom is a large green 'Login' button.

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

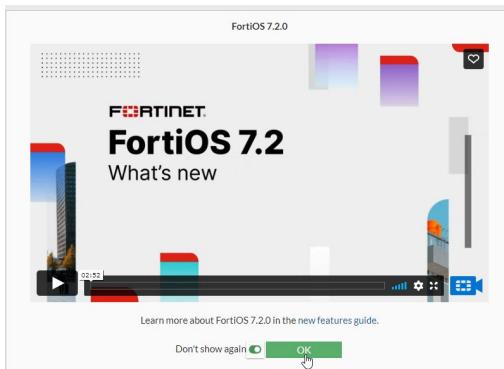
A screenshot of a FortiGate login interface, identical in layout to the one shown in step 6. It has a green header with a circular logo, two input fields for 'Username' and 'Password', and a green 'Login' button.

► 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 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
```

```
fgaa-FGT-A # config system auto-scale
fgaa-FGT-A (auto-scale) #     set status enable
fgaa-FGT-A (auto-scale) #     set sync-interface "port2"
fgaa-FGT-A (auto-scale) #     set role primary
fgaa-FGT-A (auto-scale) # end
fgaa-FGT-A #
```

► Task 12 - Configure FortiGate Active-Active config synchronization

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 >_

The screenshot shows the FortiGate fgaa-FGT-B dashboard. The status bar at the top right features a green header with the device name and a red button labeled '>_'. Below the header, there are four main sections: System Information, Licenses, Virtual Machine, and FortiGate Cloud. The 'Auto Scaling' section in the Virtual Machine section is highlighted with a red box.

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
```

The screenshot shows the CLI console window titled 'CLI Console (1)'. It displays the following configuration commands:

```
fgaa-FGT-B # config system auto-scale
fgaa-FGT-B (auto-scale) #     set status enable
fgaa-FGT-B (auto-scale) #     set sync-interface "port2"
fgaa-FGT-B (auto-scale) #     set role secondary
fgaa-FGT-B (auto-scale) #     set primary-ip 10.2.2.5
fgaa-FGT-B (auto-scale) # end
fgaa-FGT-B #
```

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

The screenshot shows the FortiGate fgaa-FGT-B dashboard. The status bar at the top right has a red box around the text 'Autoscale: Secondary'.

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

The screenshot shows the FortiGate fgaa-FGT-A dashboard. The status bar at the top right has a red box around the text 'Autoscale: Primary'. The 'Virtual Machine' section in the center is also highlighted with a red box, showing the 'Auto Scaling' status.

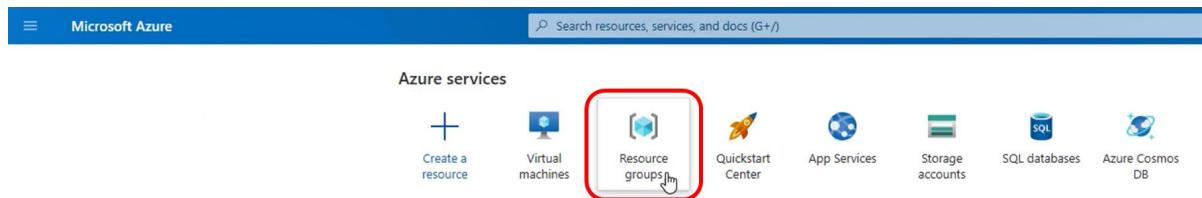
15. This task is now complete

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

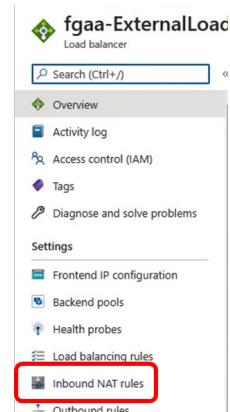
A screenshot of the 'Resource groups' blade in the Azure portal. The title bar says 'Resource groups' and 'Default Directory'. Below it, there are buttons for 'Create', 'Manage view', 'Refresh', 'Export to CSV', and 'Open'. A search bar says 'Filter for any field...' and dropdowns for 'Subscription equals all' and 'Location equals all'. There are two summary boxes: 'Unsecure resources' (0) and 'Recommendations' (0). The main list shows several resource groups, with 'Icexp99-fgtaa' selected and highlighted with a red box. Other listed groups include 'Icexp99-rgtap', 'Icexp99-fwb', and 'Icexp99-training'.

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

A screenshot of the 'Icexp99-fgtaa' resource group blade in the Azure portal. The title bar says 'Icexp99-fgtaa' and 'Resource group'. On the left, there's a navigation menu with 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Resource visualizer', 'Events', 'Settings' (with sub-options like 'Deployments', 'Security', 'Policies', 'Properties', 'Locks', 'Cost management', and 'Cost analysis'), and a 'Search' bar. The main area shows 'Essentials' information: Subscription (move) to 'FTNT-Training', Subscription ID, and Tags (edit). Below this is a 'Resources' section with a list of resources, including 'fcaa-ExternalLoadBalancer', which is selected and highlighted with a red box. Other resources listed include 'consolerenvzvkoxdm3le', 'fcaa-AvailabilitySet', 'fcaa-FGT-A', and 'fcaa-FGT-A-Nic1'.

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

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

Load balancer | Inbound NAT rules ...

Name ↑↓	Frontend IP ↑↓	Frontend port/range ↑↓
fgaa-FGT-ASSH	20.163.217.20	50030
fgaa-FGT-AGFAdminPerm	20.163.217.20	40030
fgaa-FGT-BCCW	20.163.217.20	50031

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 **azureadadm** and the previously chosen password.



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

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

Destination	Gateway IP	Interface
0.0.0.0/0	10.2.1.1	port1
10.2.0.0/16	10.2.2.1	port2
168.63.129.16/32	10.2.2.1	port2
168.63.129.16/32	10.2.1.1	port1

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

New Static Route

Destination: Subnet Internet Service
10.3.0.0/24

Gateway Address: 10.2.2.1

Interface: port2

Administrative Distance: 10

Comments: Write a comment... 0/255

Status: Enabled

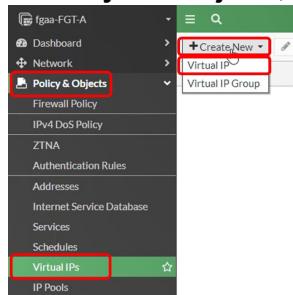
OK

9. Confirm the routing entries with the screen below

Destination	Gateway IP	Interface	Status
0.0.0.0/0	10.2.1.1	port1	Enabled
10.2.0.0/16	10.2.2.1	port2	Enabled
168.63.129.16/32	10.2.2.1	port2	Enabled
168.63.129.16/32	10.2.1.1	port1	Enabled
10.3.0.0/24	10.2.2.1	port2	Enabled

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

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

New Virtual IP

VIP type: IPv4

Name: **Public-LB-IP**

Comments: Write a comment... 0/255

Color: Change

Network

Interface: any

Type: Static NAT

External IP address/range: 20.163.217.20

Map to:

IPv4 address/range: 10.3.0.4

Optional Filters

Protocol: TCP

Port Mapping Type: One to one

External service port: 2022

Map to IPv4 port: 22

OK

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

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

The screenshot shows the FortiGate management interface. The left sidebar has a tree structure with 'fgaa-FGT-A' at the top, followed by 'Dashboard', 'Network', 'Policy & Objects' (which is expanded), 'Firewall Policy', 'IPv4 DoS Policy', and 'ZTNA'. The 'Policy & Objects' section is highlighted with a green background. The main pane title is 'IPv4 Virtual IP 1'. It contains one entry: 'Public-LB-IP' with details '20.163.217.20 → 10.3.0.4 (TCP: 2022 → 22)' and a checkbox 'any'. A red box highlights the entire row for 'Public-LB-IP'.

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

The screenshot shows the FortiGate management interface. The left sidebar has a tree structure with 'fgaa-FGT-A' at the top, followed by 'Dashboard', 'Network', 'Policy & Objects' (which is highlighted with a red box), 'Firewall Policy' (which is highlighted with a green background), 'IPv4 DoS Policy', and 'ZTNA'. The 'Firewall Policy' section is highlighted with a green background. The main pane title is '+ Create New'. A red box highlights the '+ Create New' button.

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

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 (<i>Virtual IP</i>)
Service	SSH
Log Allowed Traffic	All Sessions

The screenshot shows the FortiGate Management UI with the left sidebar open. The selected menu path is **Policy & Objects** → **Firewall Policy**. The main pane displays a 'New Policy' configuration window.

Policy Details:

- Name:** ssh-to-linux
- Incoming Interface:** port1
- Outgoing Interface:** port2
- Source:** all
- Destination:** Public-LB-IP
- Service:** SSH
- Action:** ACCEPT

Inspection Mode: Flow-based

Firewall/Network Options:

- NAT: Enabled
- IP Pool Configuration: Use Outgoing Interface Address
- Preserve Source Port: Enabled
- Protocol Options: PROT default

Security Profiles:

- AntiVirus: Enabled
- Web Filter: Enabled
- DNS Filter: Enabled
- Application Control: Enabled
- IPS: Enabled
- File Filter: Enabled

SSL Inspection: no-inspection

Logging Options:

- Log Allowed Traffic: Enabled (highlighted with a red box)
- Security Events: Enabled
- All Sessions: Selected (highlighted with a red box)
- Generate Logs when Session Starts: Enabled
- Capture Packets: Enabled

Comments: Write a comment... / 0/1023

Enable this policy: Enabled

Buttons: OK (highlighted with a red box) and Cancel

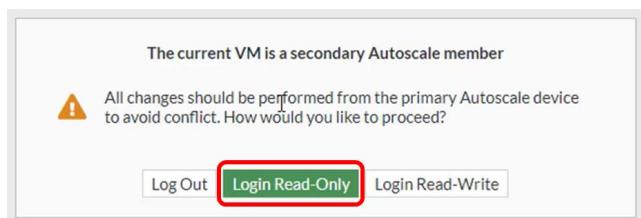
► Task 13 - Configure FortiGate Active-Active Routing and Security Policies

15. Confirm the Policy created with the screen below

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log
ssh-to-linux	all	Public-LB-IP	always	SSH	ACCEPT	Enabled	ssl no-inspection All

16. Open another web browser tab to https:// of the FrontEnd IP address along with the port for FortiGate fgt-a, <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 fgt-b click on **Network**, then **Static Routes**. Confirm the static route created on FortiGate fgt-a is synchronized over to FortiGate fgt-b

Destination	Gateway IP	Interface	Stat
0.0.0.0/0	10.2.1.1	port1	Enabled
10.2.0.0/16	10.2.2.1	port2	Enabled
168.63.129.16/32	10.2.2.1	port2	Enabled
168.63.129.16/32	10.2.1.1	port1	Enabled
10.3.0.0/24	10.2.2.1	port2	Enabled

19. In the same FortiGate menu, click on **Policy and Objects**, then **Firewall Policy**. Confirm the Policy created on FortiGate fgt-a synchronized over to FortiGate fgt-b

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log
ssh-to-linux	all	Public-LB-IP	always	SSH	ACCEPT	Enabled	ssl no-inspection All

20. You have completed this task

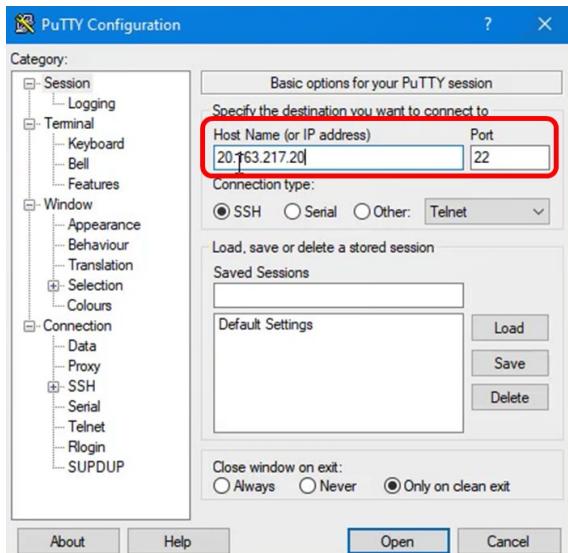
- ▶ Task 14 - Test inbound SSH to linuxssh

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 your own laptop to the FrontEnd IP address (20.163.217.20 in this example). The screenshot below shows the popular PuTTY software, but any suitable SSH client can be used.



2. Confirm you can login as per below

```
System load: 0.0          Processes:      103
Usage of /: 5.9% of 28.89GB  Users logged in:   1
Memory usage: 28%          IPv4 address for eth0: 10.3.0.4
Swap usage: 0%

* Super-optimized for small spaces - read how we shrunk the memory
  footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Last login: Thu Sep 22 13:39:57 2022
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureadm@linuxssh:~$
```

3. This task is now complete