Cloud NGFW for Azure UTD Lab Guide

Table of Contents

Purpose of This Workshop Guide

This workshop guide describes deploying Cloud NGFW for Azure by Palo Alto Networks in the Microsoft Azure public cloud to provide visibility and protection for the VNet inbound, outbound and East-West traffic

The activities outlined in this Workshop Guide are meant to contain all the information necessary to navigate the workshop interface, complete the workshop activities, and troubleshoot any potential issues with the lab environment. This guide is meant to be used in conjunction with the information and guidance provided by your facilitator.

This workshop guide covers only basic topics and is not a substitute for training classes conducted by Palo Alto Networks Authorized Training Centers. Please contact your partner or regional sales manager for more information on available training and how to register for one near you.

Lab Activities Overview

There are three parts to this lab

Part-1 : Build test setup that will be used for this workshop using ARM template

Part-2 : Create and Configure Cloud NGFW for Azure using Azure portal to secure user traffic

Part-3 : Test traffic secured through Cloud NGFW. Simulate attack and verify Cloud NGFW in action

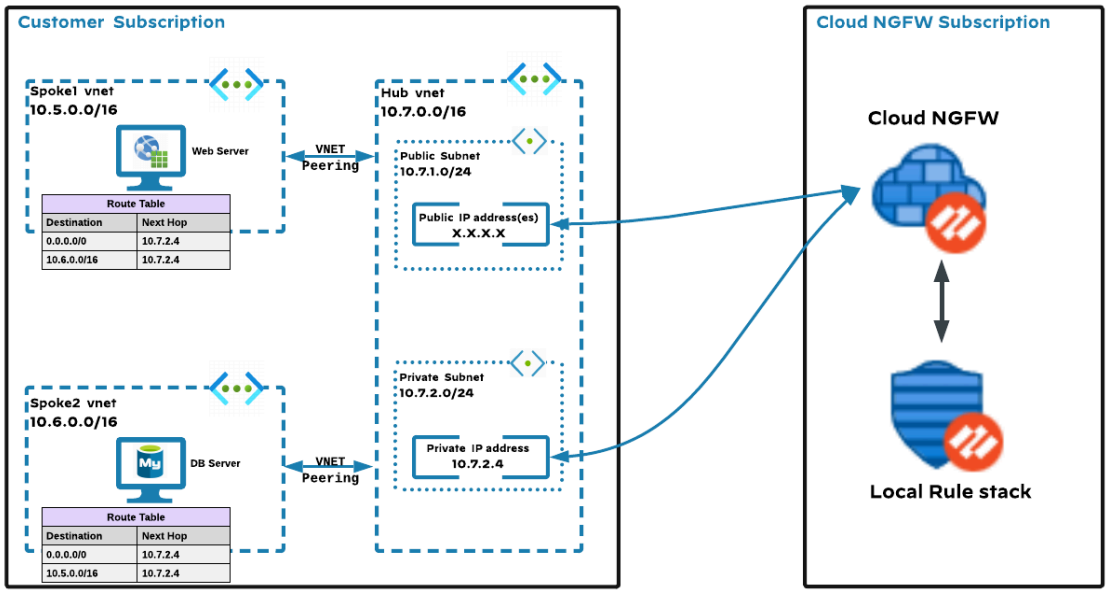
Once These Activities Have Been Completed

You should be able to:

1. Understand on how to create Cloud NGFW service using Azure portal
2. Manage security policies using Local Rule stack
3. Secure your VNet infrastructure using Cloud NGFW for Azure by Palo Alto Networks

Part-1 : Build test setup that will be used for this workshop using ARM template

Lab Topology



Activity 0: Log In to the UTD Workshop

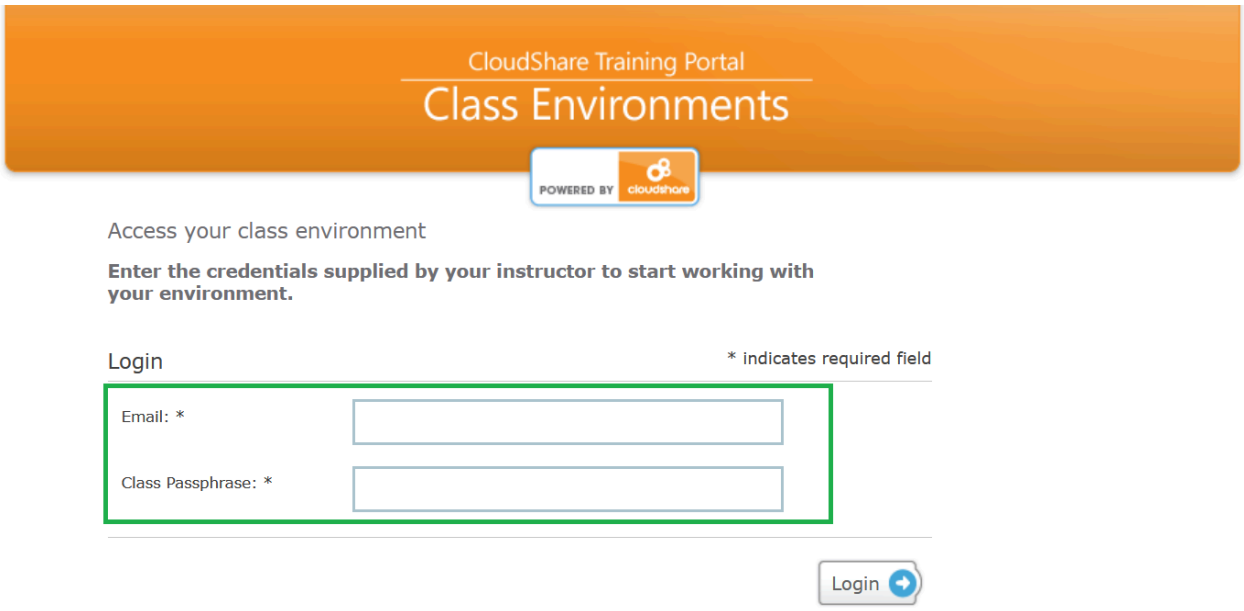
In this activity, you will:

- Log in to the Ultimate Test Drive Workshop from your laptop.
    - Understand the layout of the environment and its various components.
- Log in to the Azure portal using the account provided.

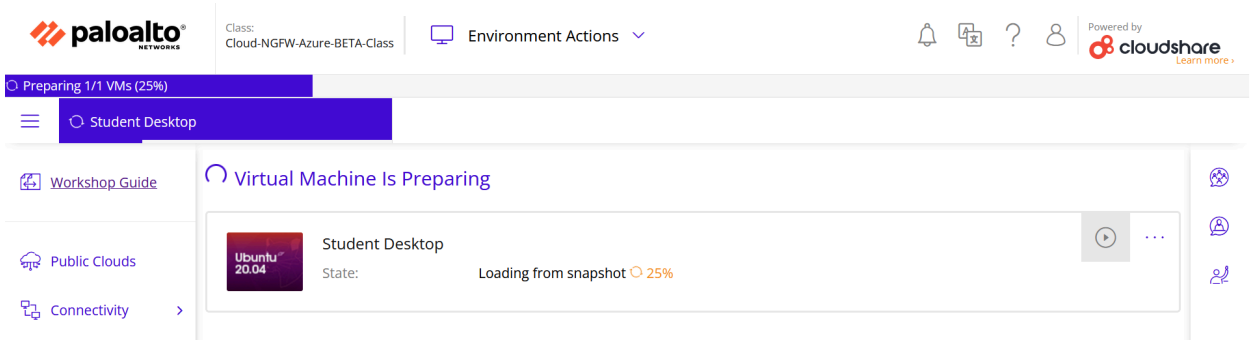
Task 1 - Login to Your Ultimate Test Drive Class Environment

- Open a browser window and navigate to the class URL. If you have an invitation email, you will find the class URL and passphrase there. Otherwise, your instructor will provide them.

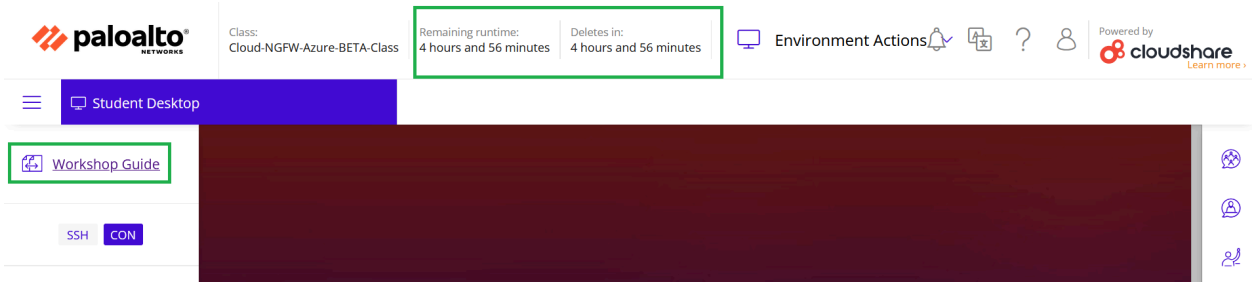
Enter your email address and the class passphrase.



- Complete the registration process by providing your name and click the **Register and Login** option that you will get at the bottom.
- Make a note of your email and password to login to the UTD lab environment. You might need email and password to re-login in the lab environment in case you logged out.
- Once you have logged in, the system will create a unique UTD environment for you. Please note that this process may take a while, as indicated by the progress bar at the top of the screen. This will look something like the following screen



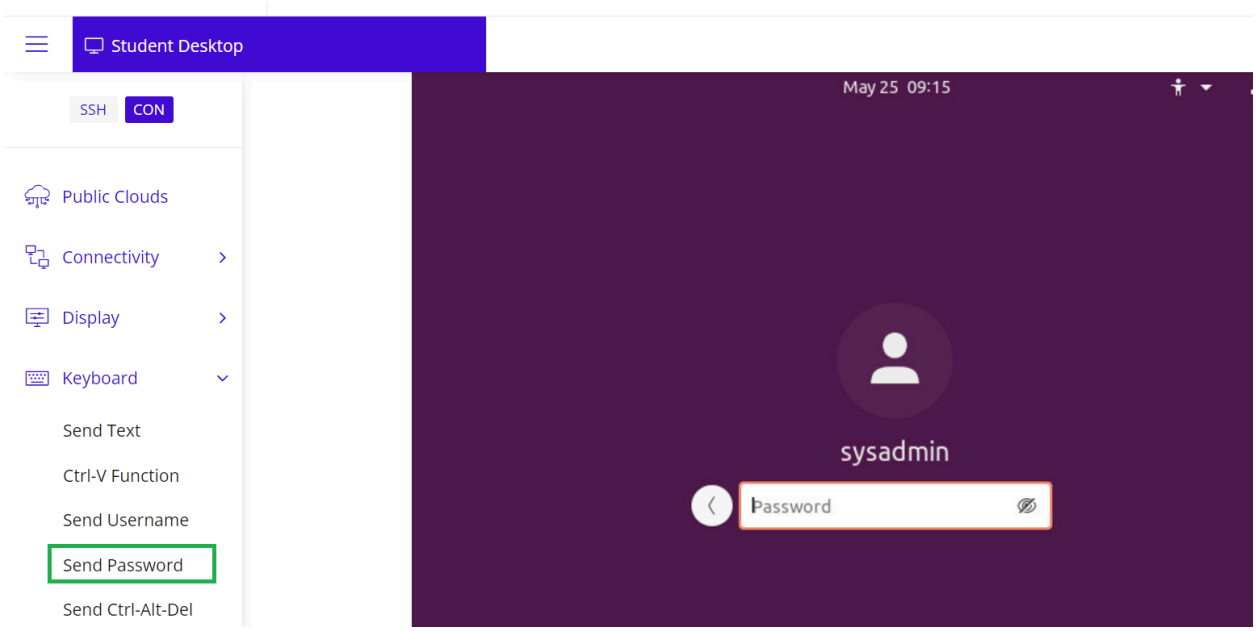
- On Successful creation of the lab, you will see the lab runtime as shown in the below screenshot. Click on the Workshop Guide tab to open the lab guide in a new tab and follow the instructions as per the guide to complete the workshop.



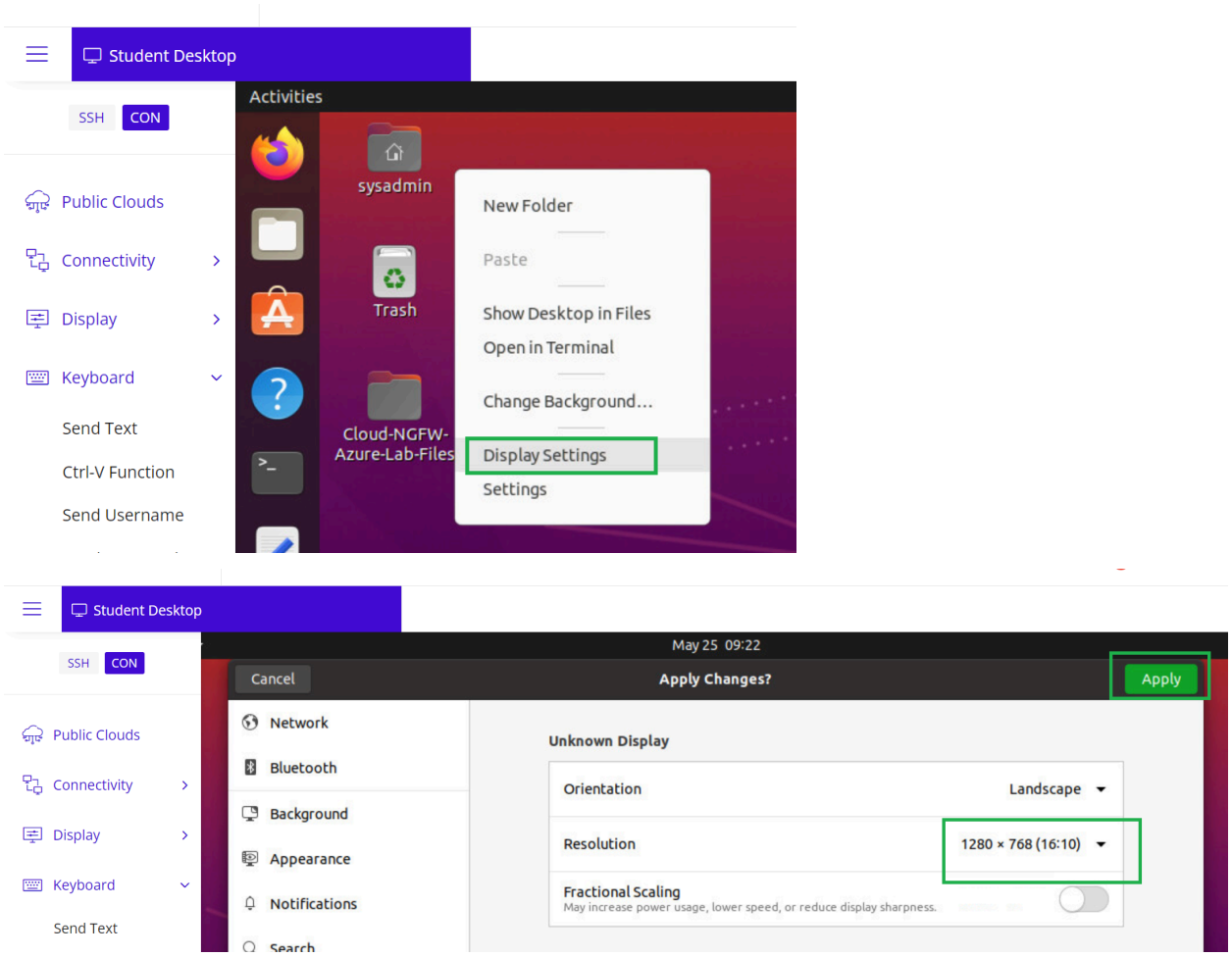
Task 2 : Log in to the Azure portal using the account provided.

This hands-on lab lets you do the lab activities yourself in a real cloud environment, not in a simulation or demo environment. It does so by giving you new, temporary credentials that you use to sign in and access the Azure portal for the duration of the lab.

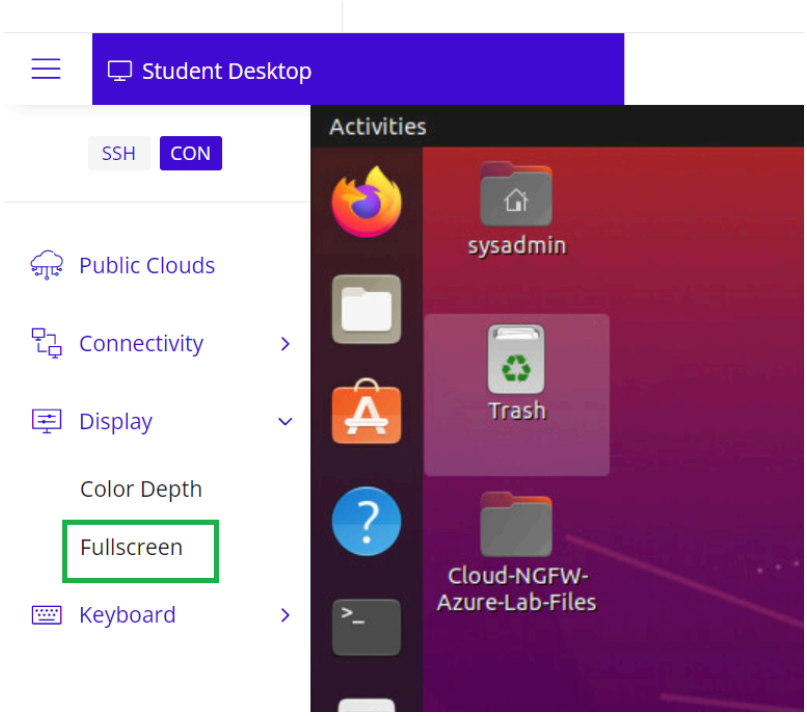
- Go to the CloudShare lab environment and click on the Student Desktop tab at the top of the page.
- In the left-hand side Action panel under the Keyboard, click on the Send Password to log in on Student Desktop.



- If the Student Desktop resolution is too high or too low for your laptop display, you can adjust the resolution by right clicking on the desktop and then select the Display Settings. Select the resolution from Resolution drop drown. The recommended resolution is 1280 x 768 (16:10).

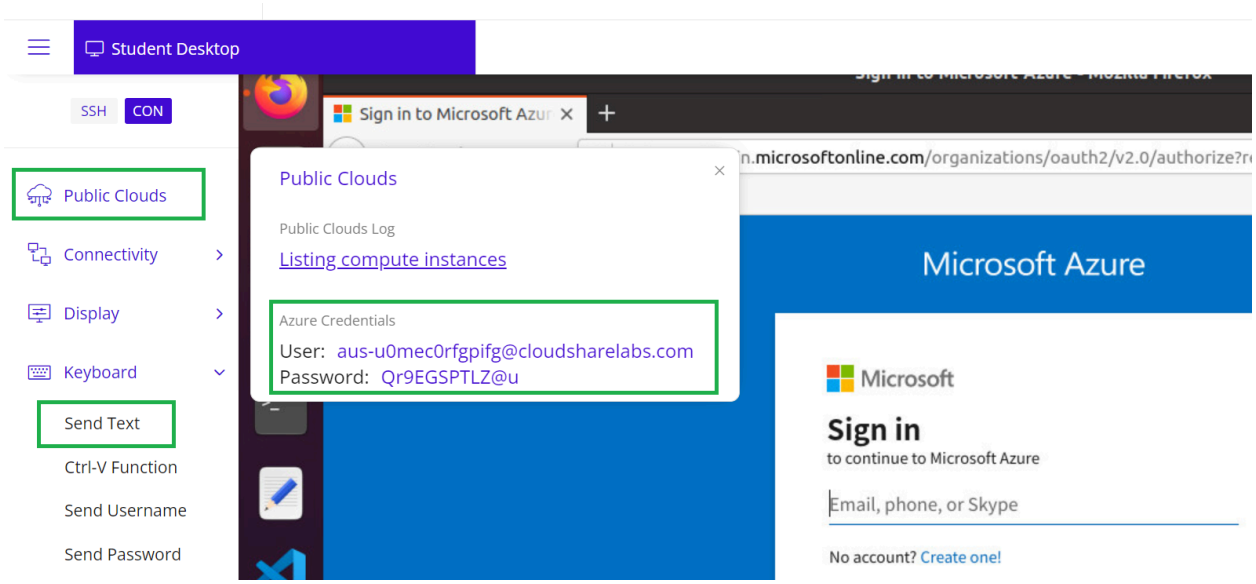


- From the left-hand Action panel. You can also click the Full screen icon to maximize the display.

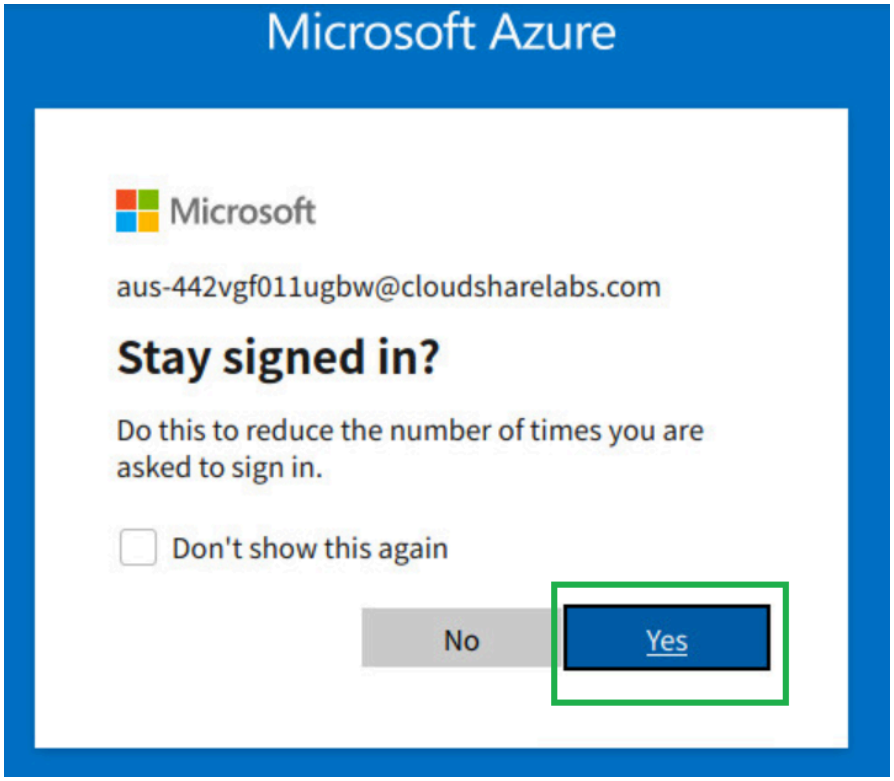


- To exit the full-screen mode, use the esc key on our keyboard or click the black arrow at the top of the window to open the dropdown menu; then click **Exit**.
- In the **Student Desktop** window click on the **Firefox Web browser** icon.
- Click on **Azure Portal** bookmark tab to open a Azure portal login page. Follow the below steps to copy and paste the login credentials from the left-hand Action panel to login on Azure portal.
    - Under the **Public Clouds > Azure Credentials** click on the **User** and then click on the **Keyboard > Send Text** icon, paste the copied user name and click Send. On the Azure Sign page click **Next**.
    - Repeat step A to copy and paste the **Password**.
    - Finally Click **Sign-in**.

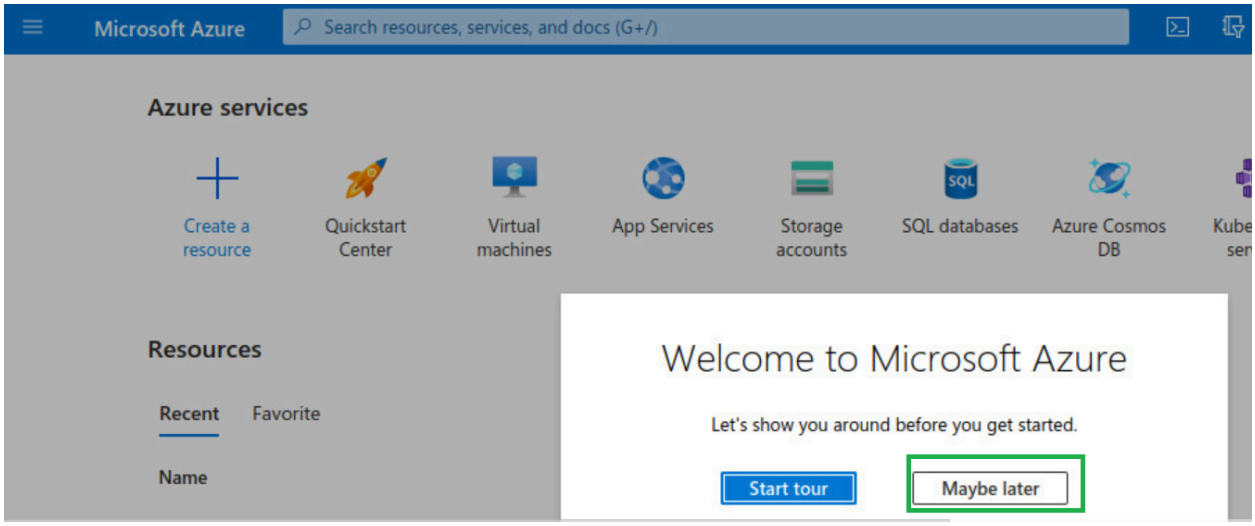

You can also access the Azure portal from your laptop browser and login using the credentials provided by the Cloudshare lab environment.



- To stay signed in to the portal, click **Yes** as shown in the below screenshot



- Click on **Maybe later**, to avoid a tour around the portal. If you wanted to view available options on the portal, you can click on “Start tour” option



End of Activity-0

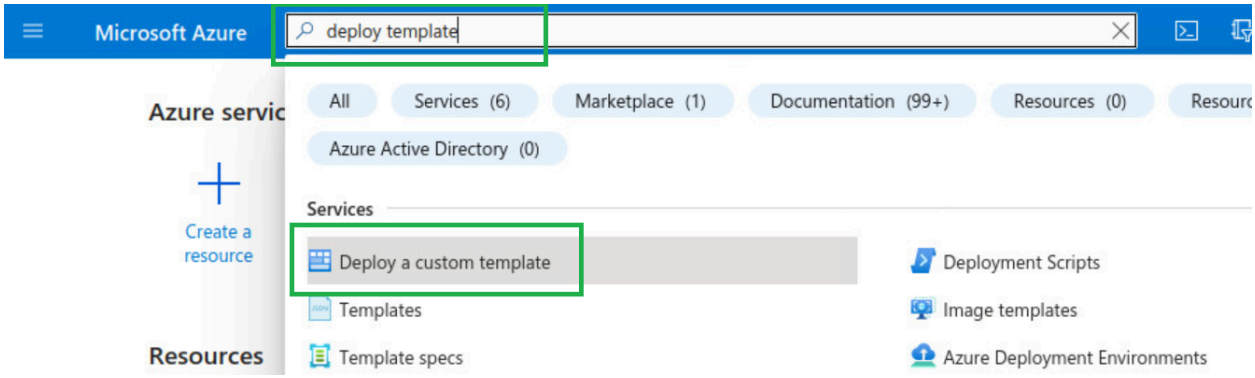
Activity 1: Deploy Lab Environment with ARM Template

In this activity, you will use the Azure Resource Manager (ARM) Template to deploy the lab resources that include

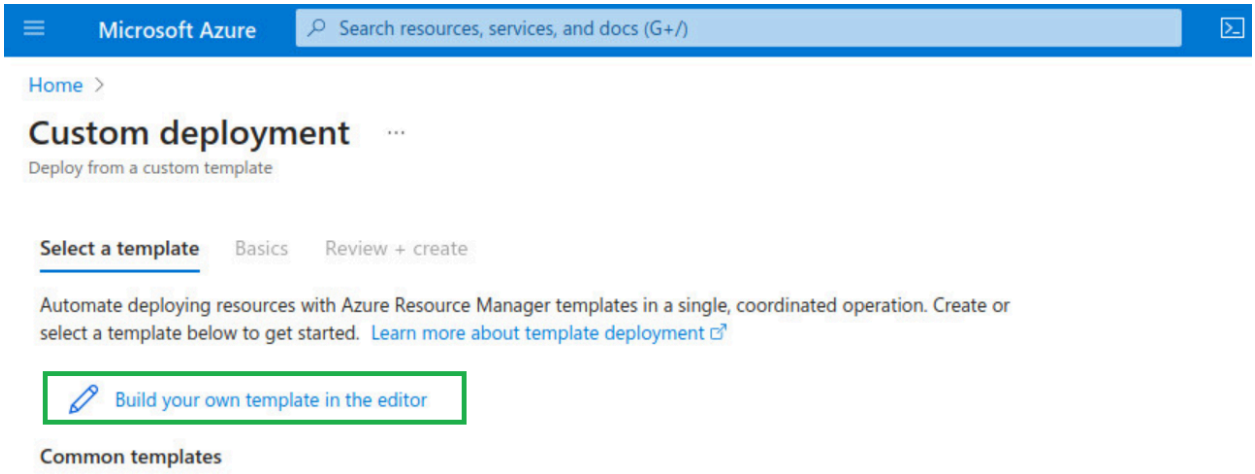
- Spoke VNets with Web and DB servers
- Hub VNet with subnets delegated to Cloud NGFW service
- Spoke VNets peered with Hub VNet
- Log analytics workspace

Task 1 - Launch ARM Template to deploy lab resources

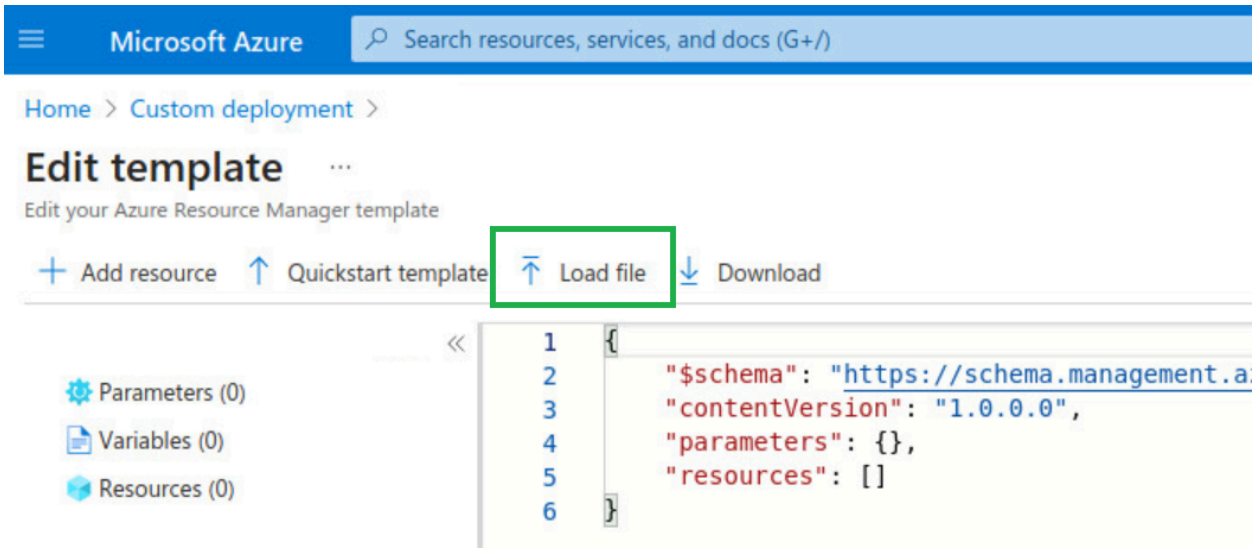
- In the Azure portal, type "**deploy template**" in the global search box and select **Deploy a custom template** option as shown below.



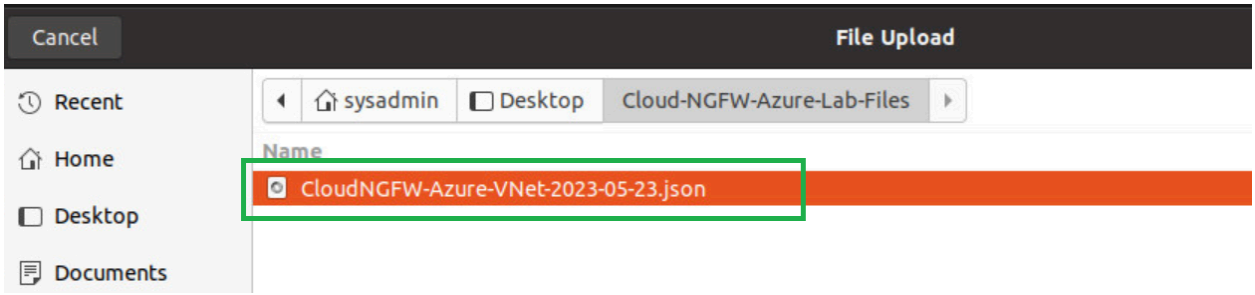
- Select Build your own template in the editor.



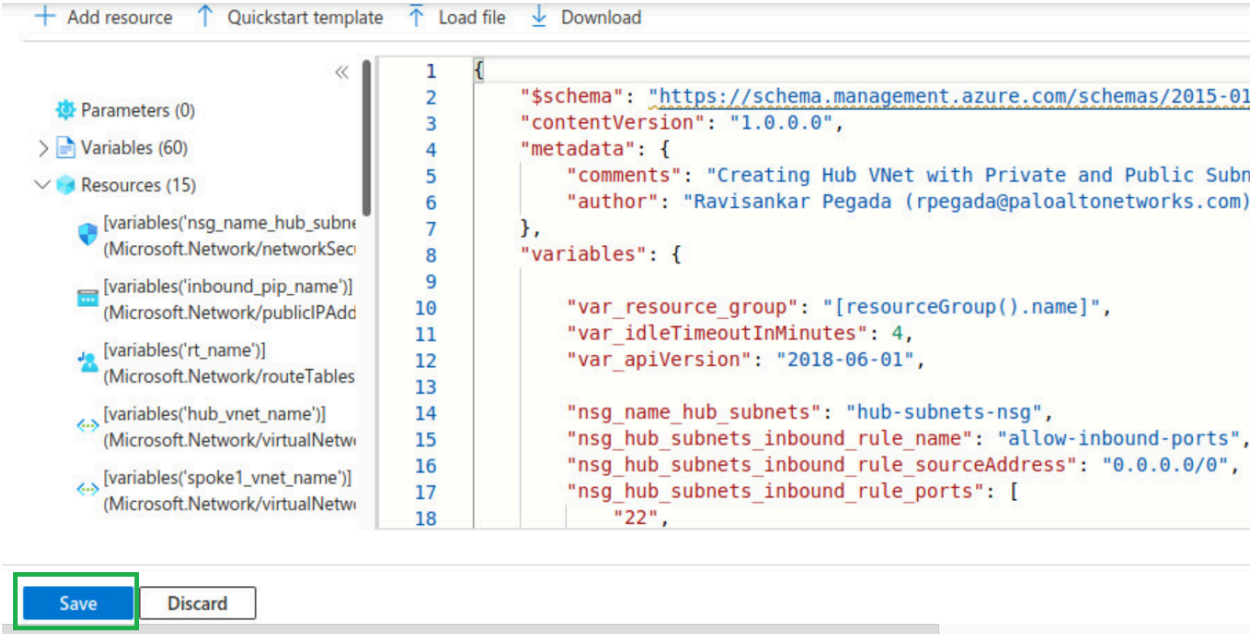
- Use **Load file** option to load custom ARM template



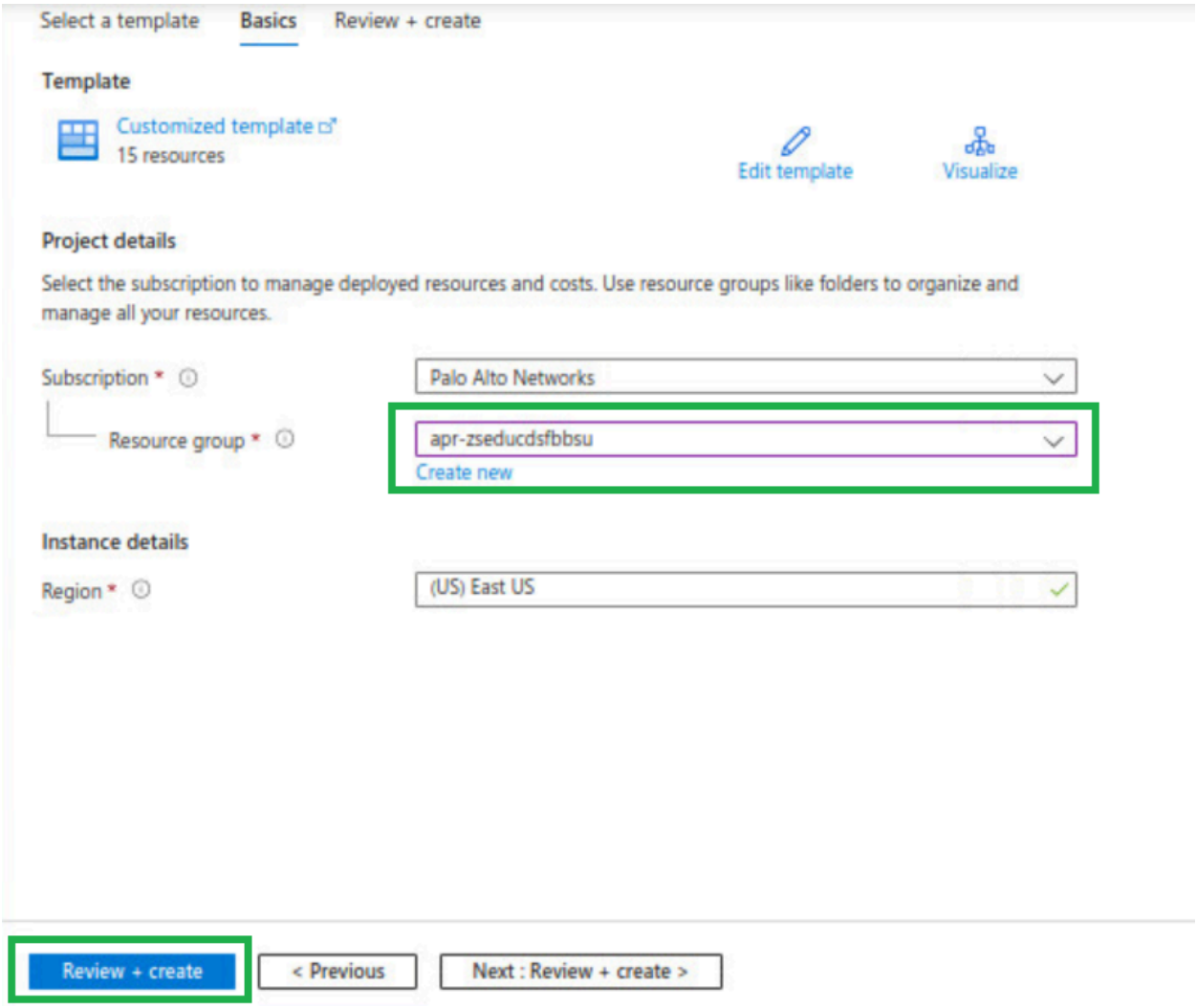
- Browse "**Cloud-NGFW-Azure-Lab-Files/cloudNGFW-Azure-NNet-2023-05-23.json**" file available on Student Desktop as shown below and click on **Open** towards the right or **double click** on the file to upload



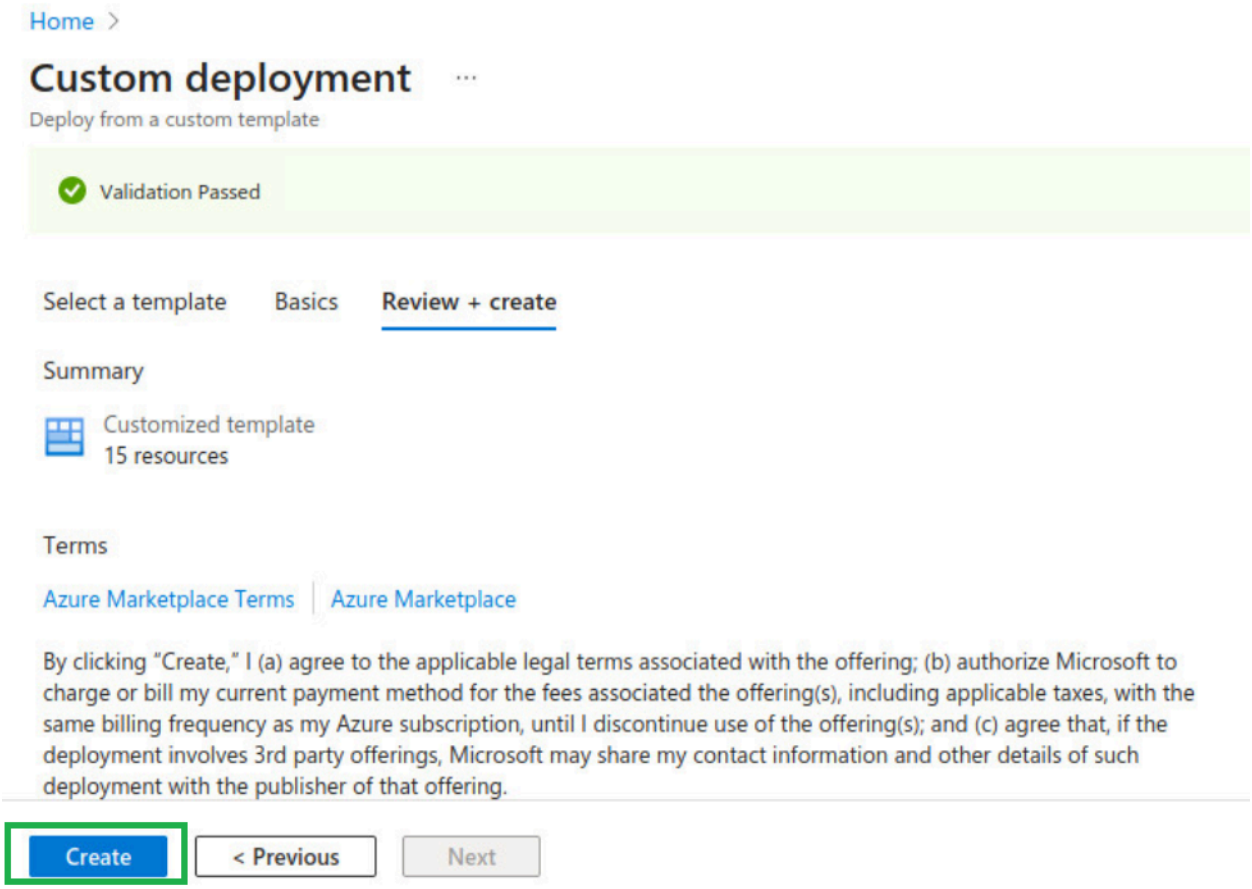
- Click on “**Save**” to save the template



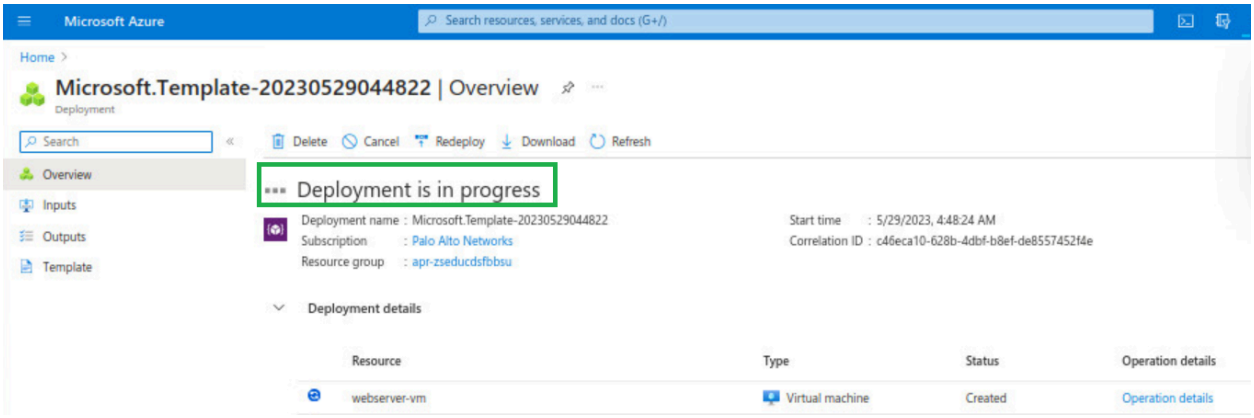
- Now Select the “**Resource group**” from the drop down(you will have a unique single resource group) and click on “**Review + create**” as shown below



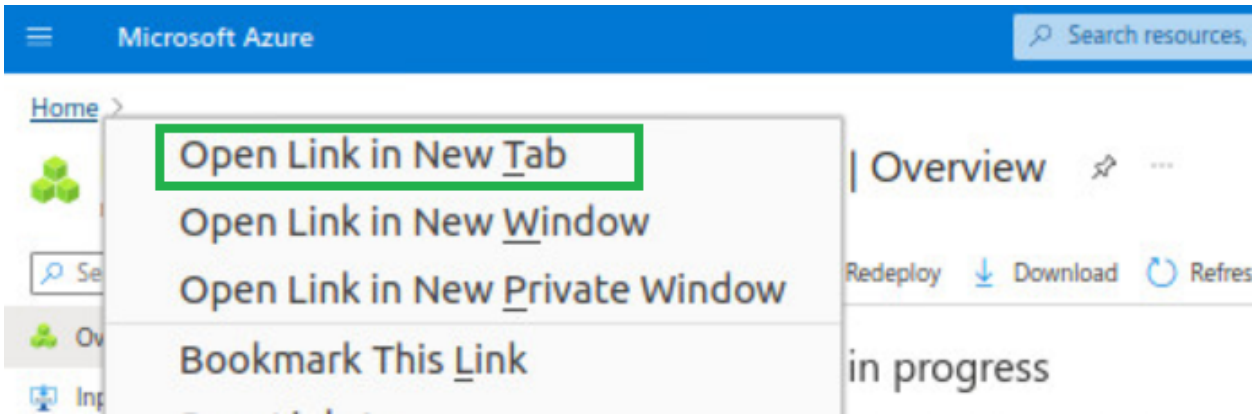
- After successful validation, click on "**Create**" to start creation of resources as per the custom template



- You will see "... Deployment is in progress" screen as shown below



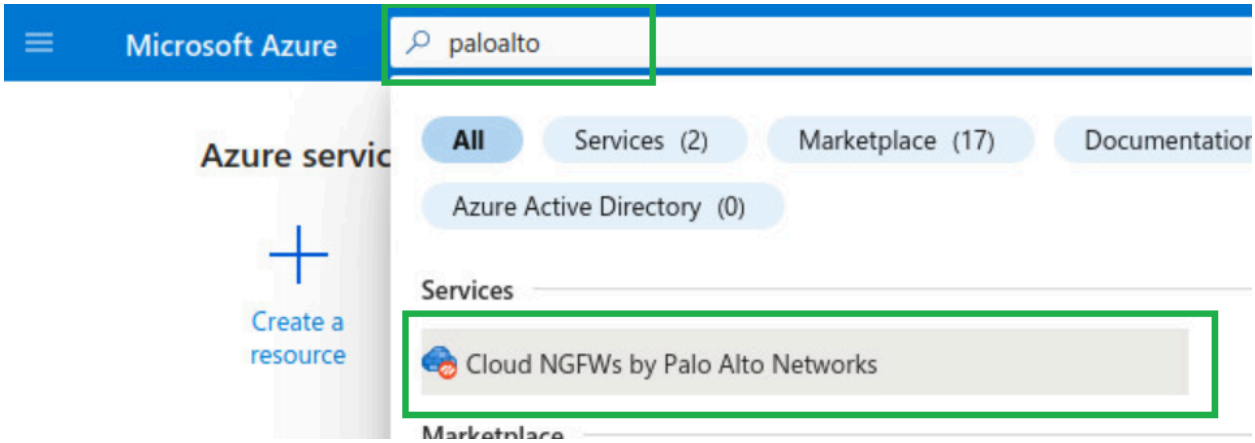
You can wait for the deployment to complete or
While the deployment is in progress, right click on "**Home**" and open Azure portal in another tab.



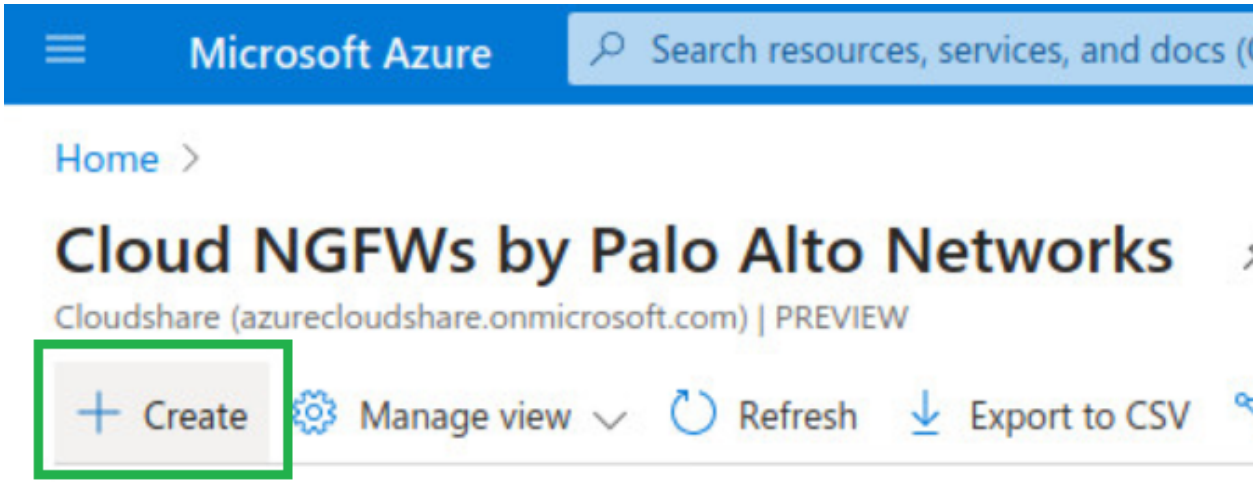
Part-2 : Create and Configure Cloud NGFW for Azure using Azure portal to secure user traffic

Activity 1: Create Cloud NGFW Service

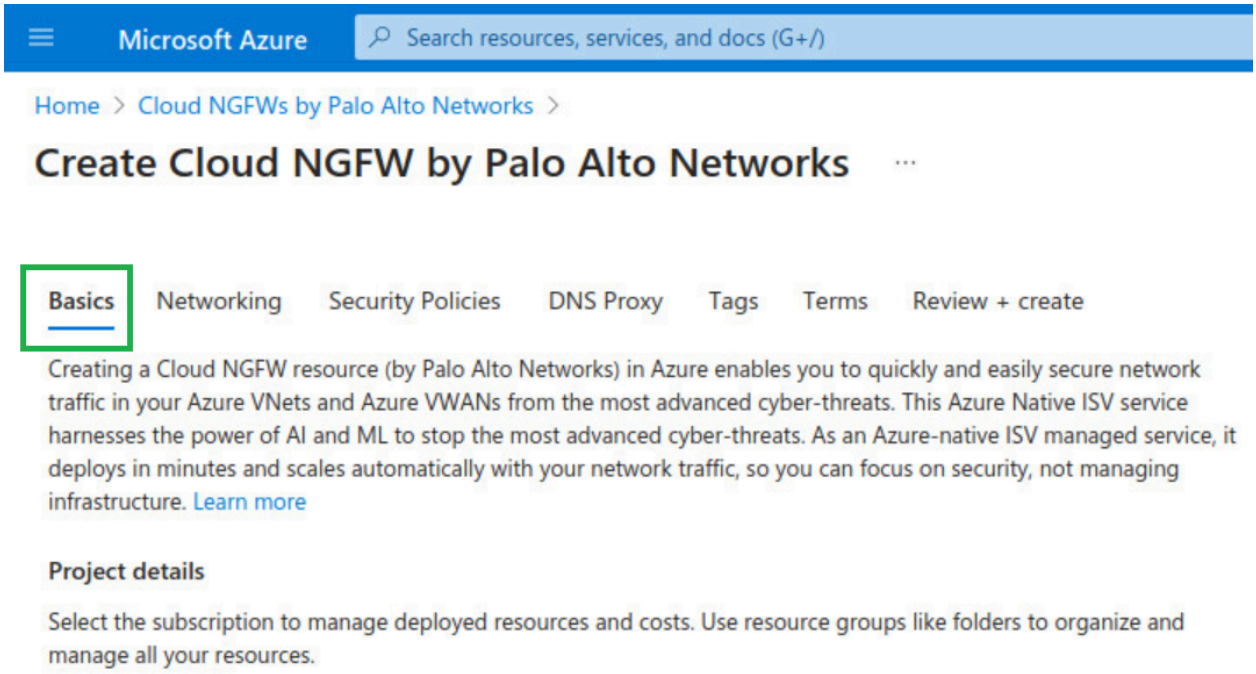
- Within the new tab with Azure portal opened, search for "**paloalto**" as shown below and click on "**Cloud NGFWs by Palo Alto Networks**" to start creation of Cloud NGFW service



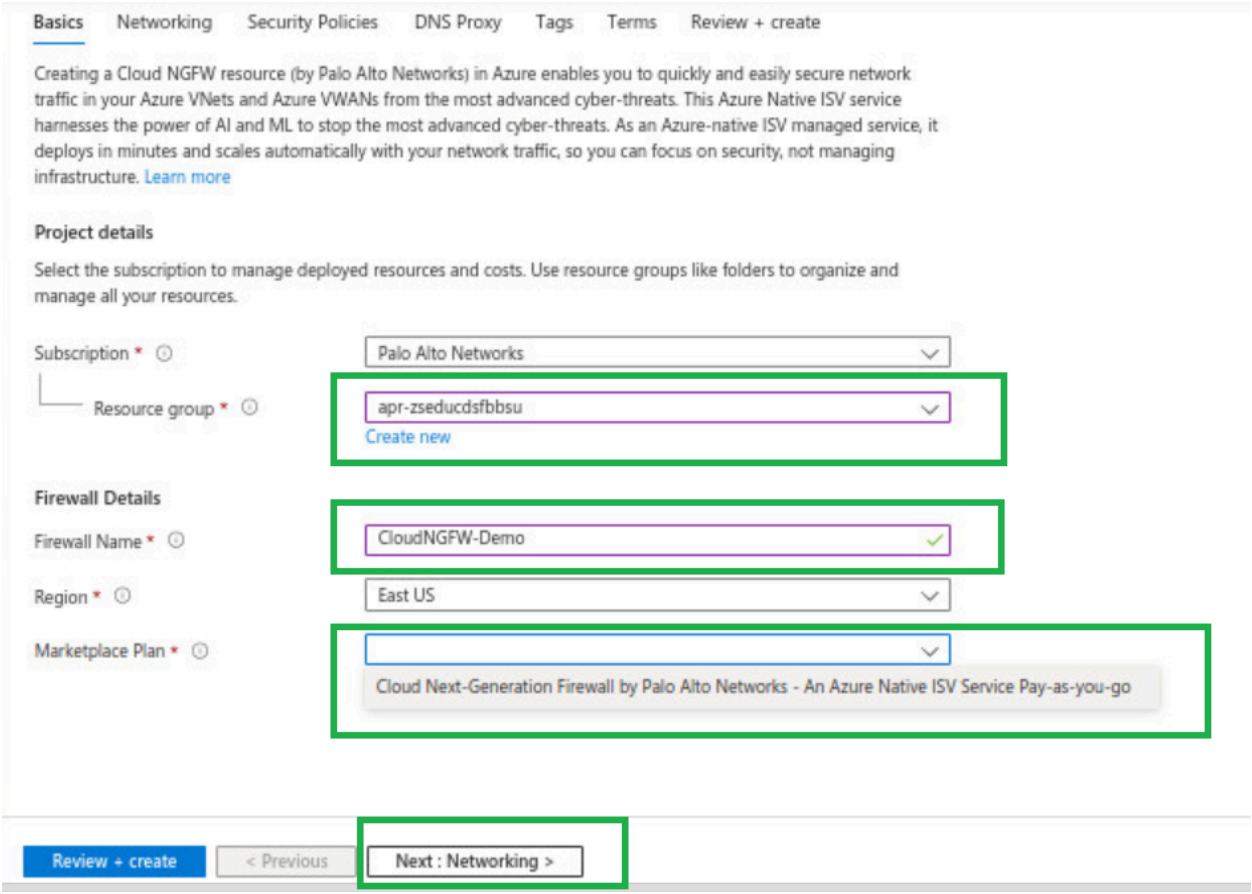
- You will be presented with the screen as shown below. Click on "**Create**" option to start creation of Cloud NGFW Service



- After clicking on "Create" you will be presented with the following screen.



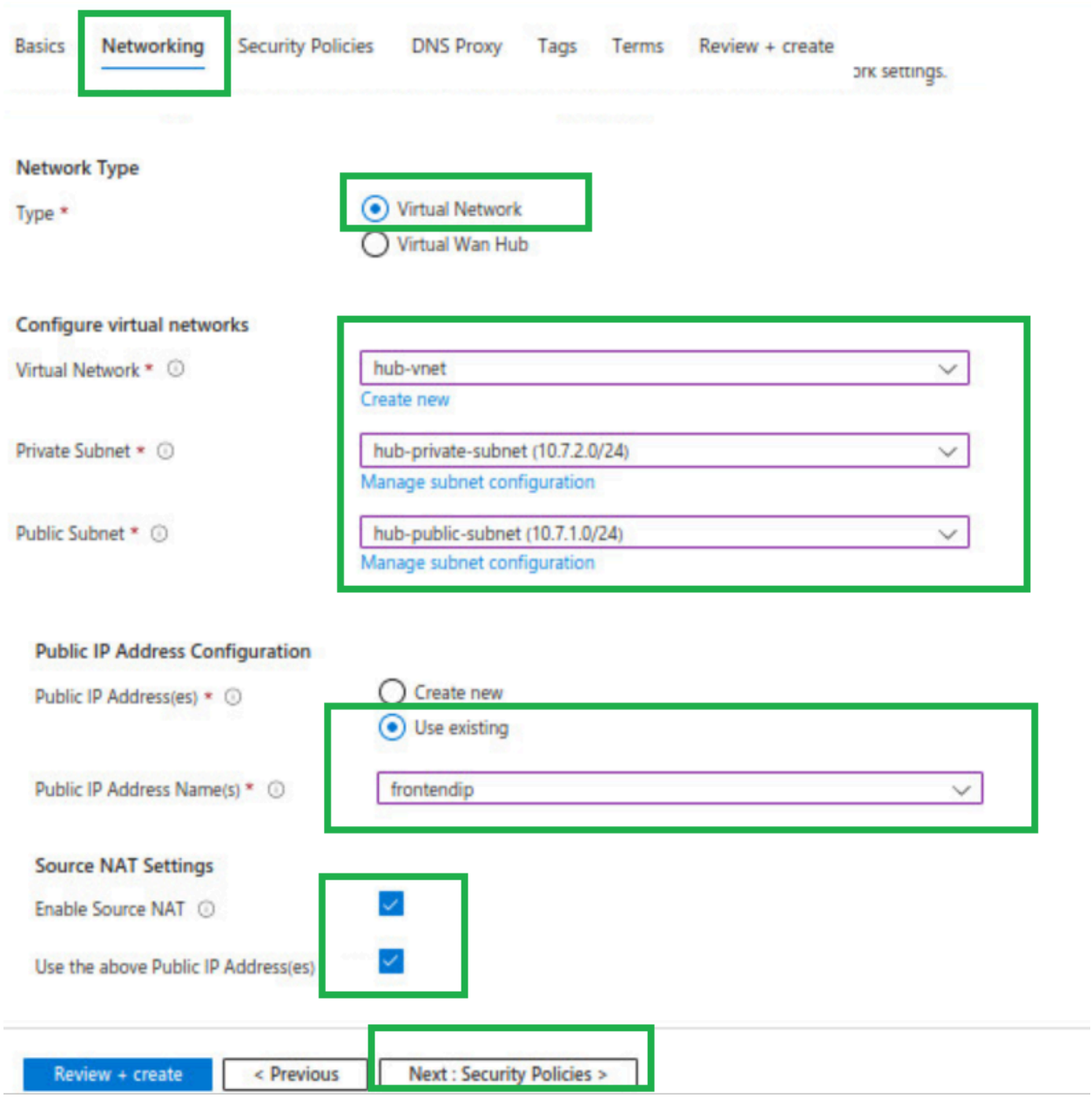
- Within the "**Basics**" tab, select the available "**Resource group**" from the drop down. Provide a name for "**Firewall Name**", Ex: *CloudNGFW-Demo* and select "**Marketplace Plan**" by leaving **Region** to default(East US) as shown in below screenshot.
  Click on "**Next : Networking >**" to proceed further with creation of Cloud NGFW



- Within the Networking section leave the Network Type to default "**Virtual Network**". Configure **Virtual Network** by selecting "**hub-vnet**" from the drop-down, configure **Private Subnet** by selecting "**hub-private-subnet (10.7.2.0/24)**" from the drop-down and **Public Subnet** by selecting "**hub-public-subnet (10.7.1.0/24)**" from the drop-down as shown in the screenshot below.

  Public IP Address Configuration : Select "**Use Existing**" radio button and select "**frontendip**" from the drop-down against Public IP address Name(s)

  Source NAT Settings : Click on **Enable Source NAT** radio button and select "**Use the above Public IP Address(es)**" option as shown below

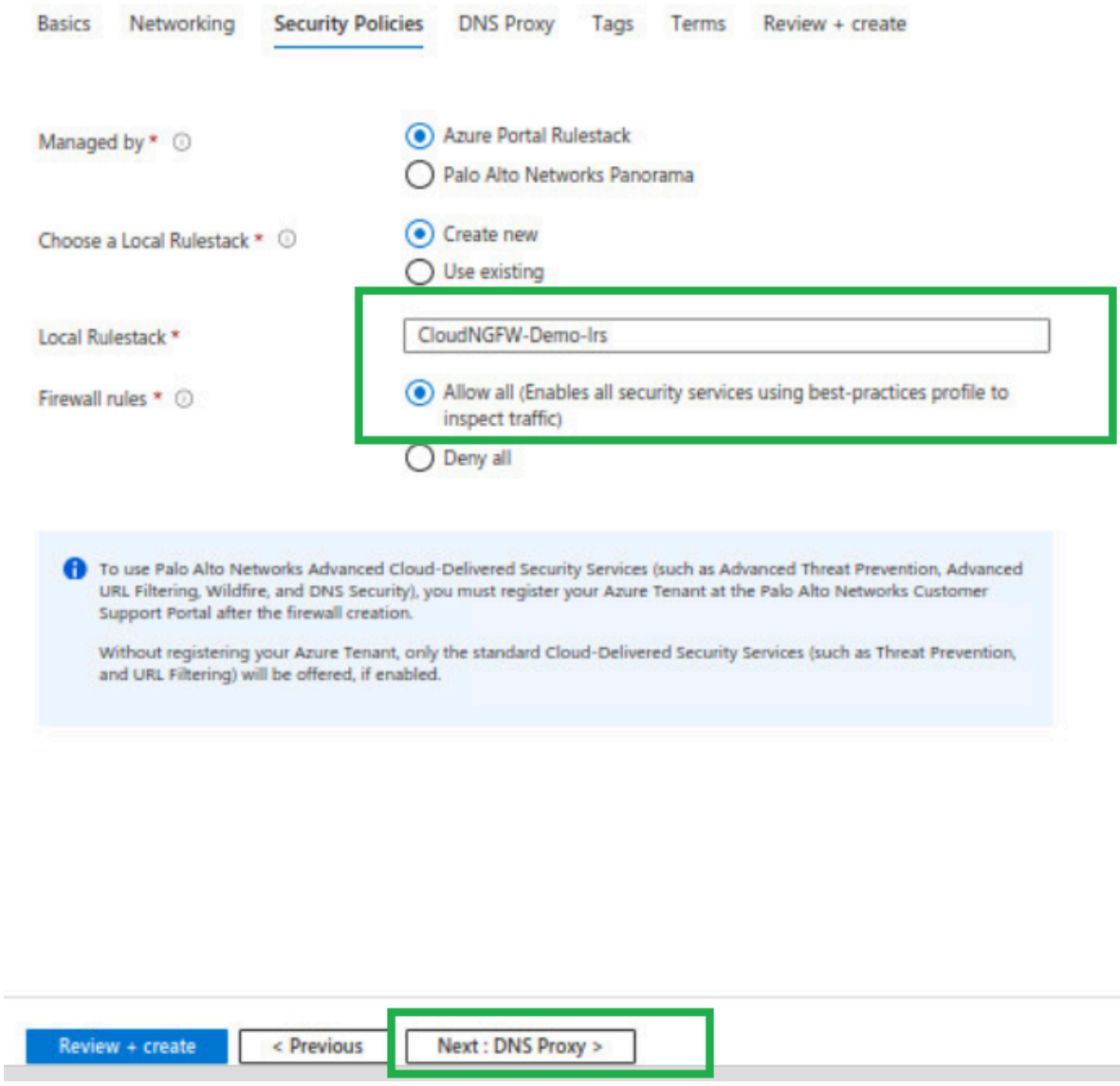


NOTE: You can directly go to "**Terms**" tab and proceed further with creation of cloud NGFW service by leaving remaining settings to defaults

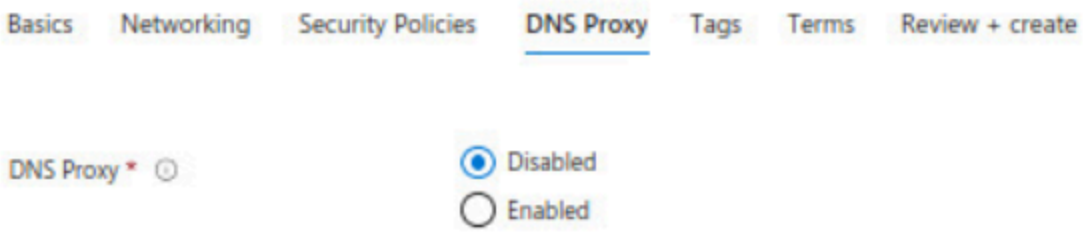
- Review **Security Policies** configuration
  Security policies associated to Cloud NGFW can be managed using Azure Portal Rule stack or Palo Alto Panorama
  For this workshop, we are going to manage policies using local rule stack from within Azure portal.

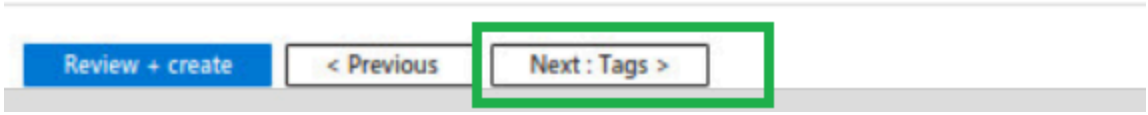
By default Security Policies will be managed using Rule Stack. As part of Cloud NGFW creation a new Local Rulestack will be created with Allow All traffic.

So, leave Security Policies settings to default values and click on "**Next : DNS Proxy >**" to proceed further.

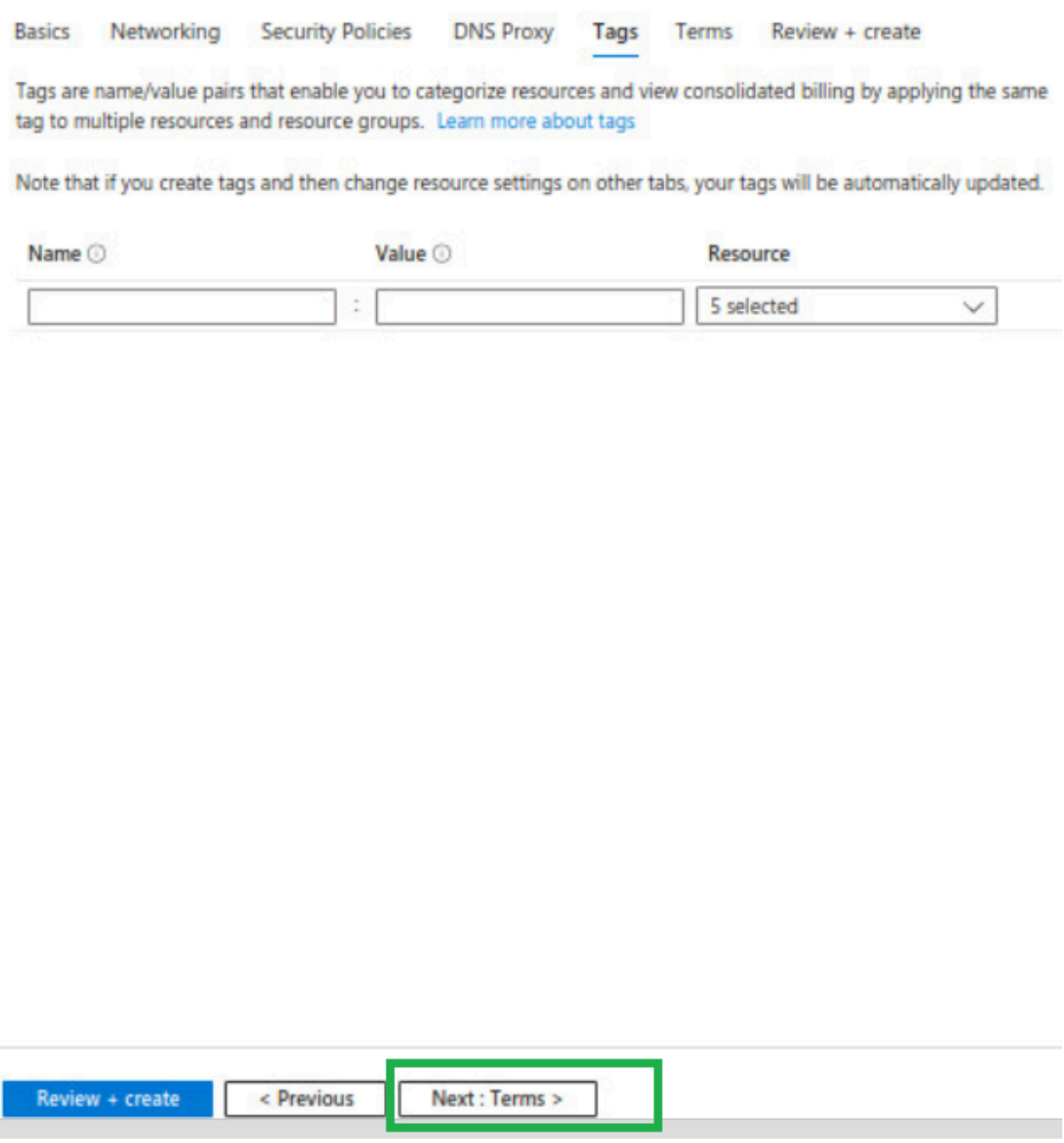


- Review **DNS Proxy** settings
  Cloud NGFW can be configured as a DNS proxy. By default this setting will be disabled.
  Leave the configuration to default and click on "**Next : Tags >**"

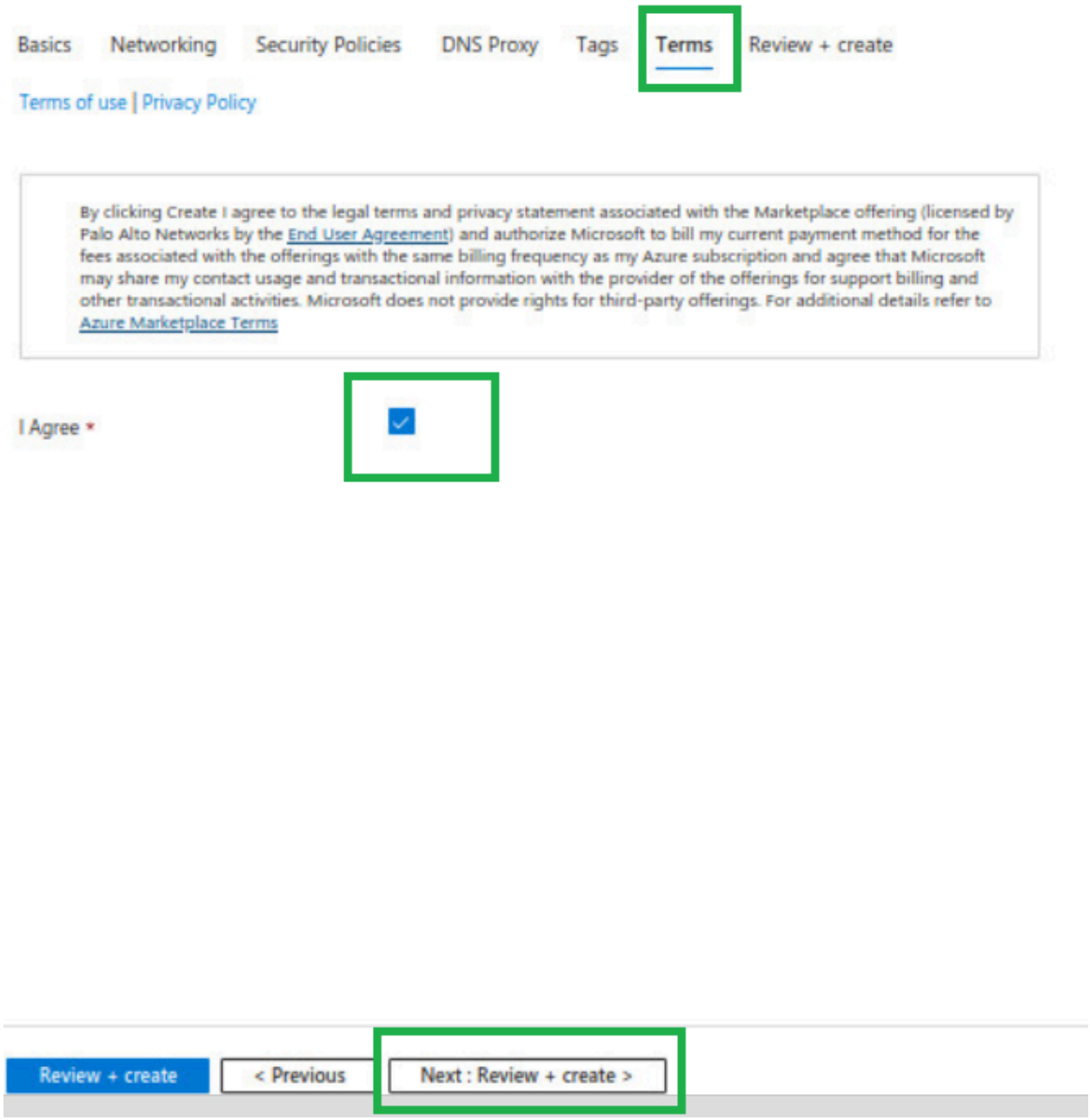




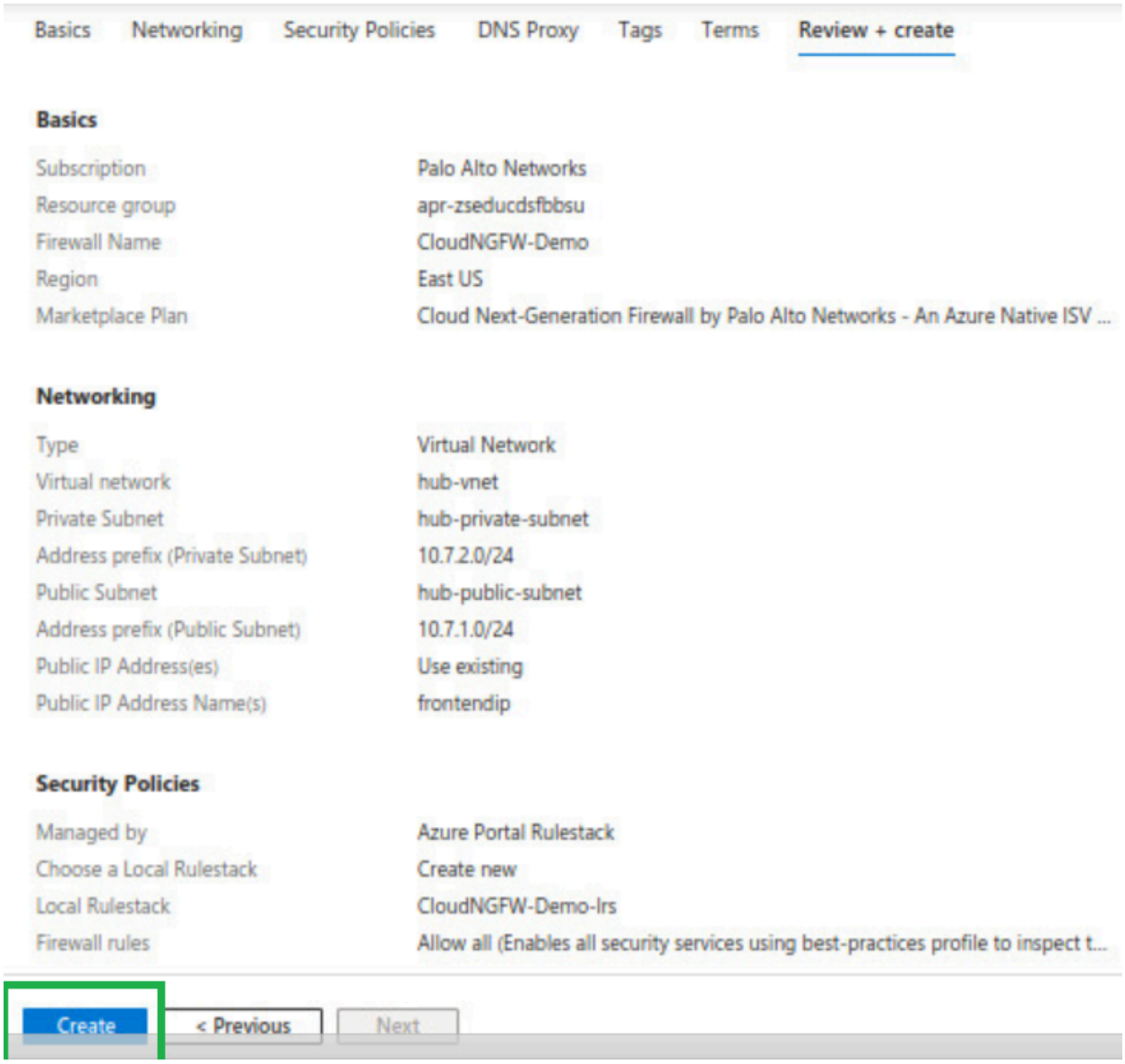
- Review **Tags** settings
  Cloud NGFW resources can be assigned with Tags as per customer's requirement.
  Leave the configuration to default and click on "**Next : Terms >**"



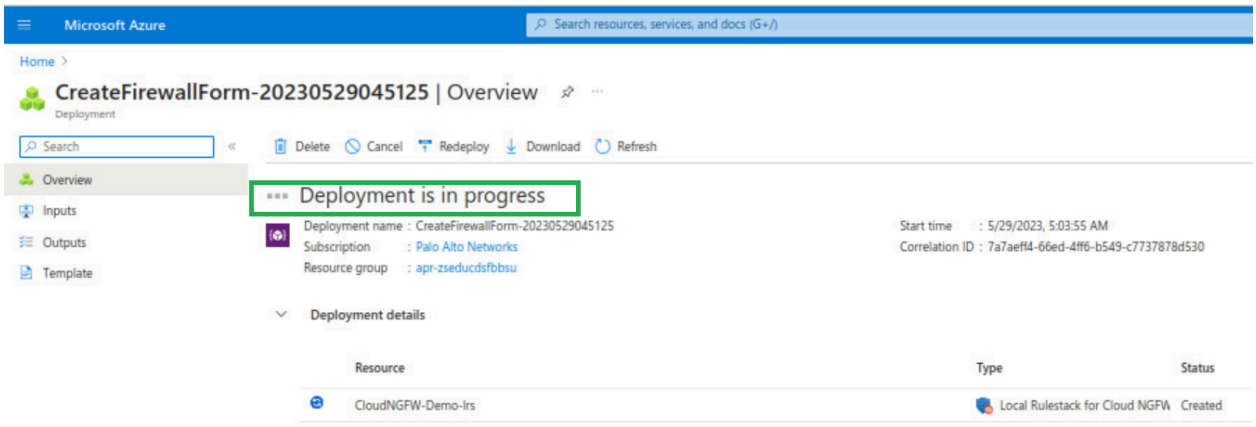
- Accept the terms
  Click on check-box to agree for the terms and conditions as shown below and click on "**Next : Review + Create >**" to proceed further



- Review the configuration and **Create** Cloud NGFW



- You will be presented with below screen



While this is being created, let's discuss in detail about what cloud NGFW is and how it's going to secure workloads on Azure.

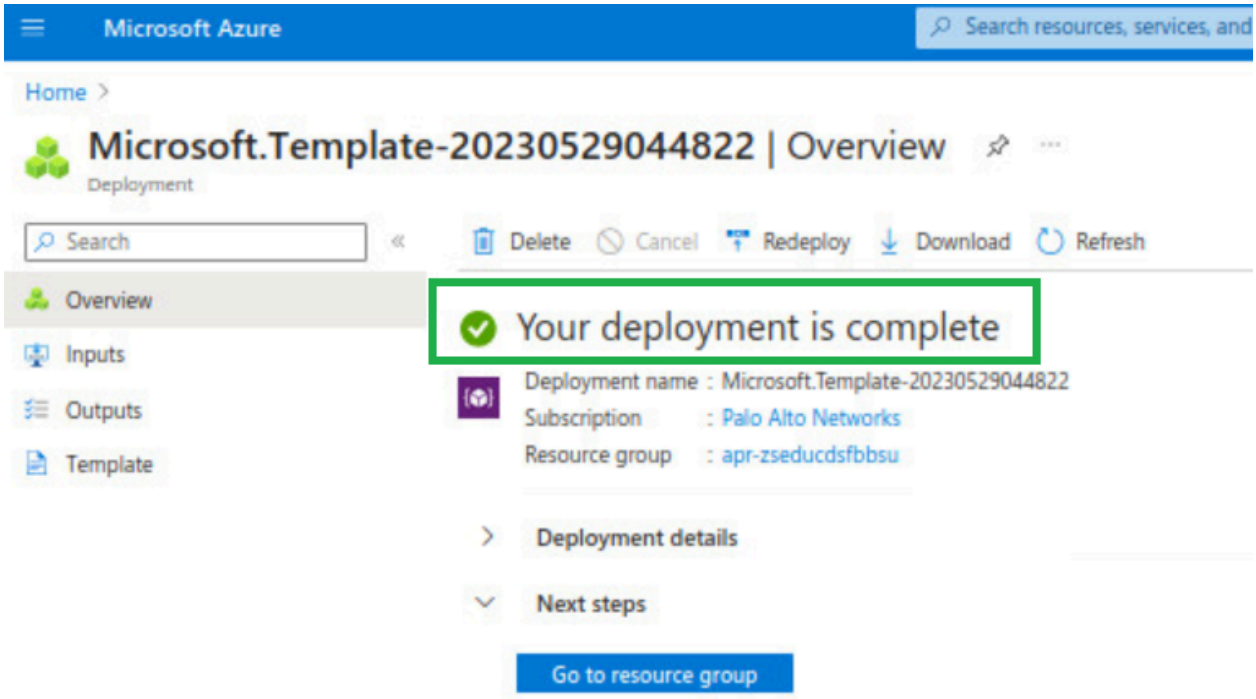
Activity 2: Review ARM template and Cloud NGFW deployment status

Let us now review the deployment status of

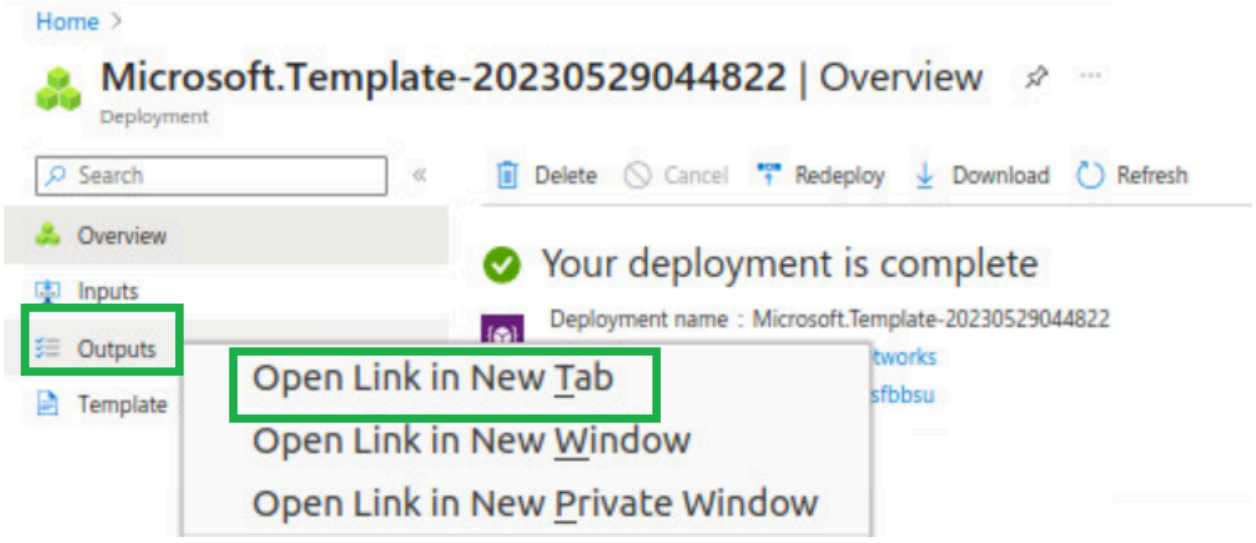
- ARM Template that we deployed in Part-1 Activity 1
- Cloud NGFW creation in Part-2 Activity 1

Task 1 - Review ARM Template deployment status

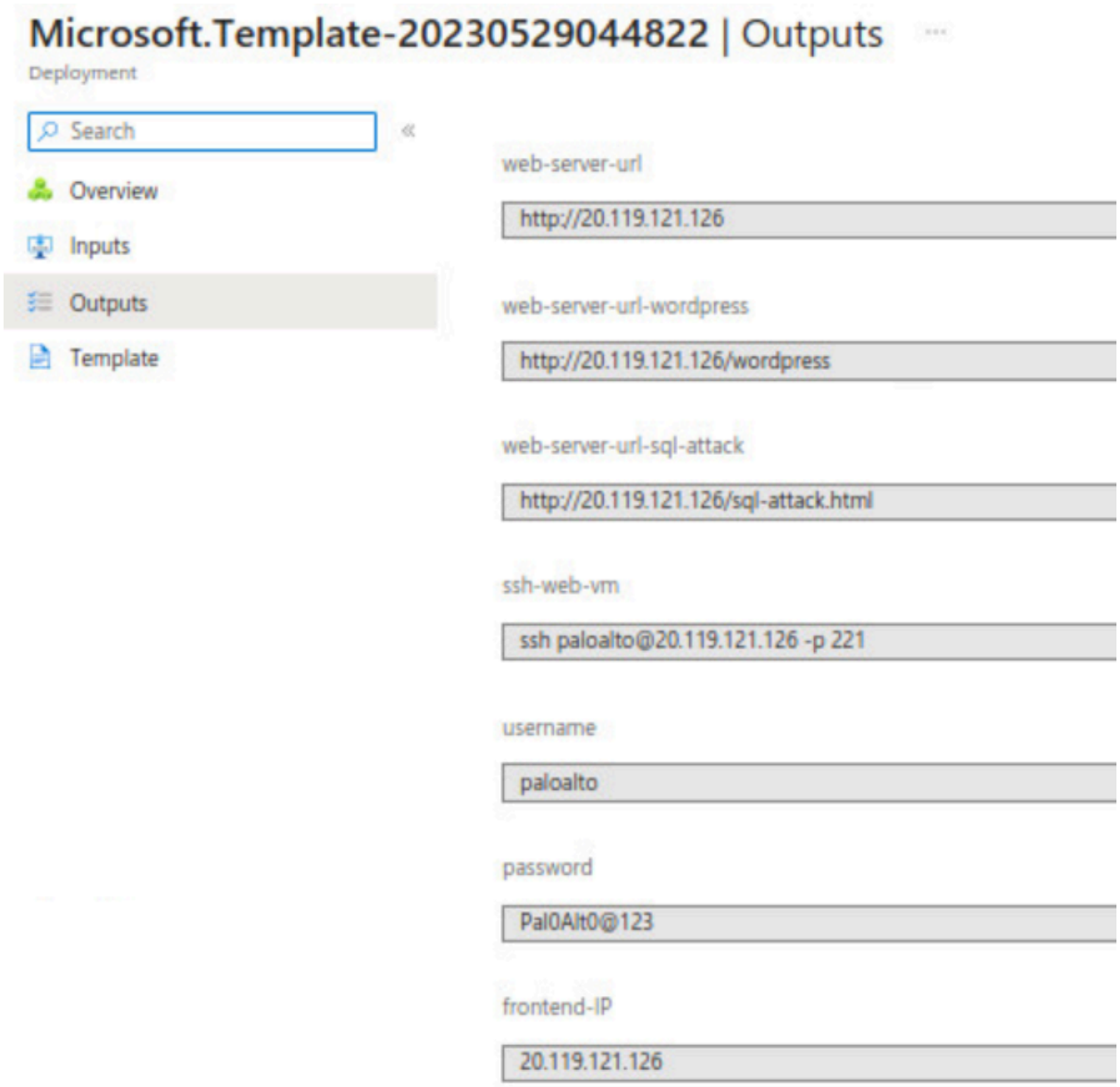
- Go to the first tab on your browser and check if the ARM template deployment has completed. You should see the below mentioned screen on successful deployment.



- Review Outputs of the ARM template deployment
  Right click on the “Outputs” option available on the left menu and open on a new tab to open the outputs page

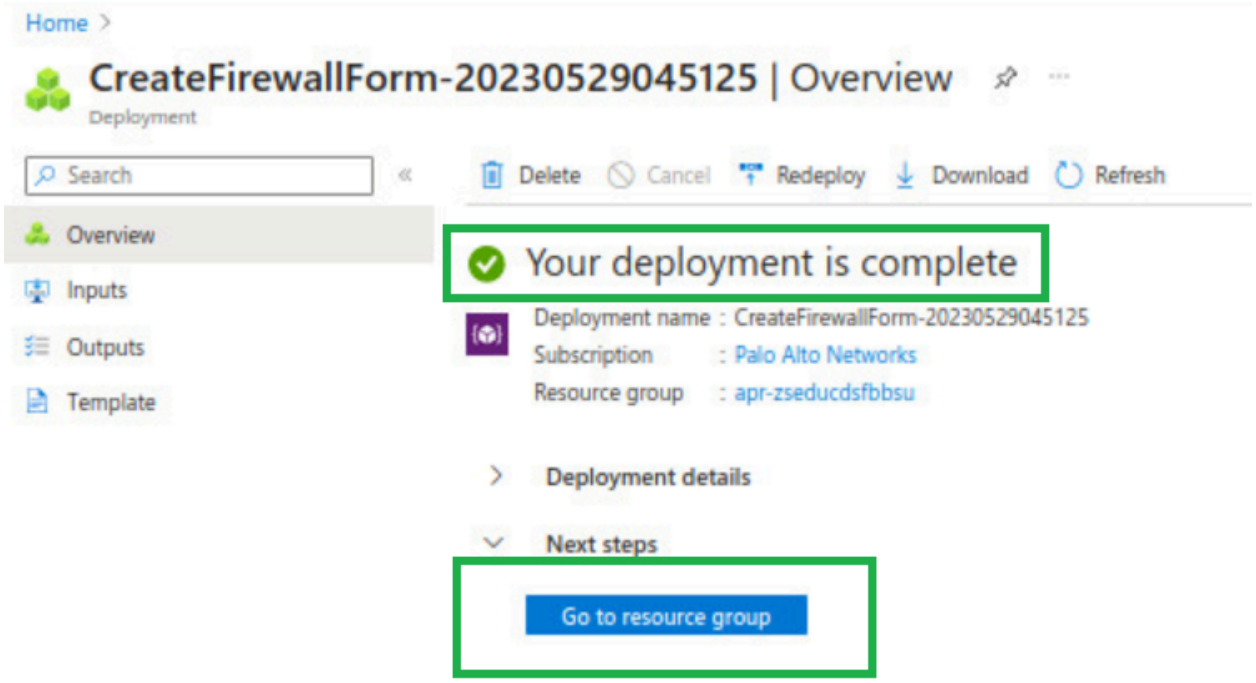


- The Outputs page will contain details as shown below. Keep this tab opened, we are going to use all these outputs to send traffic and initiate attacks through Cloud NGFW

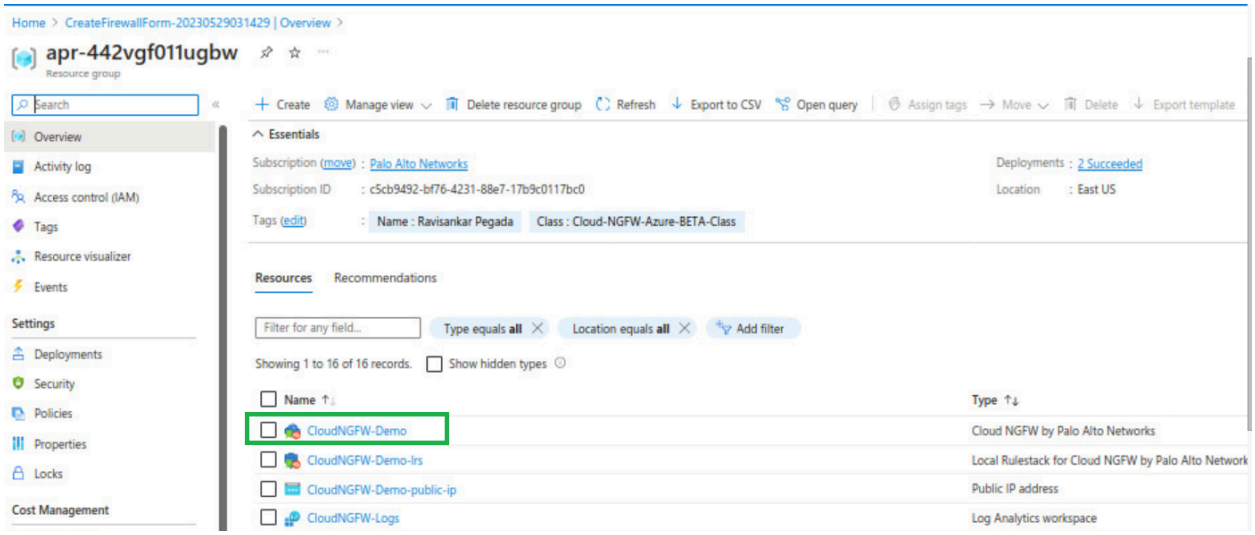


Task 2 - Review Cloud NGFW deployment status

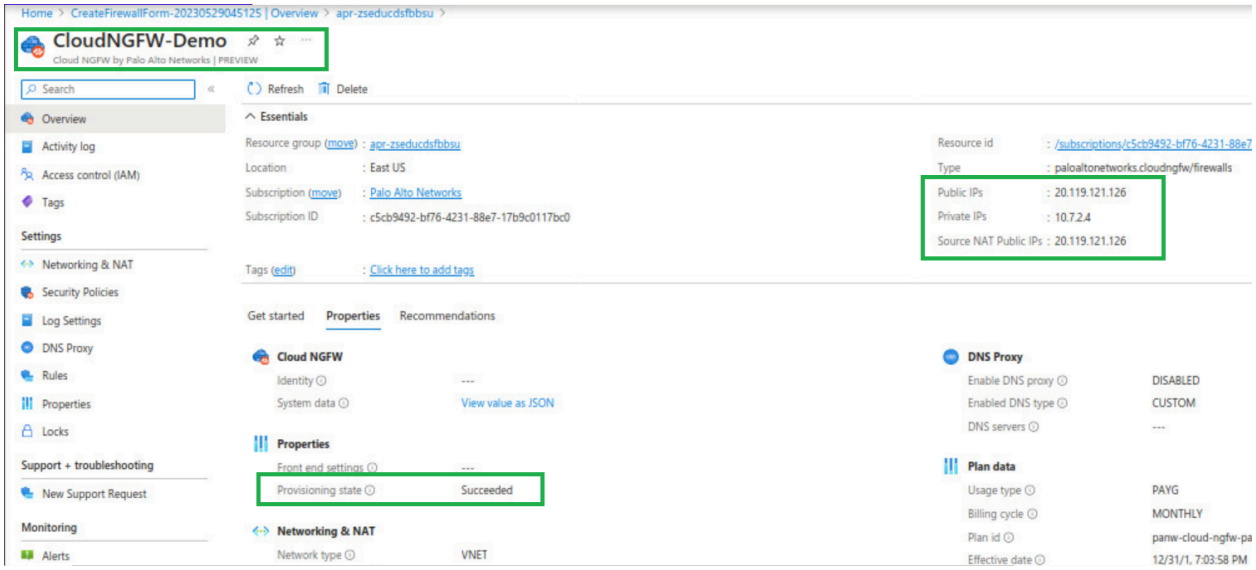
- Go to the tab where we have deployed Cloud NGFW and check for the status and it should be completed as shown below.
- Click on "**Go to resource group**" to review Cloud NGFW and its resources



- Within the resource group, click on "**CloudNGFW-Demo**" resource as shown below



- You should see that Cloud NGFW service got created successfully with Provisioning state as "Succeeded". You will be able to use the Public and Private IP Addresses exposed to route traffic through Cloud NGFW service for inspection

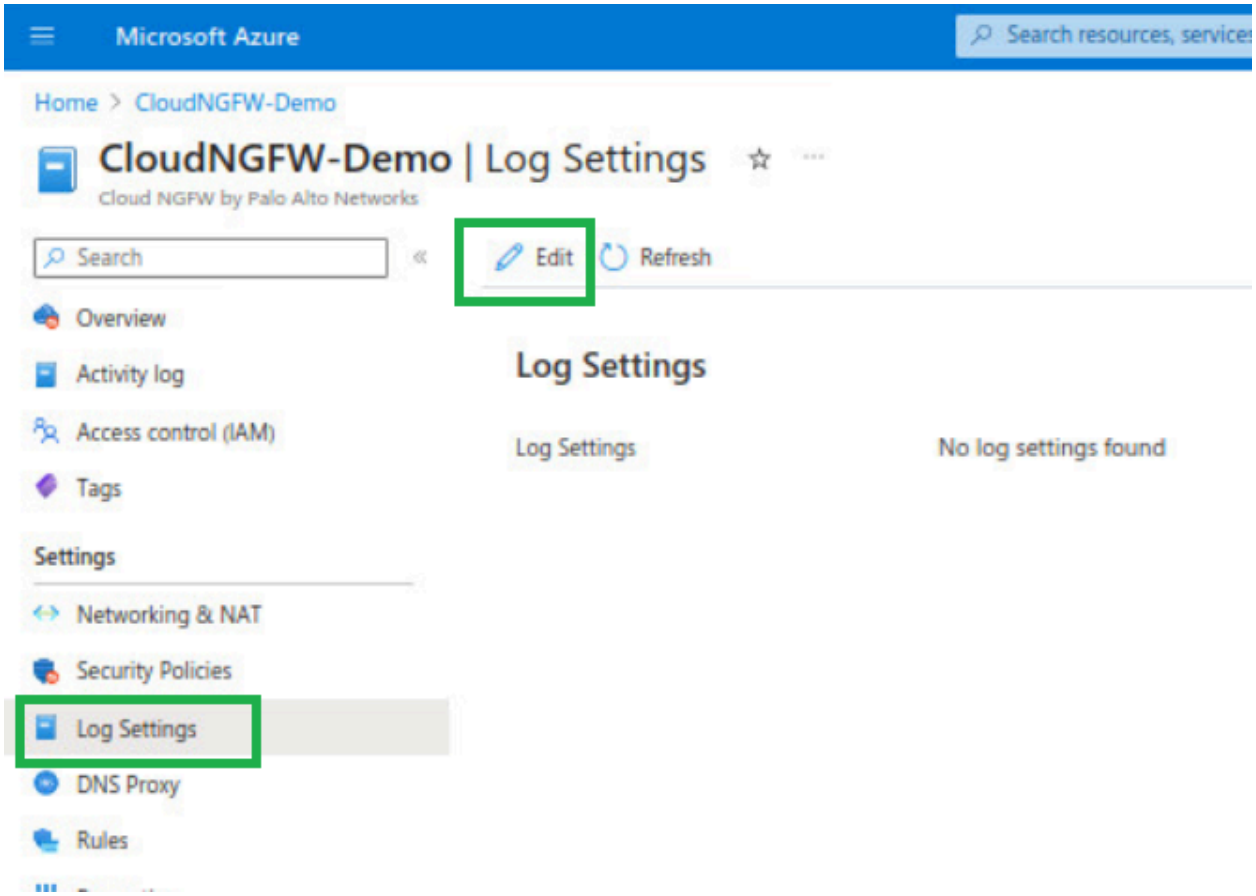


Activity 3: Create Cloud NGFW Service

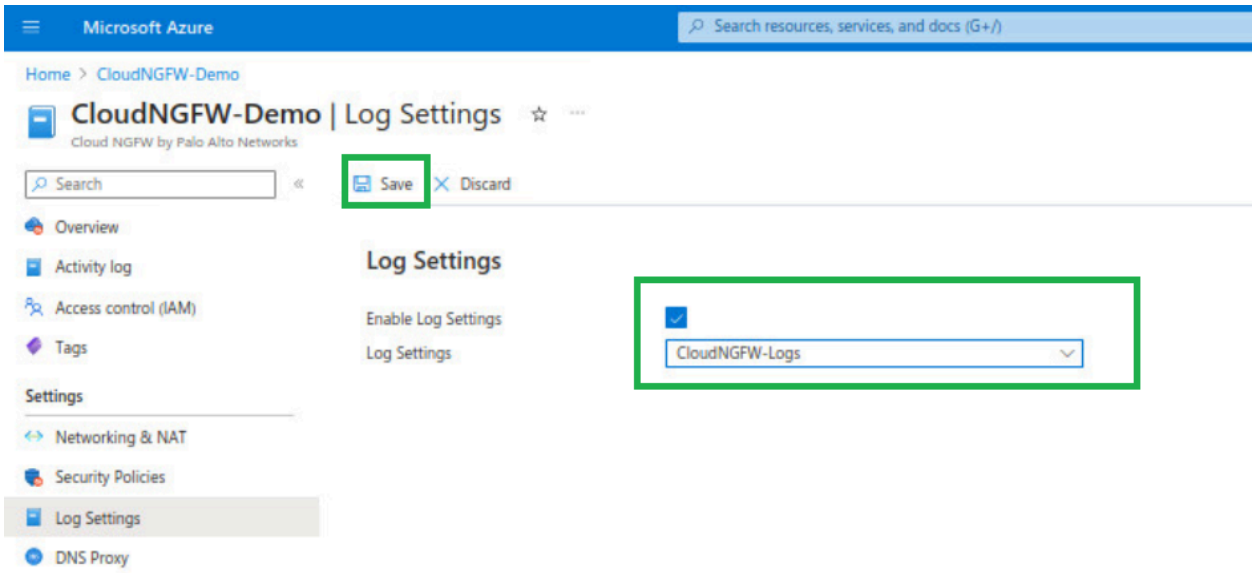
Task 1 - Configure Logging

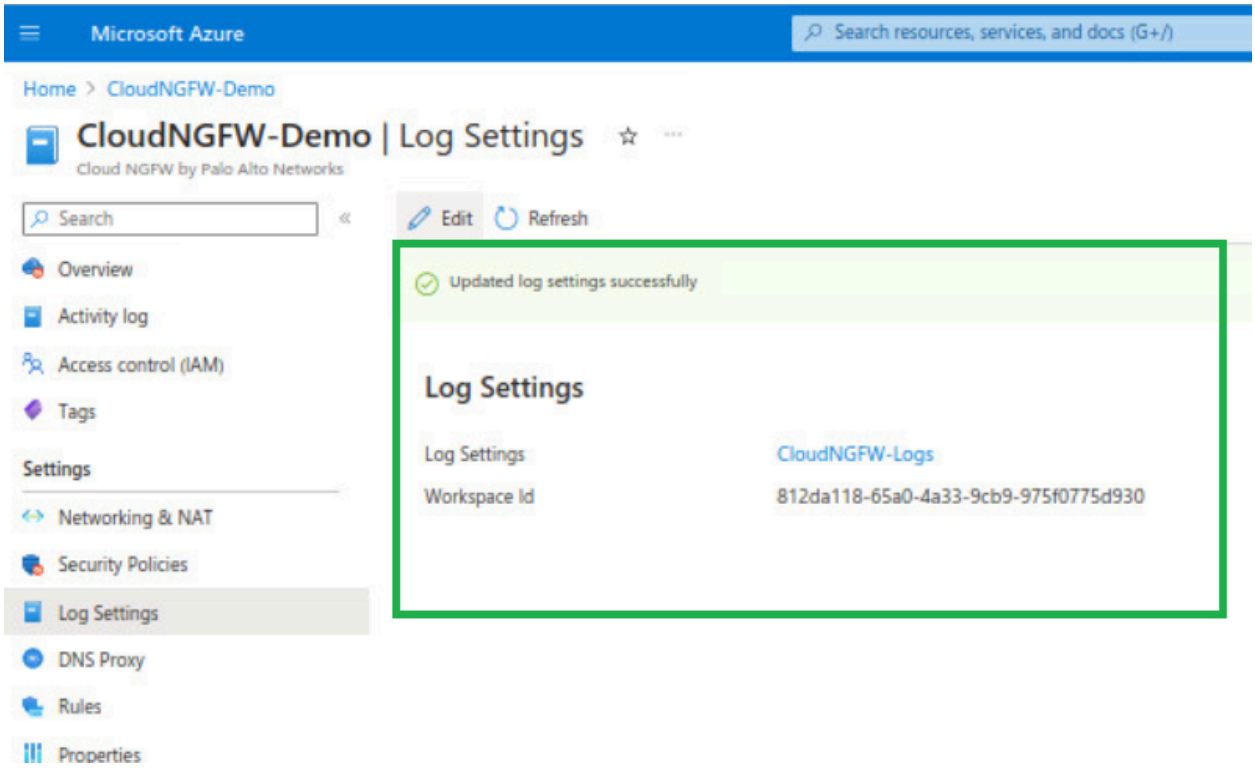
- Cloud NGFW policies can be managed using Azure Portal Rulestack or using Palo Alto Panorama.
- If the policies are managed using Panorama, all the traffic logs can be monitored using Panorama or log collector.
- If the policies are managed using Rule stack, traffic processed by Cloud NGFW service will be logged into Azure Cloud native Log Analytics Workspace.
- In this workshop we are managing policies using Rulestack and hence we are going to configure Log settings to redirect logs to Azure Log Analytics workspace

- Go to Cloud NGFW created in above step and navigate to “**Log Settings**” on left menu and click on “**Edit**” option as shown below



- Enable Log Settings by clicking on on the check-box and select the Log Analytics workspace "**CloudNGFW-Logs**" from the drop down as shown below and click on **Save**

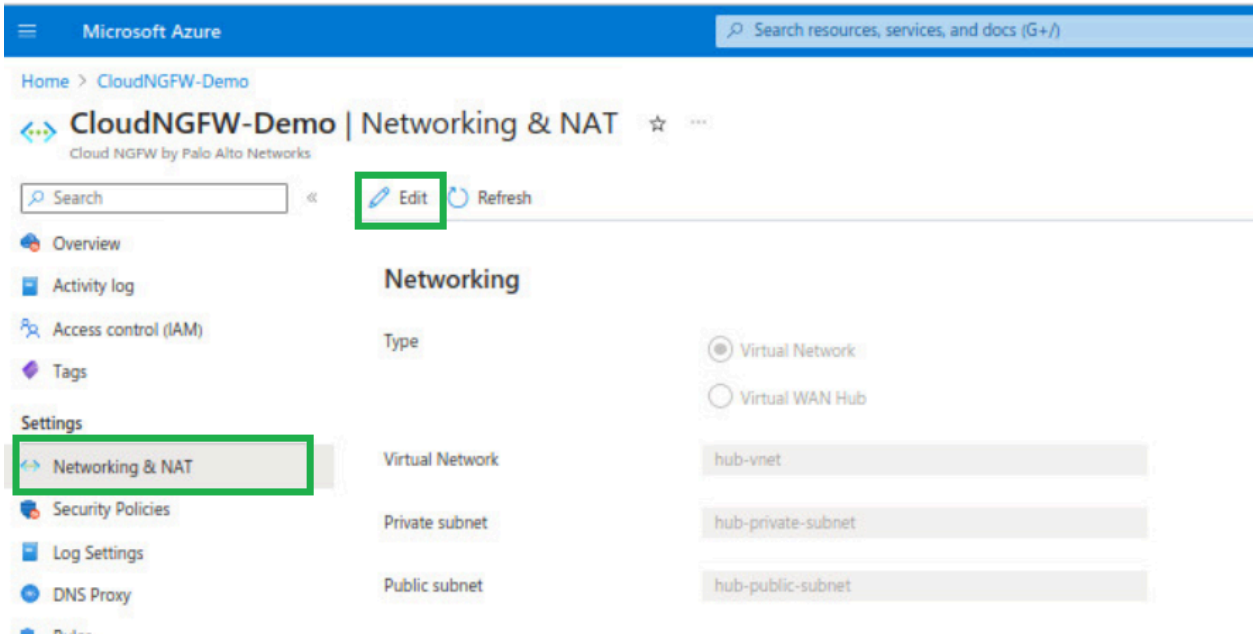




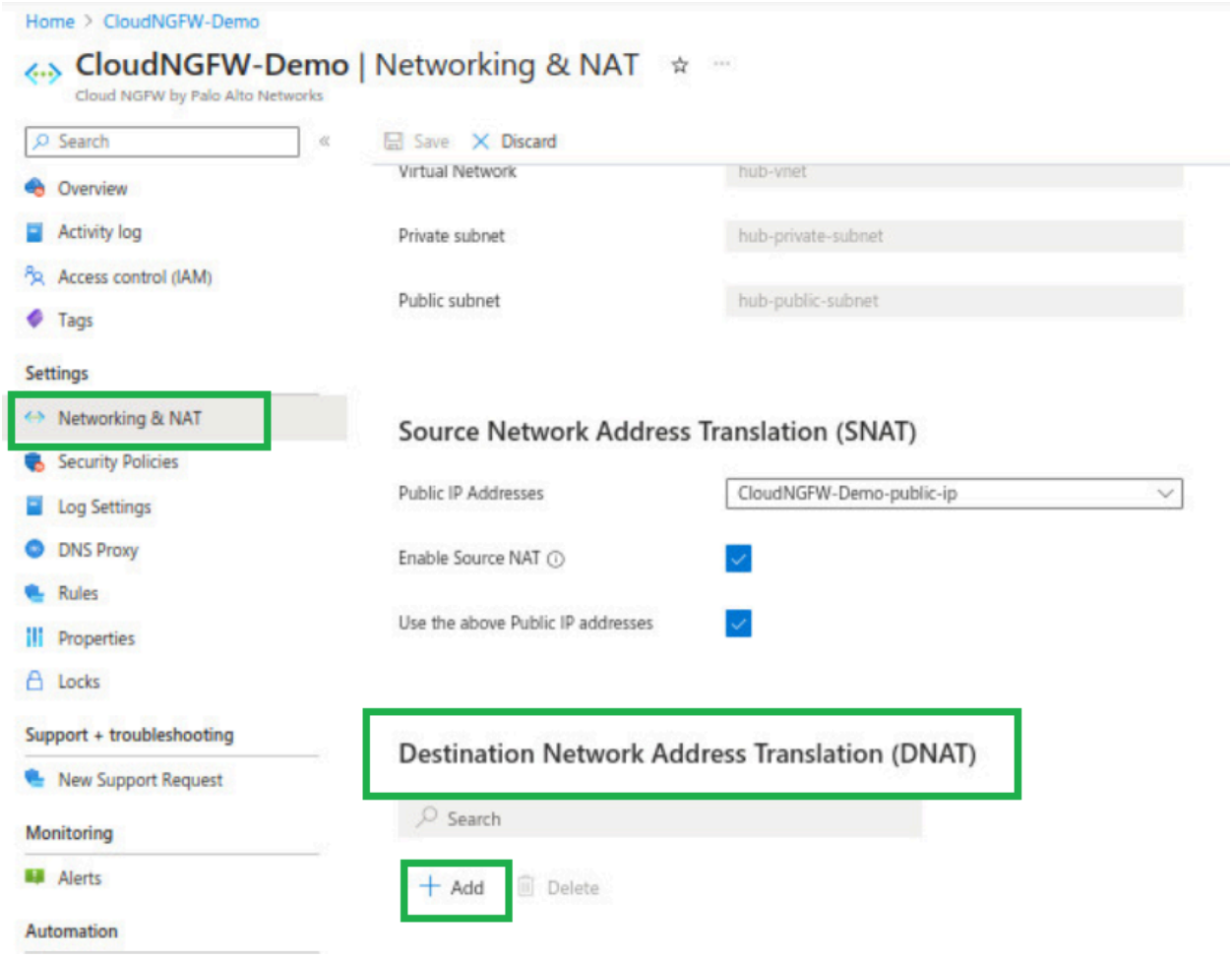
Task 2 - Configure Destination NAT

- Configure Destination rules on Cloud NGFW
    - To provide secure inbound access for the Web application running in Spoke VNet-1 peered with Hub VNet
    - To provide SSH access to the Web server

- To configure Destination NAT, navigate to "**Networking & NAT**" and click on **Edit** option

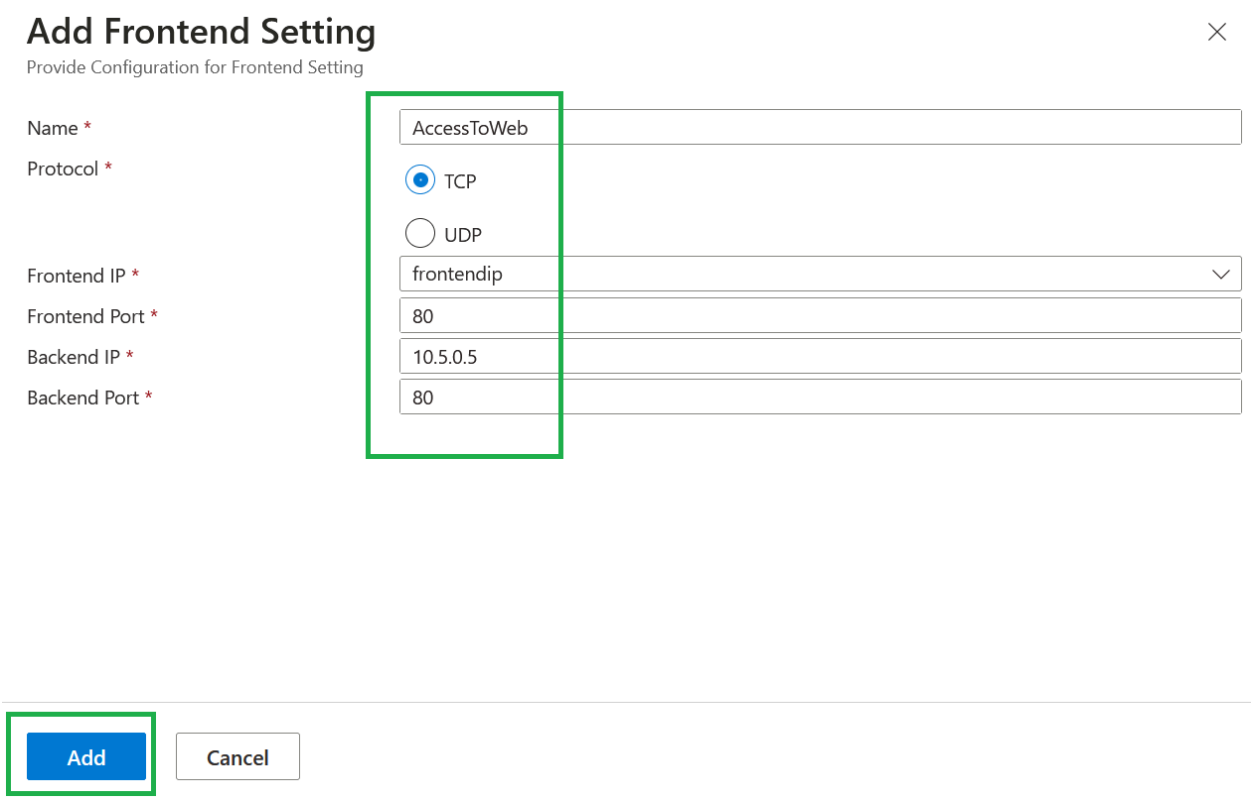


- Scroll down and click on "**+Add**" option within Destination NAT section as shown below to add destination nat rule(Frontend setting) to provide access to Web server running in Spoke1 VNet

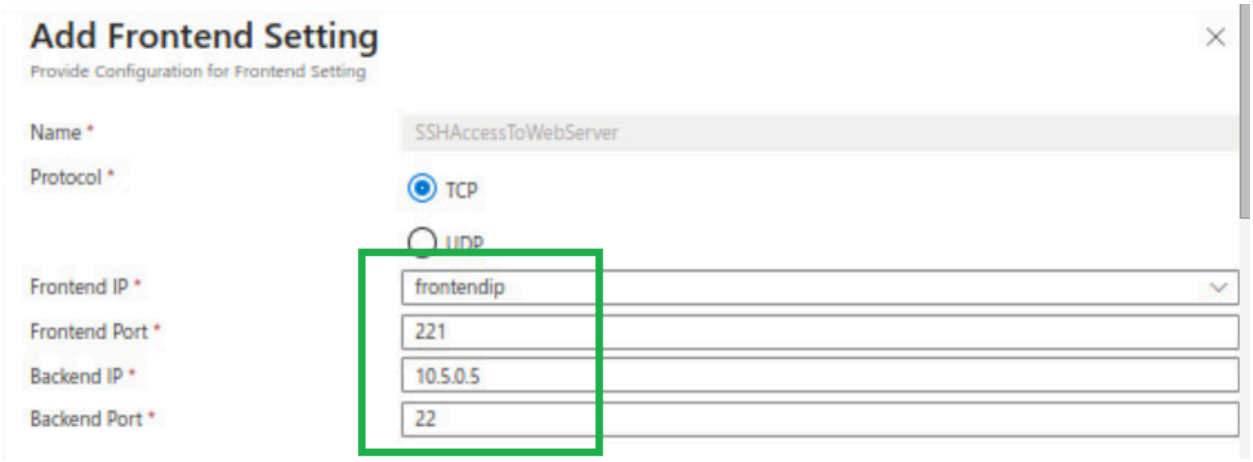


- As per the deployment topology, Web Server is assigned with “10.5.0.5” IP Address. Add destination NAT rule by configuring the Frontend settings as shown below
    - Provide the Name “AccessToWeb”
    - Keep the protocol as TCP
    - Select the Frontend IP as the Public IP address associated with the Cloud NGFW from the drop-down.
    - Specify the Frontend Port as 80
    - Backend IP address is nothing but the IP address of Web Server(10.5.0.5)
    - Backend Port will be 80

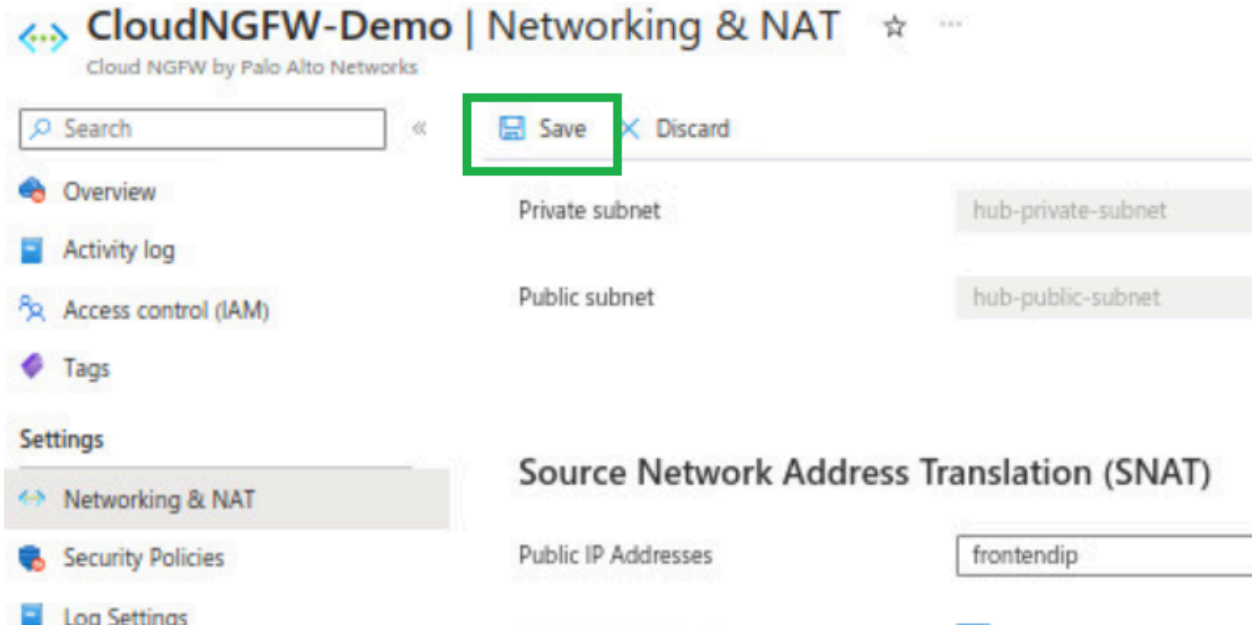
  Click on Add after providing all the above specified information to add destination NAT rule



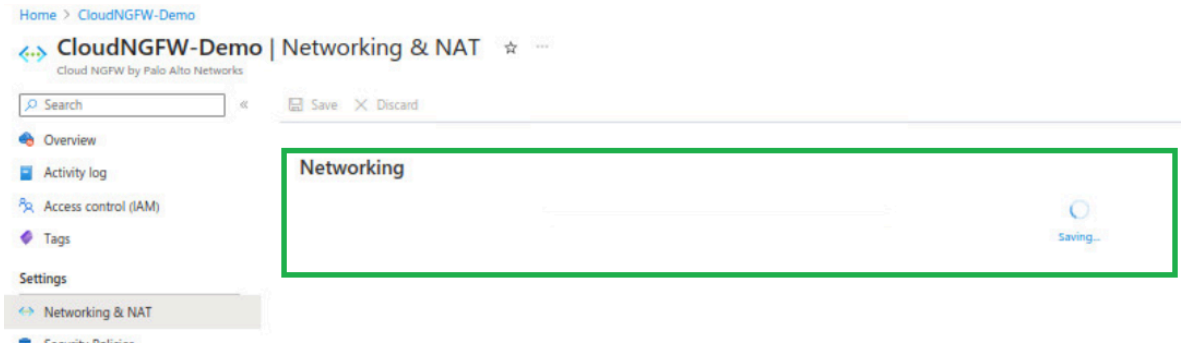
- Add one more destination nat rule to provide SSH access to the Web server.
    - Provide the Name “SSHAccessToWeb”
    - Keep the protocol as TCP
    - Select the Frontend IP as the Public IP address associated with the Cloud NGFW from the drop-down.
    - Specify the Frontend Port as 221
    - Backend IP address is nothing but the IP address of Web Server(10.5.0.5)
    - Backend Port will be 22
    -



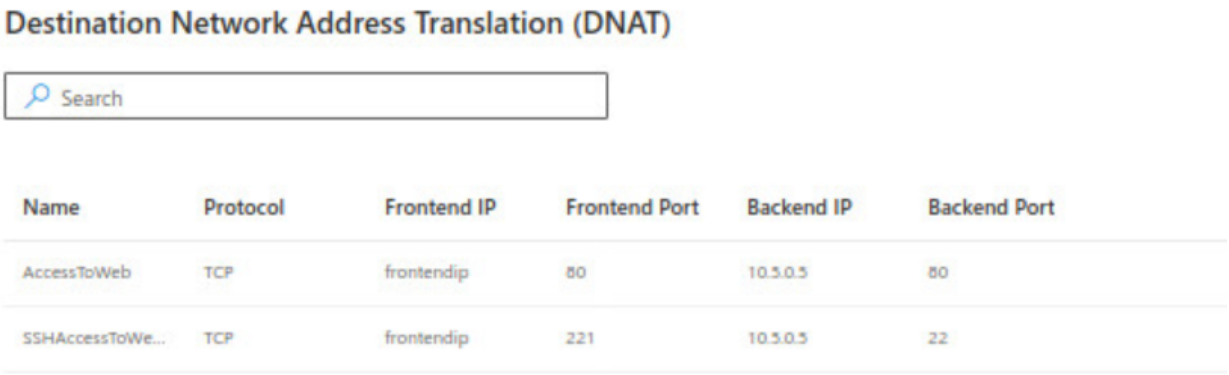
- After adding destination nat rule, click on **Save** to save the Networking & NAT configuration



- You will be presented with the below mentioned screenshot. This process will take around a minute

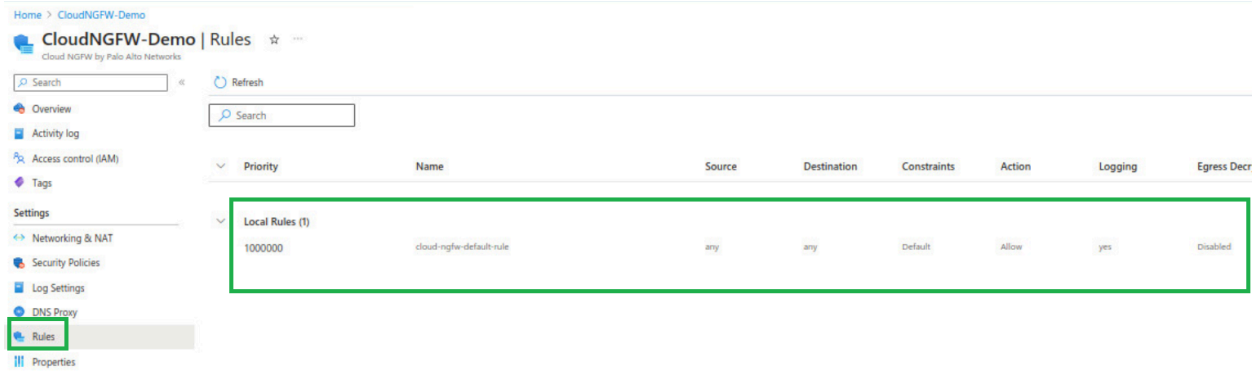


- On successfully saving the configuration, the destination NAT rules will be seen as shown below



Task 3 - Review default rule configured

Cloud NGFW security policies will be managed using Local Rule stack and the rule stack is configured with a default rule to allow all traffic as shown below.



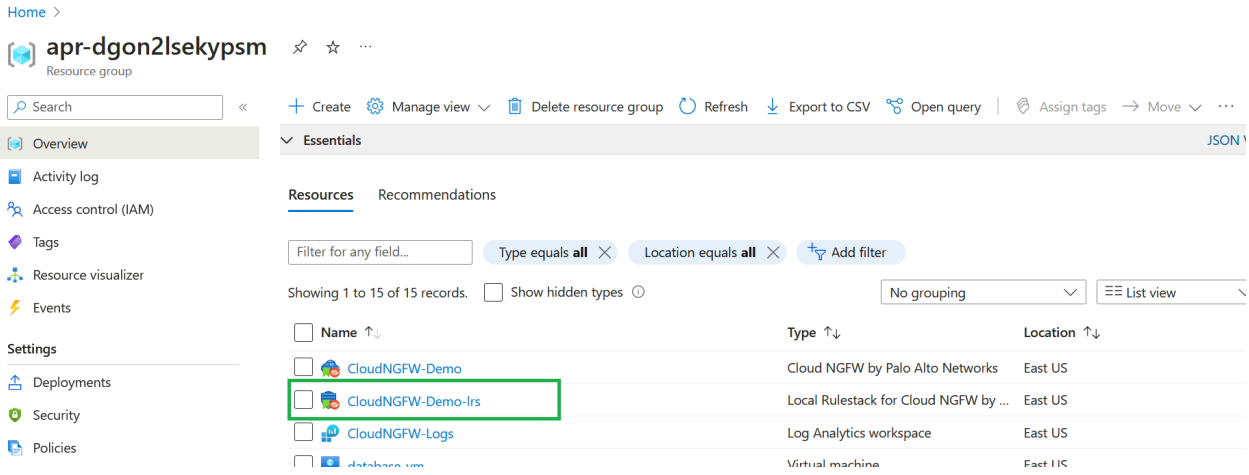
Task 4 - Configure Firewall Policies using Local Rulestack

In this task we are going to add additional rules to the Rulestack.

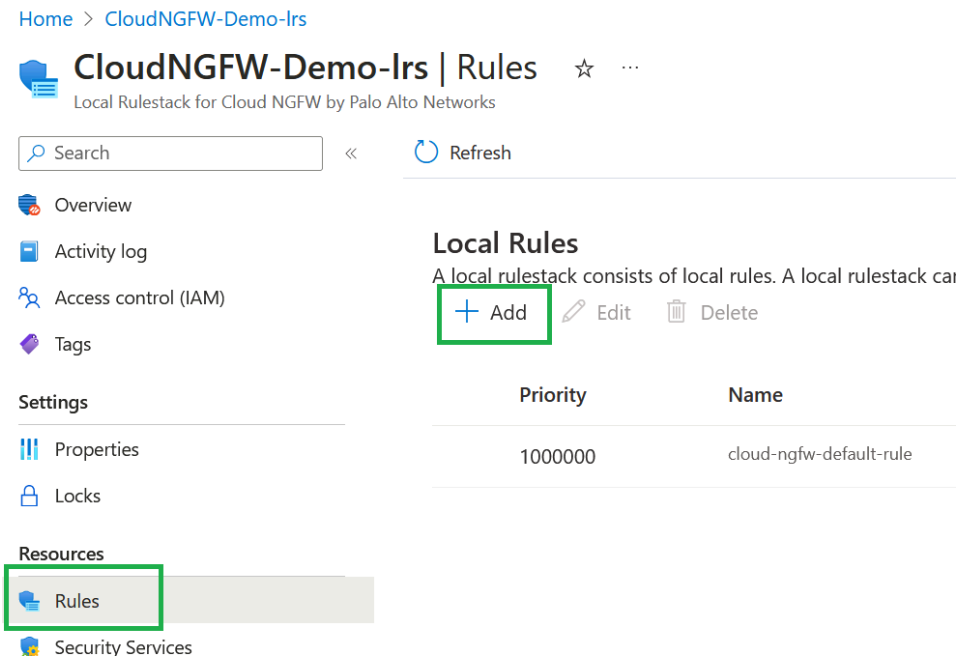
- Add rule to block Mysql from web to db servers
- Add a rule to block Social networking category

Add rule to block Mysql from web to db servers

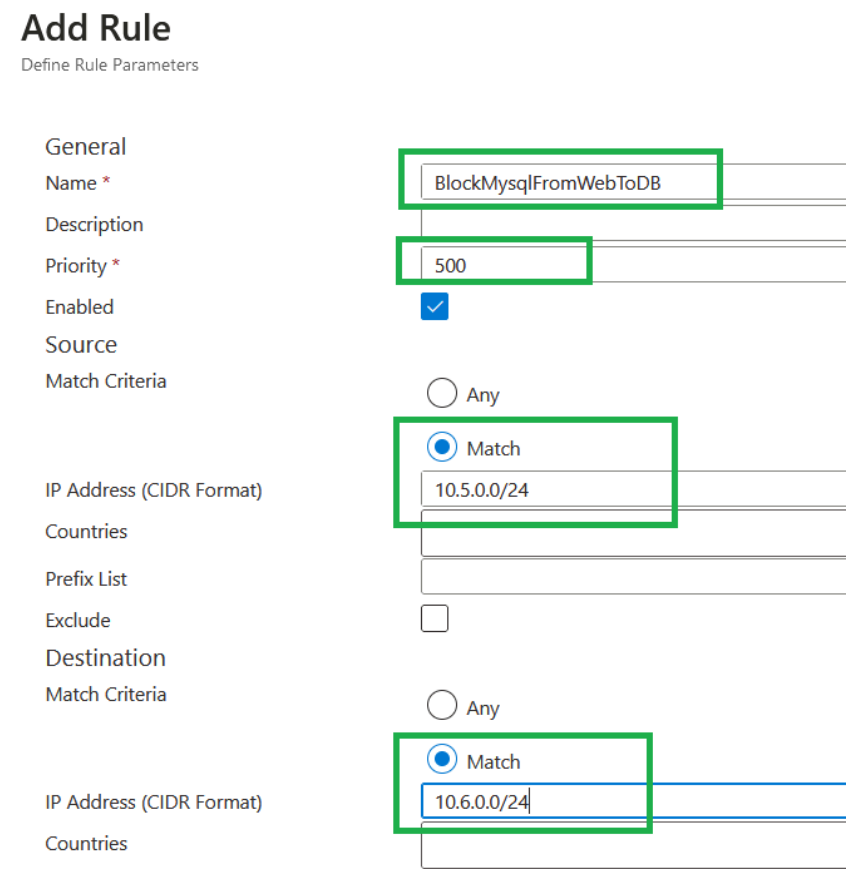
- Go to your resource group and right-click on "**CloudNGFW-Demo-lrs**" to open the local rule stack created

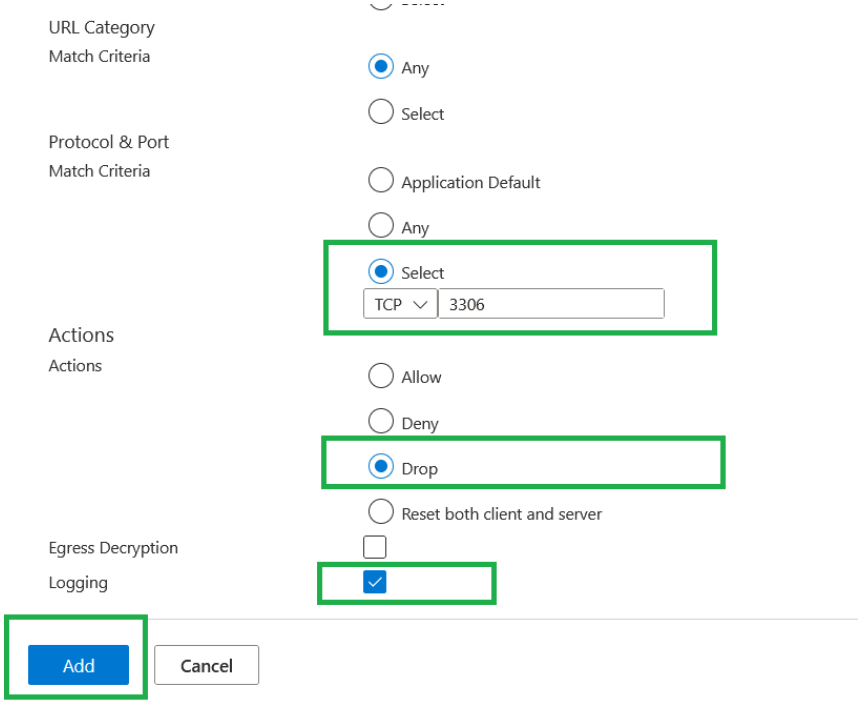


- Go to Rules on the left menu and click on on "Add" to add a new rule as shown below



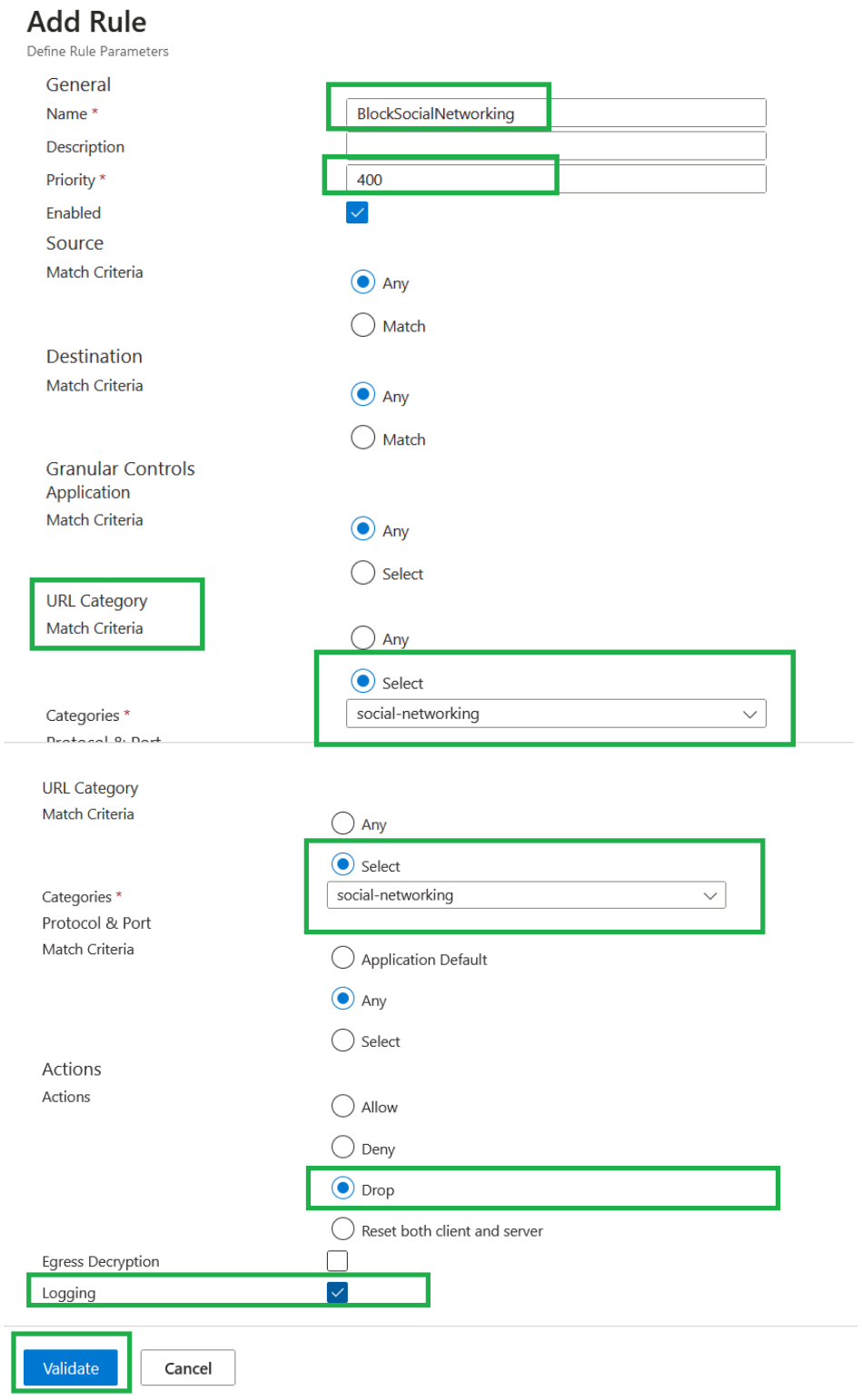
- Provide the name, priority, Source(Web) and destination(DB) subnet match as per the deployment topology. Select TCP port as 3306(mysql) with action as drop and enable logging as shown below.





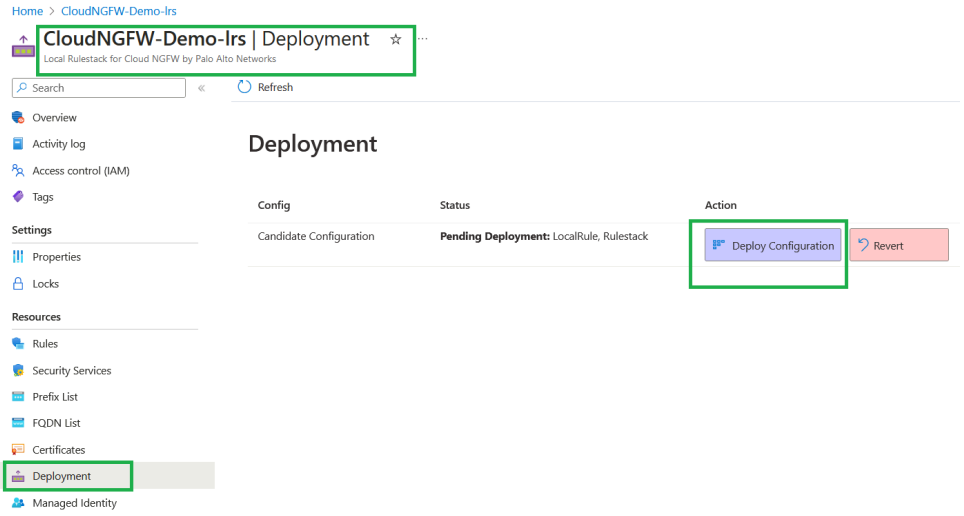
Add rule to block Social Networking

Within the Rules page, click on “Add” to add a new rule.
Provide the Name, select the URL Category as ‘**social-networking**’, action as **drop** and enable logging as shown below.
Click on **Validate** and then **Add** to add this rule

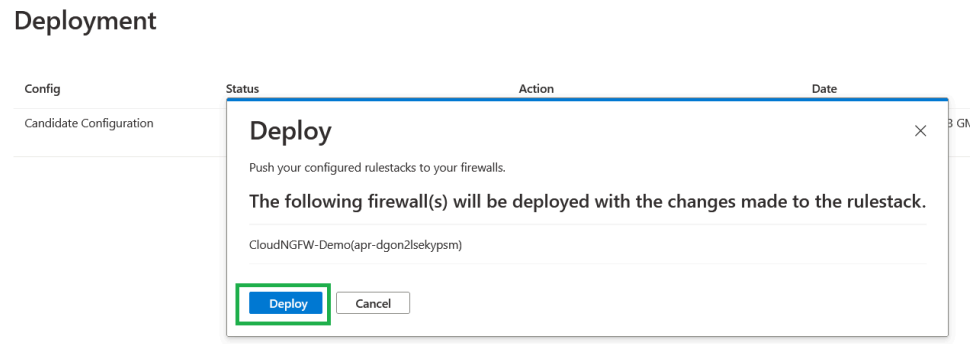

Add Rule
Define Rule Parameters
General
Name *
BlockSocialNetworking
Description
Priority *
400
Enabled
Source
Match Criteria
Any
Match
Destination
Match Criteria
Any
Match
Granular Controls
Application
Match Criteria
Any
Select
URL Category
Match Criteria
Any
Select
Categories *
social-networking
URL Category
Match Criteria
Any
Select
Categories *
social-networking
Protocol & Port
Match Criteria
Application Default
Any
Select
Actions
Actions
Allow
Deny
Drop
Reset both client and server
Egress Decryption
Logging
Validate
Cancel

Deploy configuration

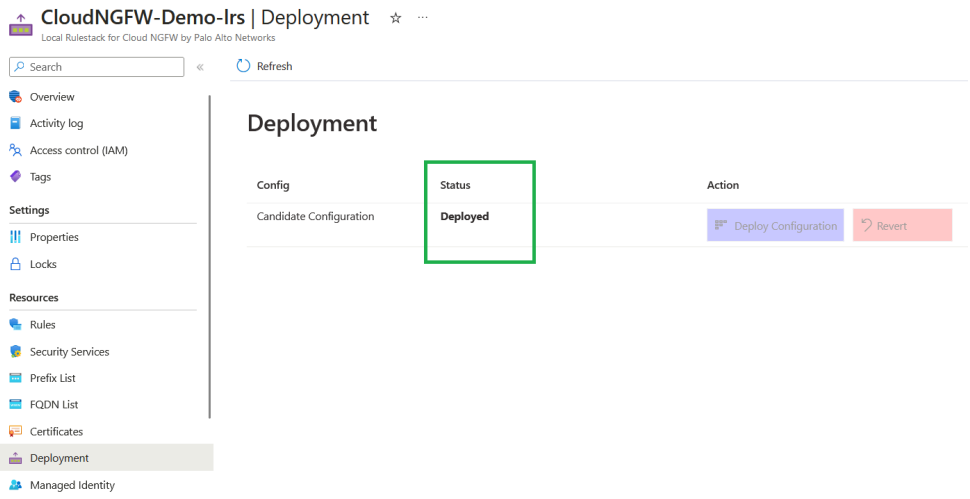
Within Local Rulestack page, goto Deployment on the left menu and click on “Deploy configuration” inorder to deploy the newly added rules onto Cloud NGFW service



You will be presented with the below mentioned screen where you need to click on “**Deploy**” to deploy the configuration.



On Successful deployment, you should see the status as “**Deployed**” as shown below

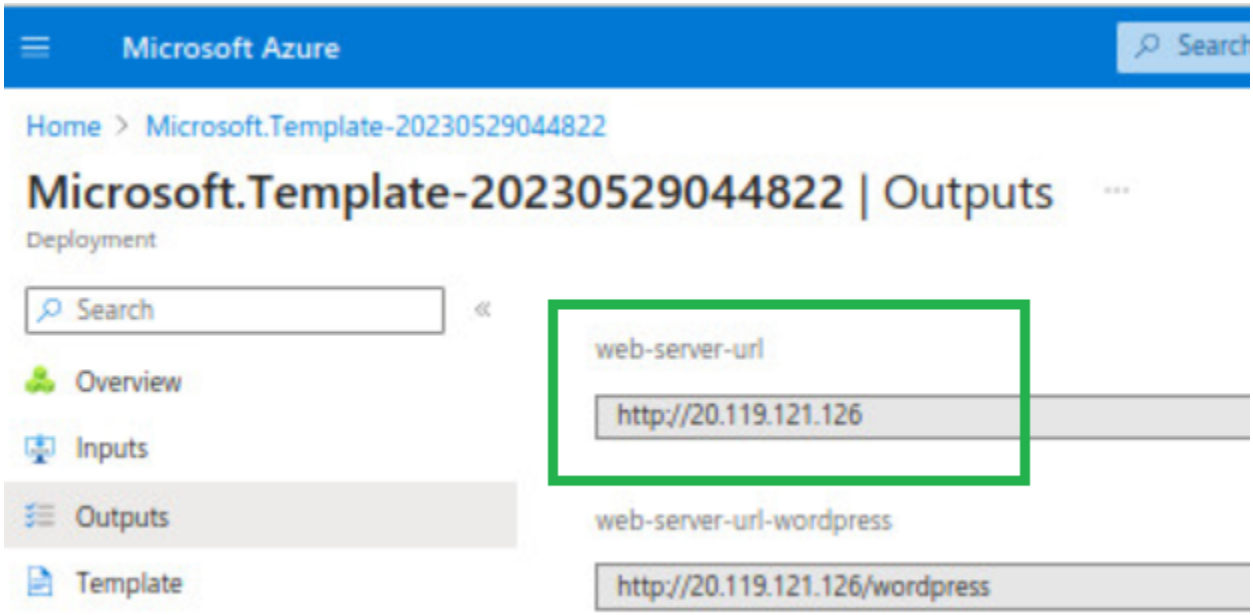


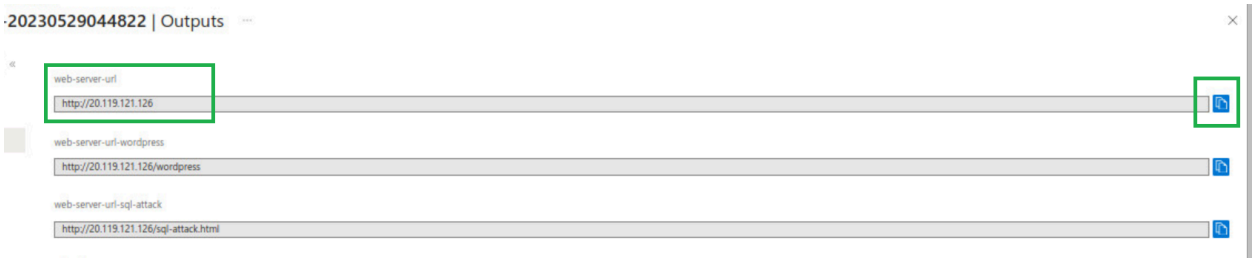
Part-3 : Secure user traffic using Cloud NGFW for Azure

Activity 1: Verify secure inbound access to Web Server

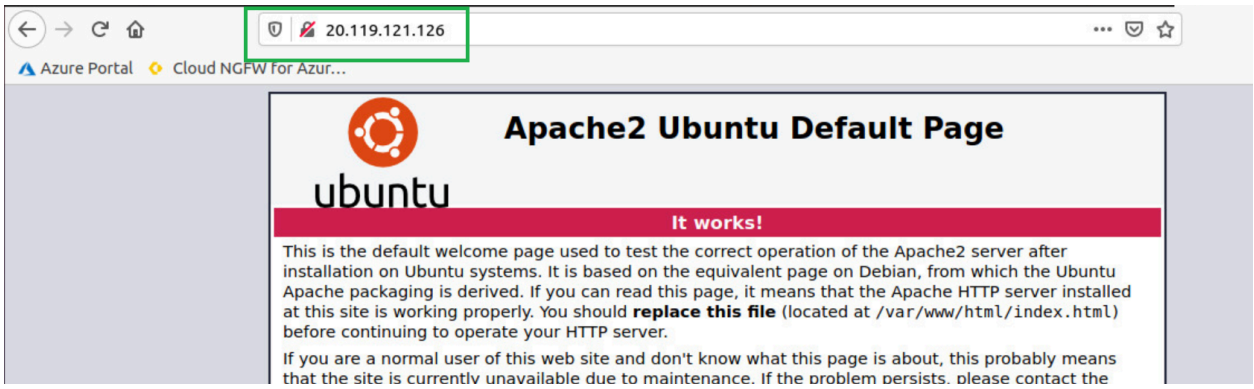
Task 1 - Access Web Server through Cloud NGFW

- Go to the Outputs of ARM Template deployment and copy "**web-server-url**"





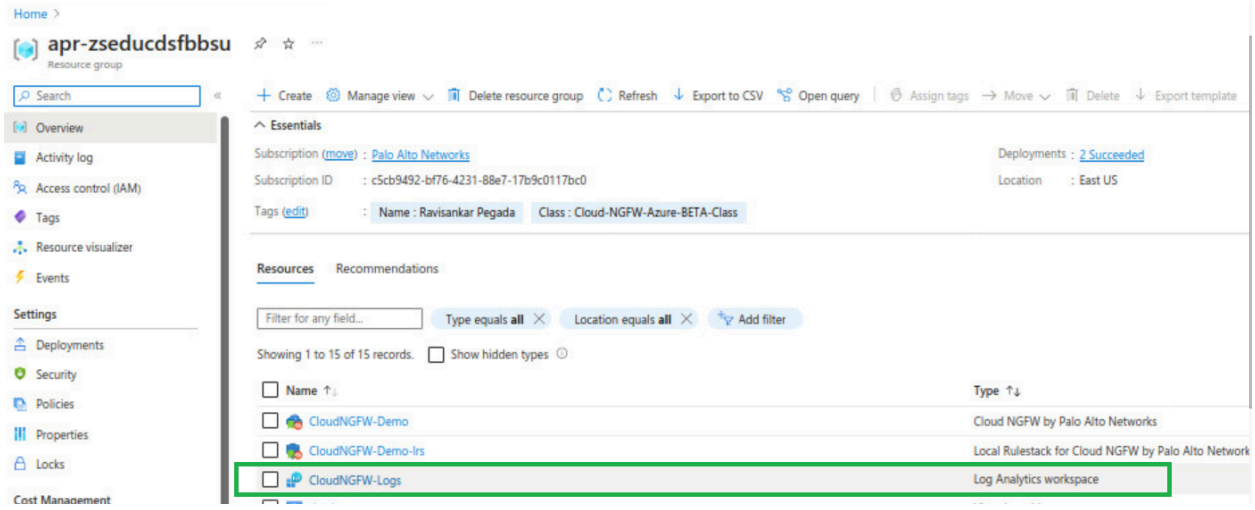
- Use the copied url and access the web server from your browser or from the browser within the student desktop. You should see the web page as shown below.



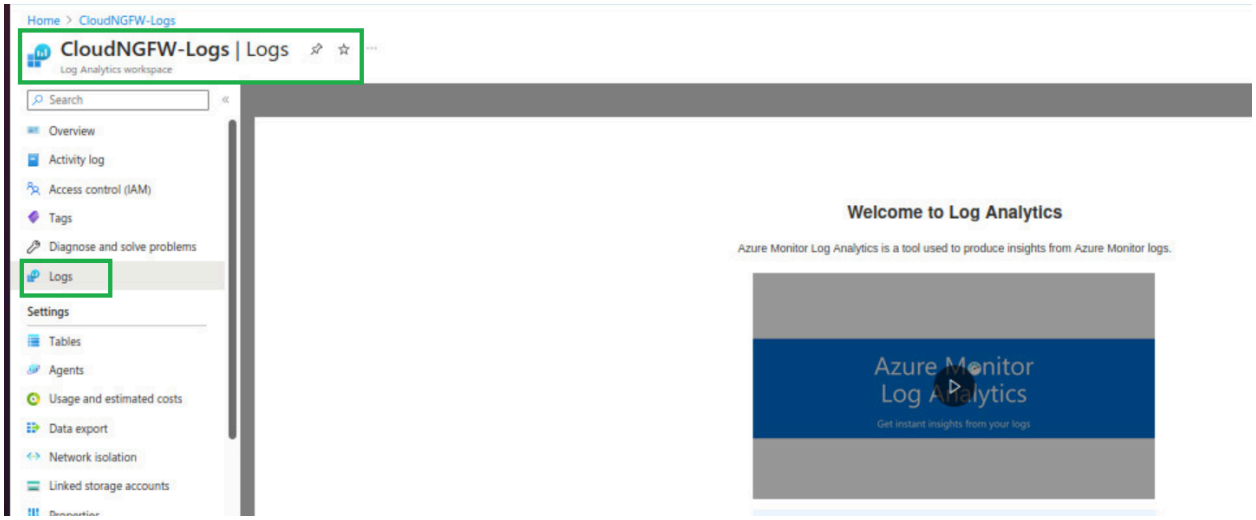
- This indicates that the web server is accessible from internet

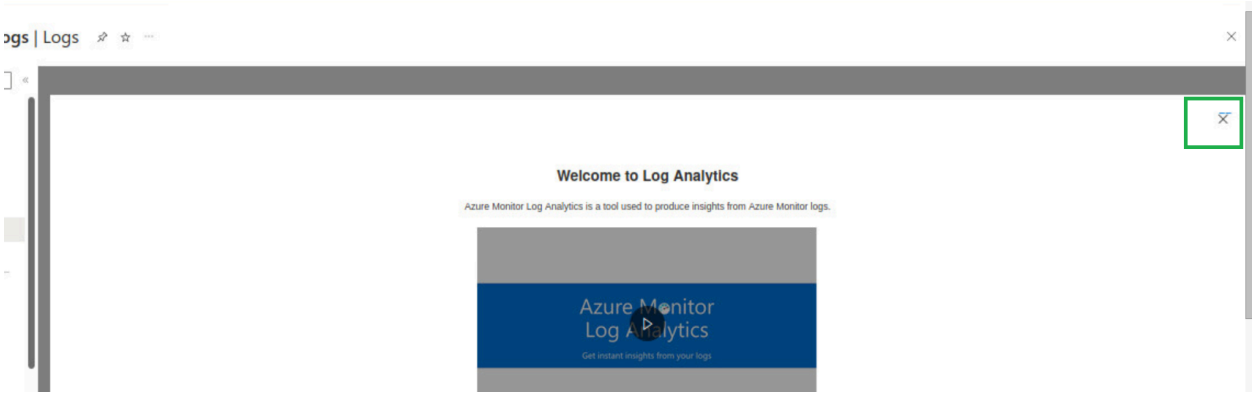
Task 2 - Verify Cloud NGFW logs using Log Analytics workspace

- Click on "**CloudNGFW-Logs**" to open Log Analytics Workspace by going to the resource group as shown below.

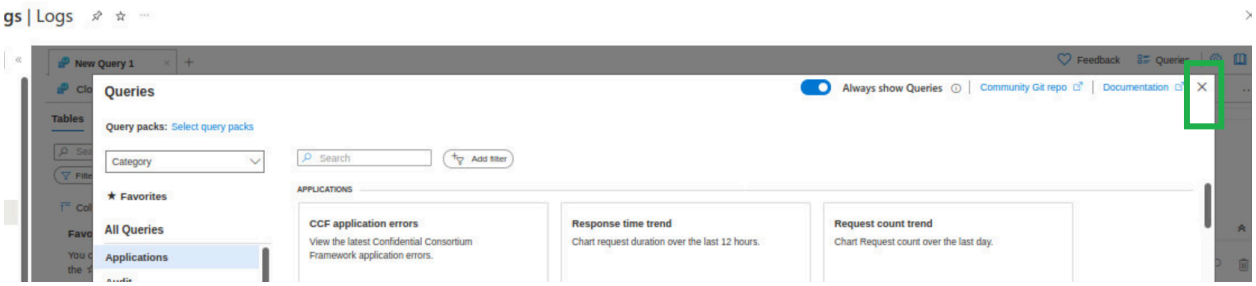


- Close "Welcome to Log Analytics" pop-up window

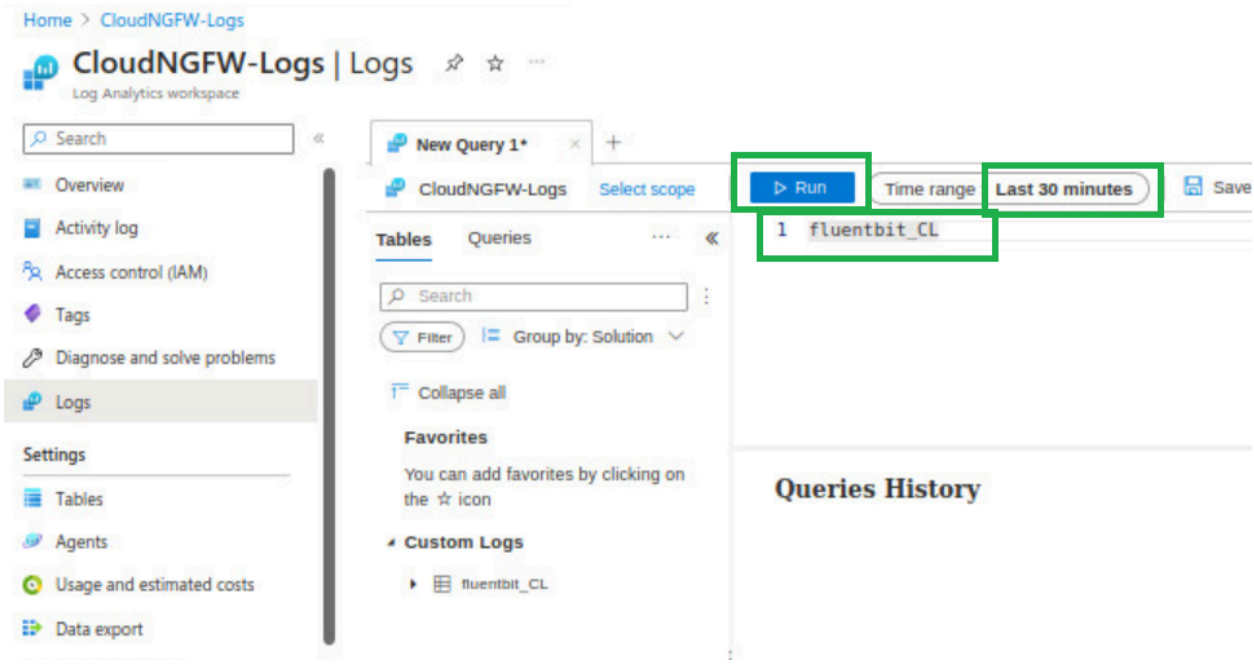




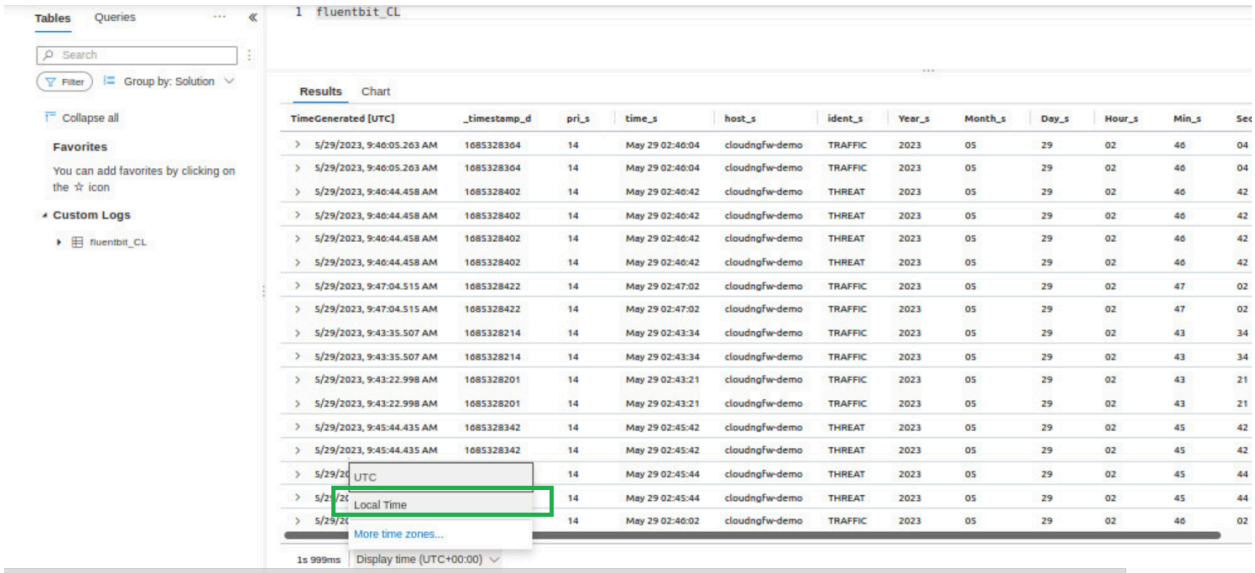
- Close the Queries page as shown below



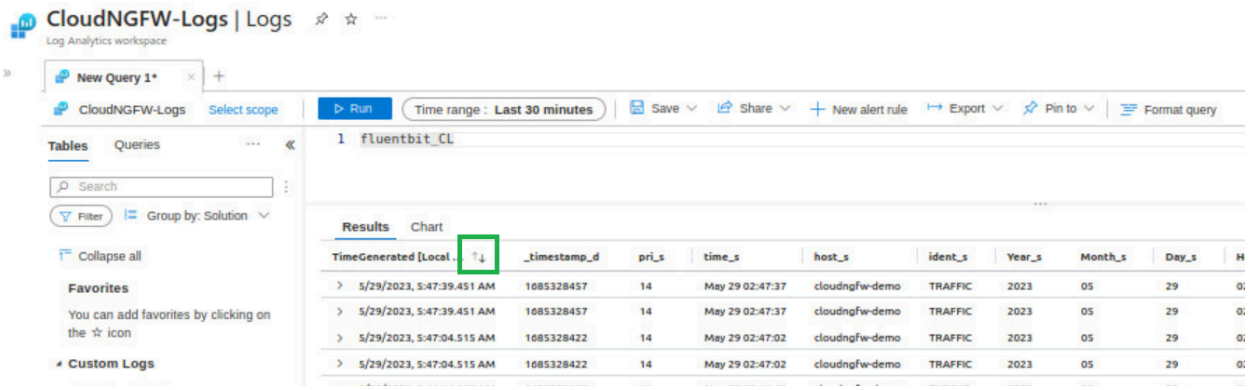
- After going to Log Analytics workspace(CougNGFW-Logs), navigate to **Logs** on the left menu
- In order to view Cloud NGFW logs we will be using custom query "**fluentbit_CL**"
- Select the time range(Ex: Last 30 Minutes) and click on **Run** to run the query inorder to view the logs



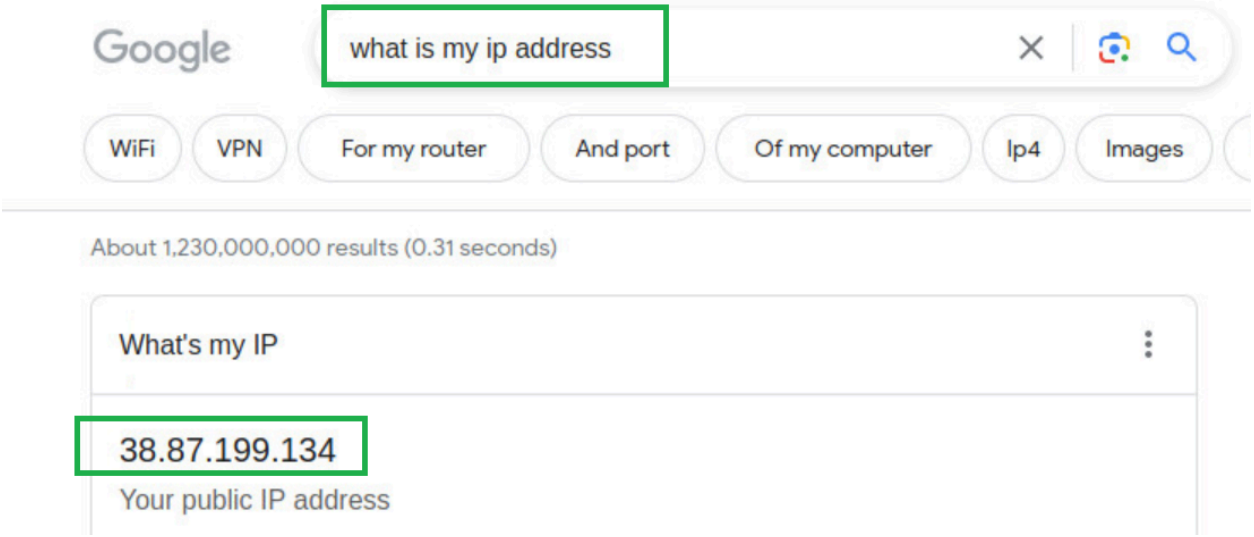
- After running the query, you will be seeing the logs as shown below. Select **Local Time** from the **Display time** at the left bottom of the page to view the logs in your local time.



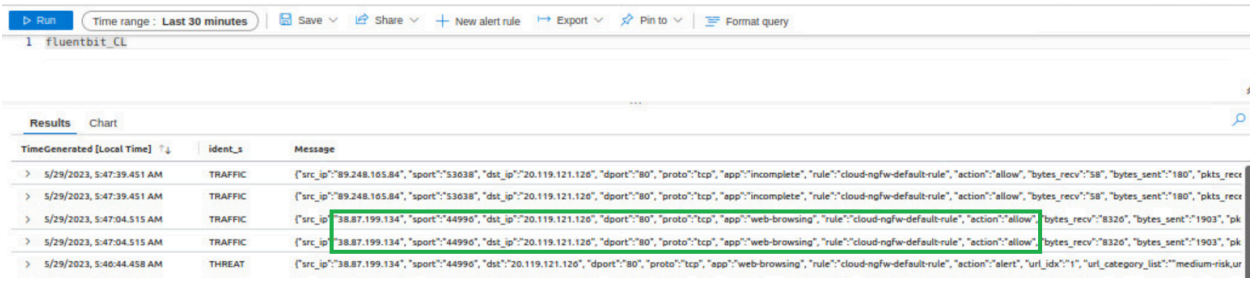
- Sort the logs to view latest on top



- Lets now verify the traffic coming from your device is going through Cloud NGFW
    - Get your public IP address as shown below



- Within the logs, go to the Message tab and check for the traffic flows and it should have the sessions initiated from your laptop or student desktop's public IP address and it should be hitting a rule on Cloud NGFW.



- 

This confirms that the internet inbound traffic is going through Cloud NGFW and processes as per the rules configured

Activity 2: Verify dynamic content on Web Server

In this task,

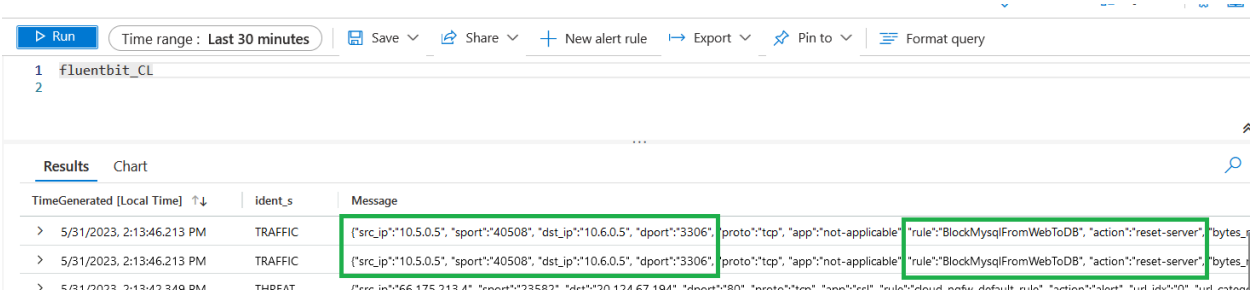
- You will generate a WordPress content request from your web browser that will trigger a database query to the MySQL server.
- Like many web-based applications, WordPress uses a backend database to create, store, and retrieve dynamic content.
- You will use the WordPress application to show exactly this type of behavior and demonstrate how the VM-Series firewall will secure this traffic.

Task 1 - Access Wordpress through Cloud NGFW

- Go to the Outputs of ARM Template deployment and copy "**web-server-url-wordpress**" as shown below.

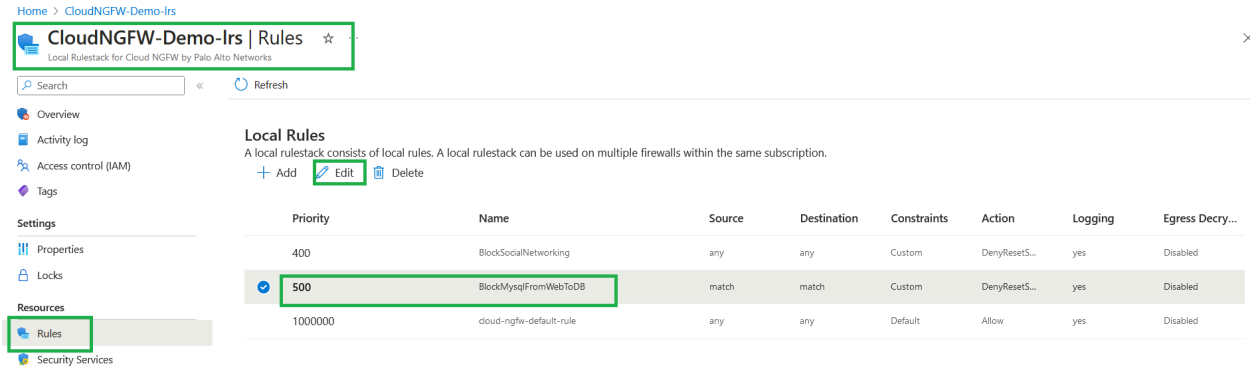
- Use the copied url and access the wordpress from your browser or from the browser within the student desktop. You should see the web page as shown below.

This is because of the deny rule that we have configured to drop Mysql traffic.
Verify the same by going to the log analytics

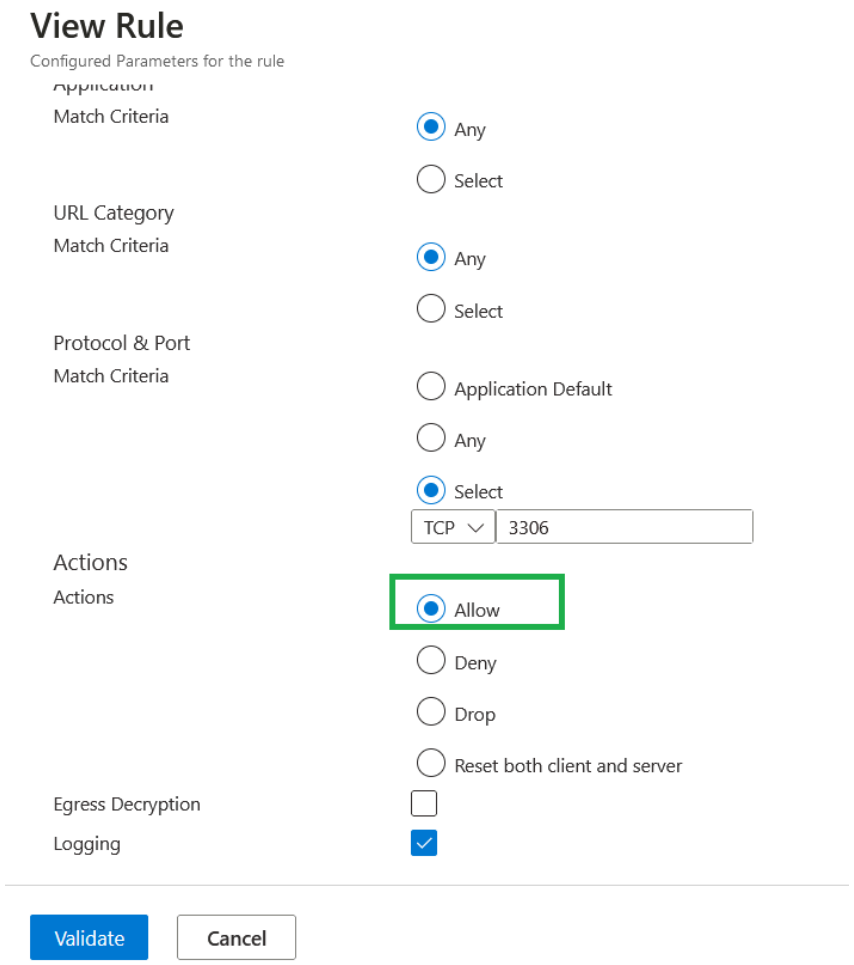


Task 2 - Update Localrustack to Allow Mysql traffic from Web to DB Servers

- Open Local Rulestack **"CloudNGFW-Demo-lrs"** and go to Rules and Edit "**BlockMysqlFromWebToDB**" rule as shown below.

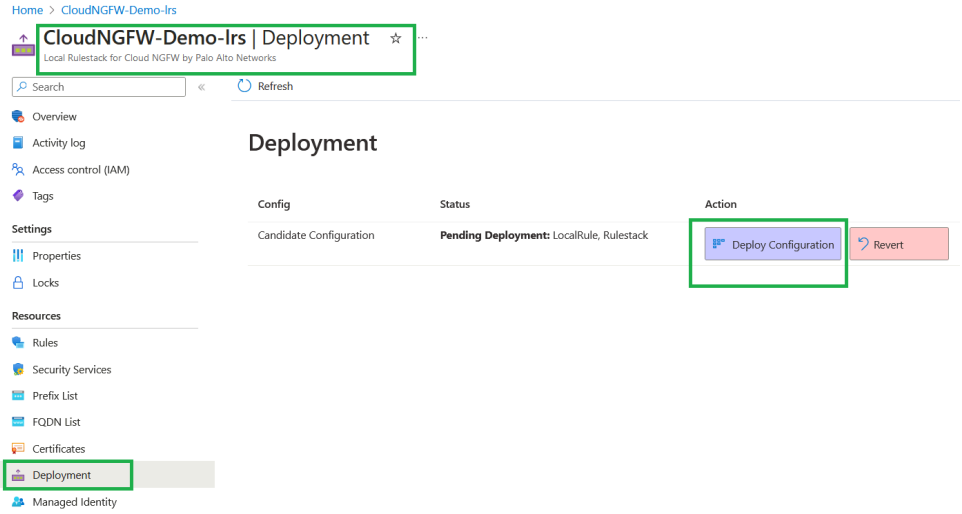


- Change the action as **Allow** and click on **Validate** and **Save**

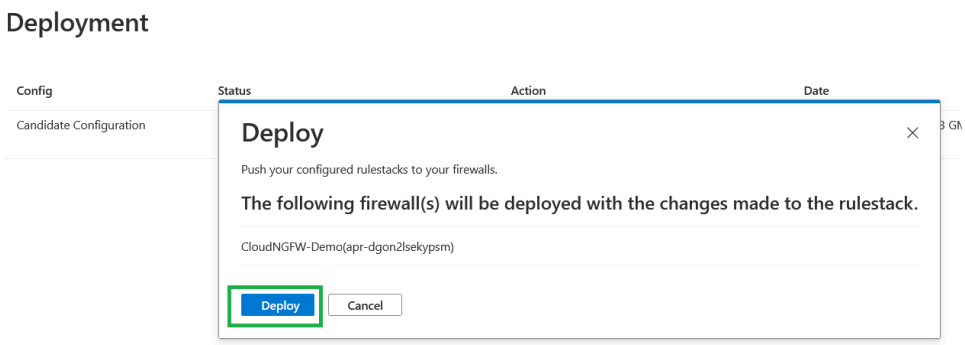


Deploy configuration

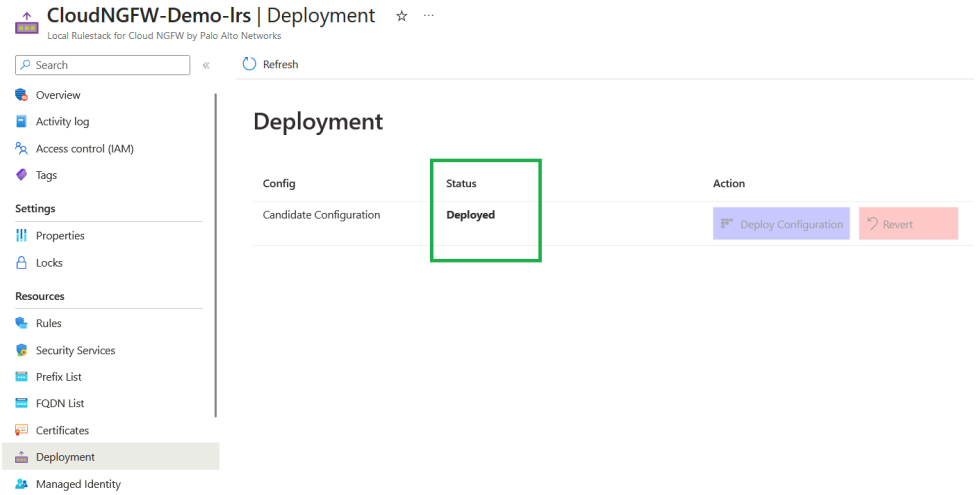
Within Local Rulestack page, goto Deployment on the left menu and click on “Deploy configuration” inorder to deploy the newly added rules onto Cloud NGFW service



You will be presented with the below mentioned screen where you need to click on "**Deploy**" to deploy the configuration.

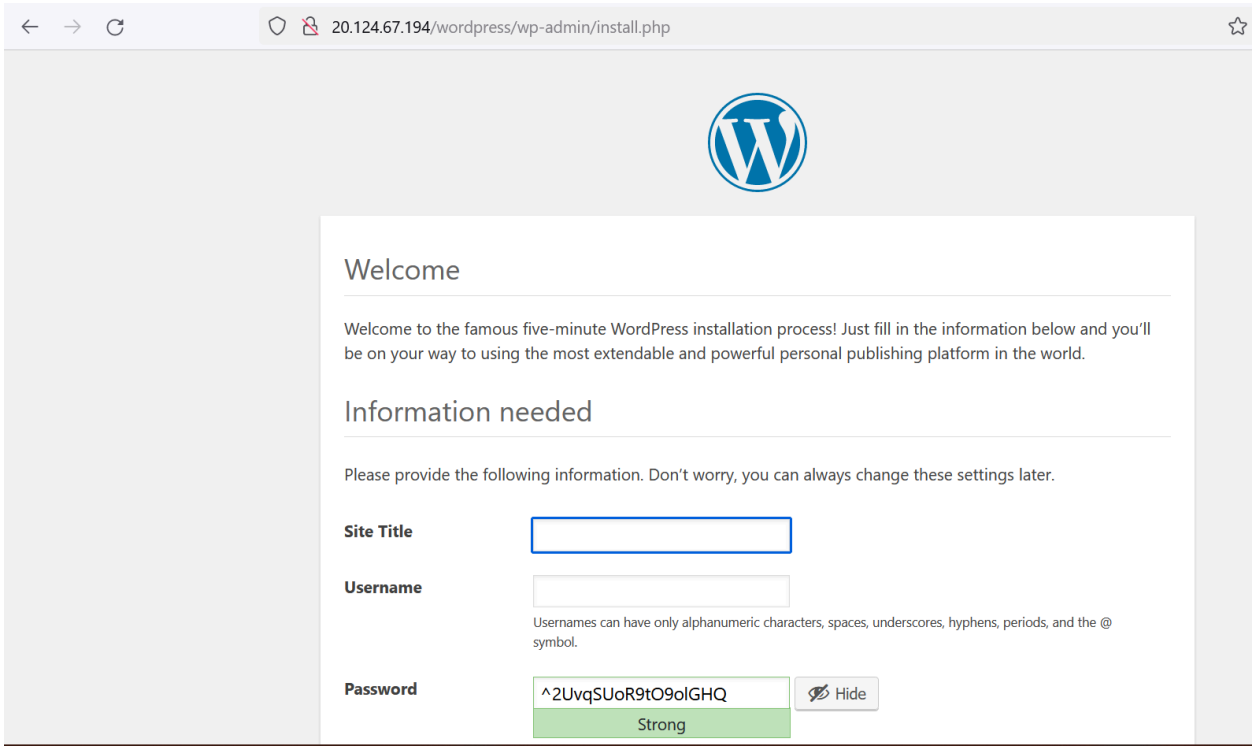


On Successful deployment, you should see the status as "**Deployed**" as shown below

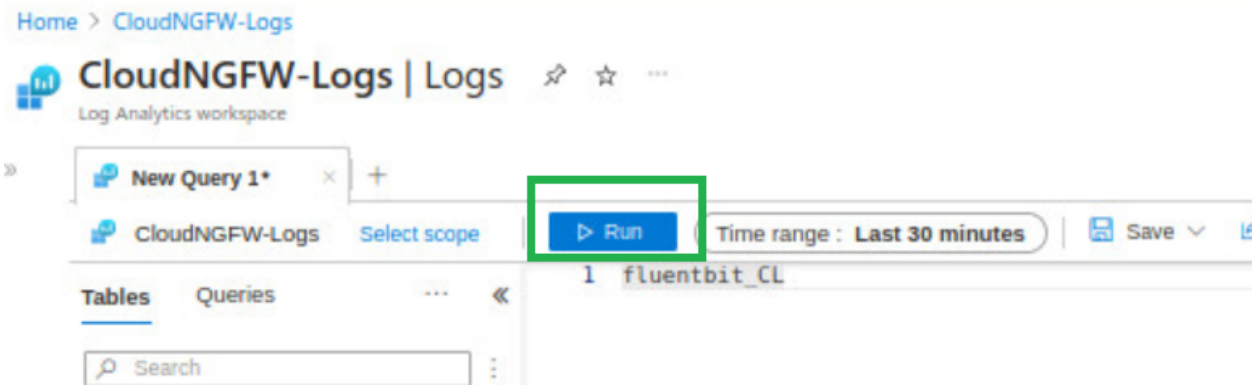


Task 3 - Re-verify Dynamic Content on Web Server

- Refresh the Wordpress URL and you should be seeing the below mentioned screen.

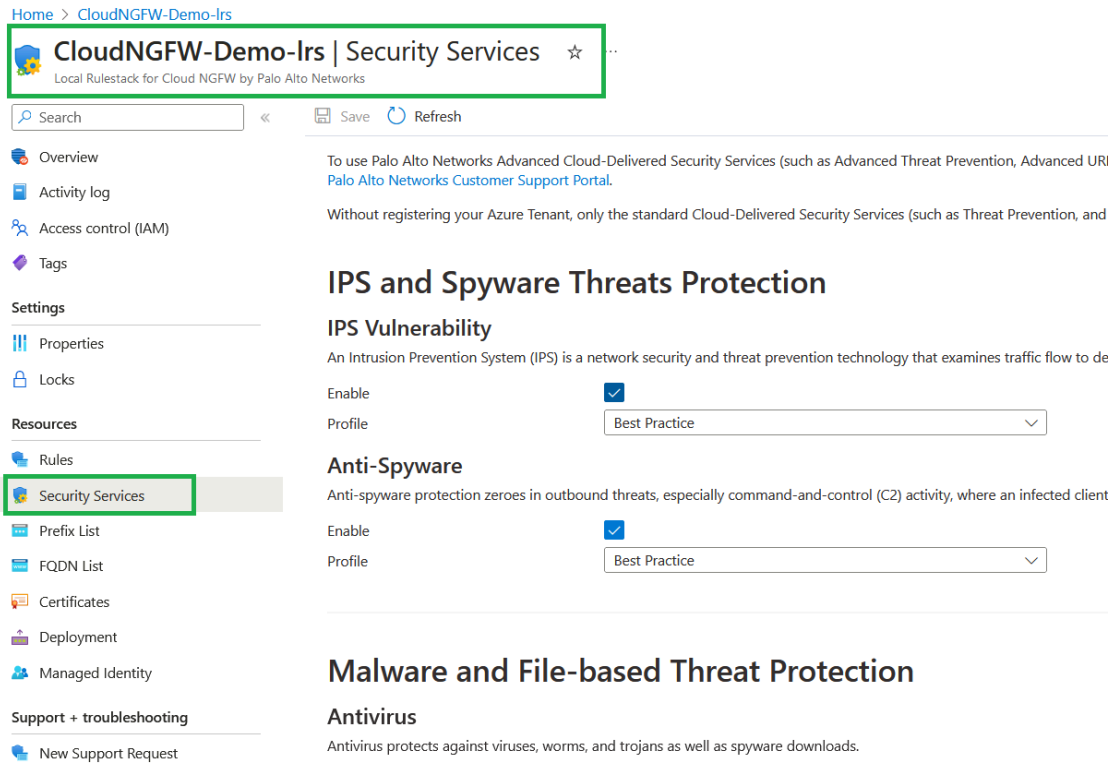


- Verify Mysql traffic was allowed between Webserver and DB Server



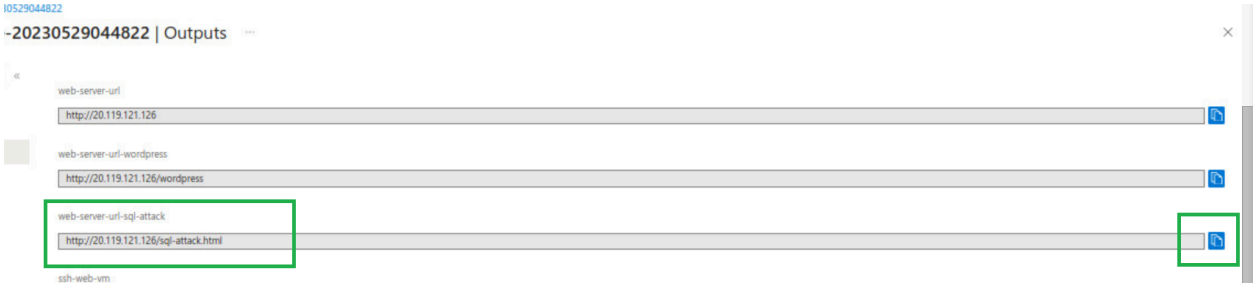
Activity 3: Protect your application from Threats using default security profiles

- Cloud NGFW by default comes with Best practice security services enabled. Your infrastructure on Azure will be protected using these services without the addition of any additional security configurations.
- Same thing can be verified by going to local rulestack as shown below

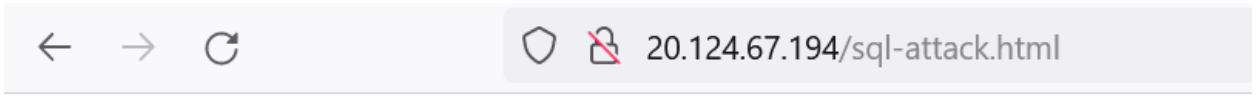


Task 1 - Access Sql attack URL

- Go to the Outputs of ARM Template deployment and copy "**web-server-url-sql-attack**" as shown below.

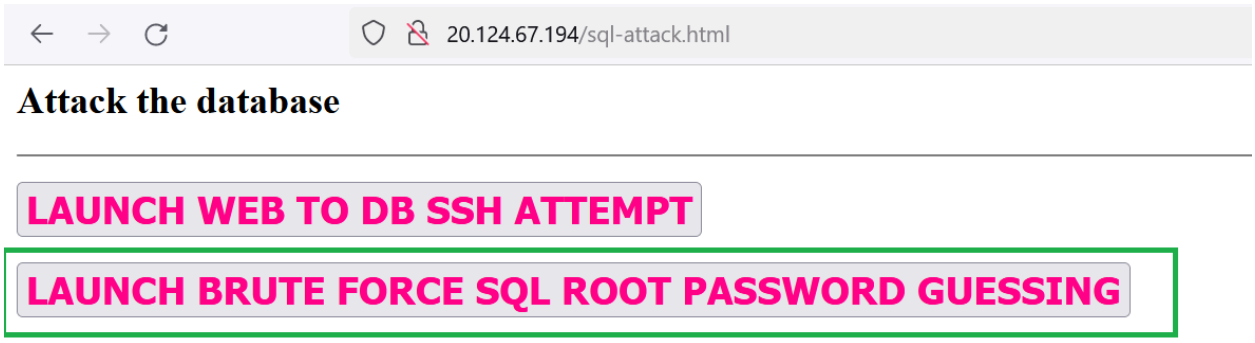


- Use the copied url and access the sql-attack URL from your browser or from the browser within the student desktop. You should see the web page as shown below.

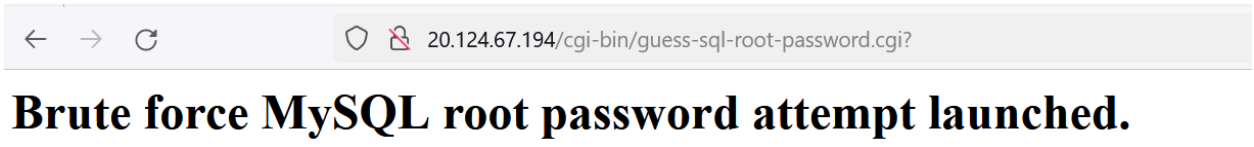


Task 2 - Launch Brute Force attack on DB Server

- Click on "LAUNCH BRUTE FORCE SQL ROOT PASSWORD GUESSING" to initiate brute force attack from web server to DB server

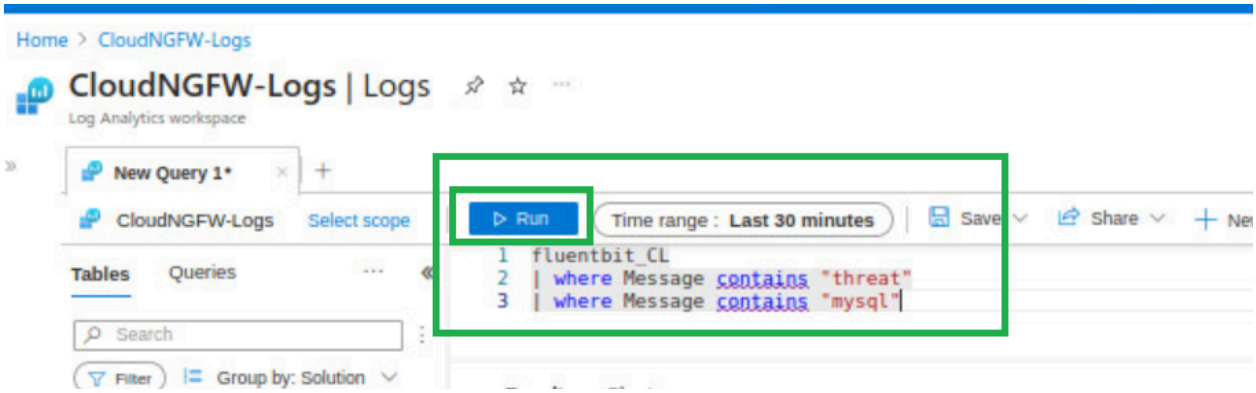


- You will be presented with below mentioned screen

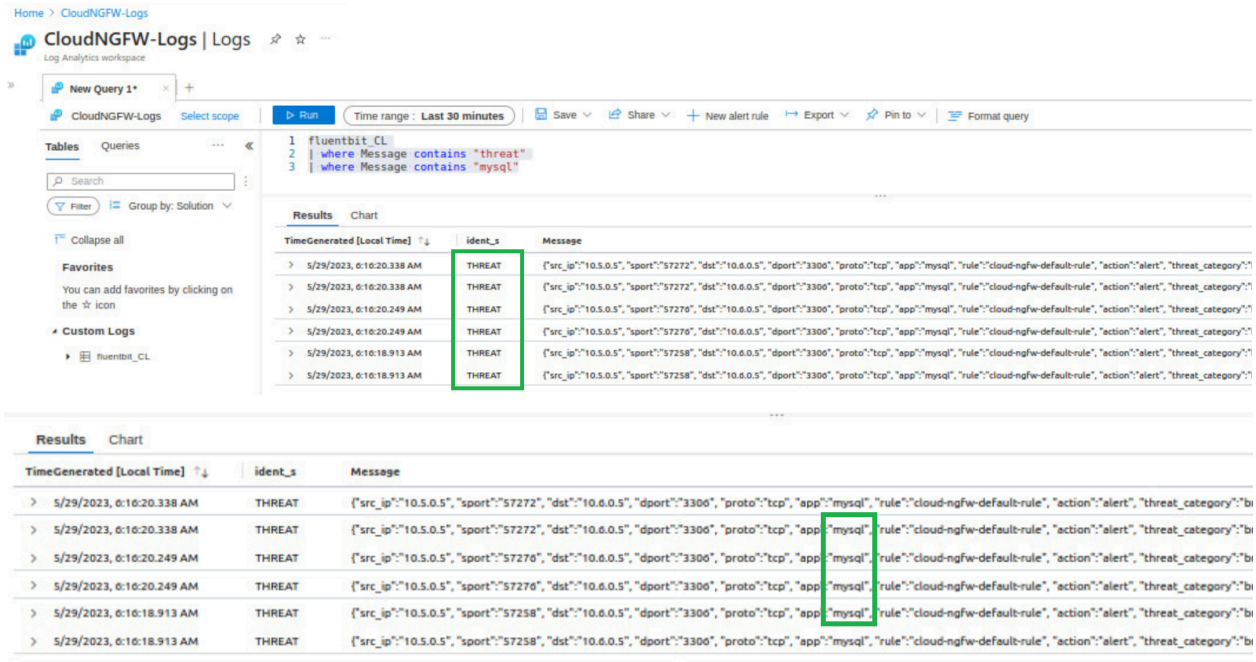


Task 3 - Verify THREAT logs on Log Analytics workspace

- To verify the threat logs, go to log analytics workspace and run the below mentioned query. This query will filter threat logs that include mysql traffic.
  fluentbit_CL
  | where Message contains “threat”
  | where Message contains “mysql”

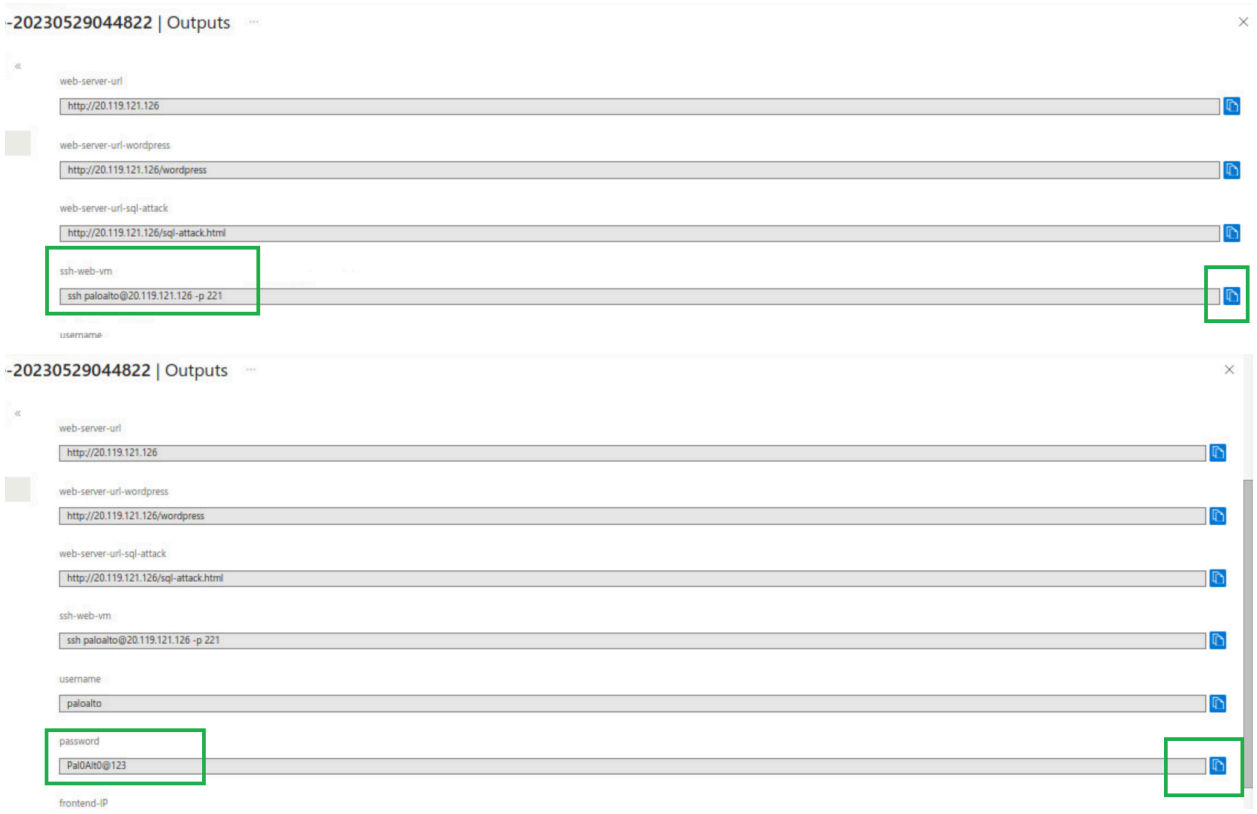


- From the log query result, we can see that Cloud NGFW is able to identify the brute force attack as Threat

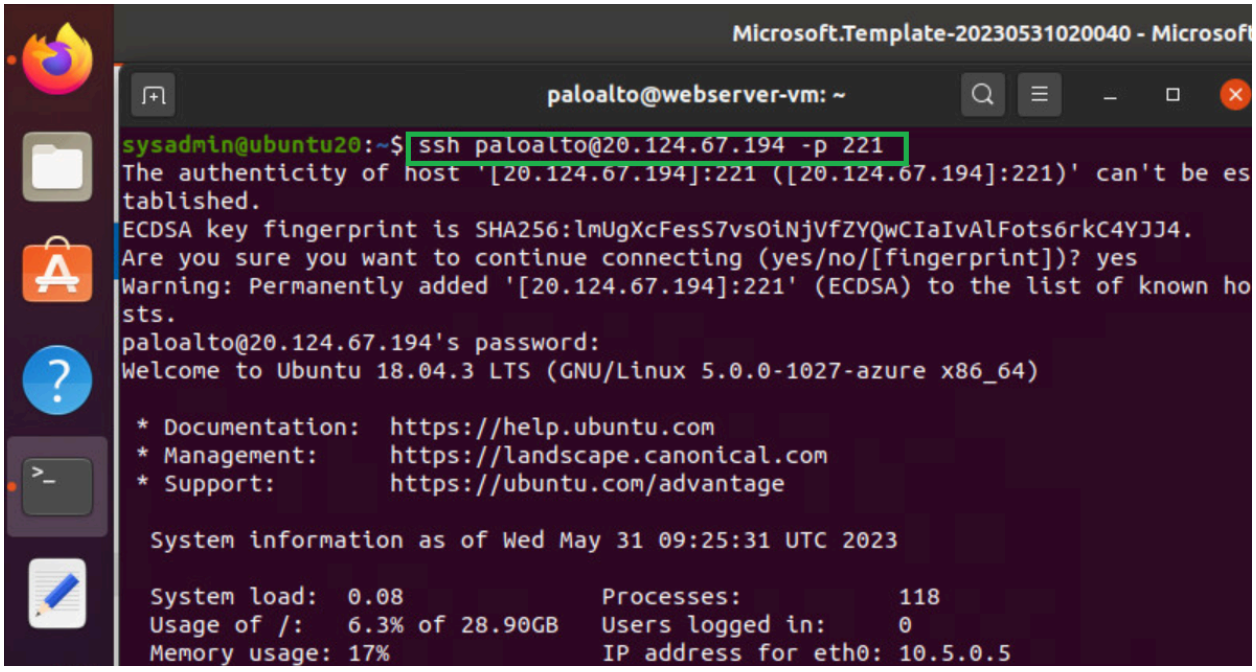


Activity 4: Validate secure outbound internet access through Cloud NGFW

- Go to the Outputs of ARM Template deployment and copy "**ssh-web-vm**" as shown below.

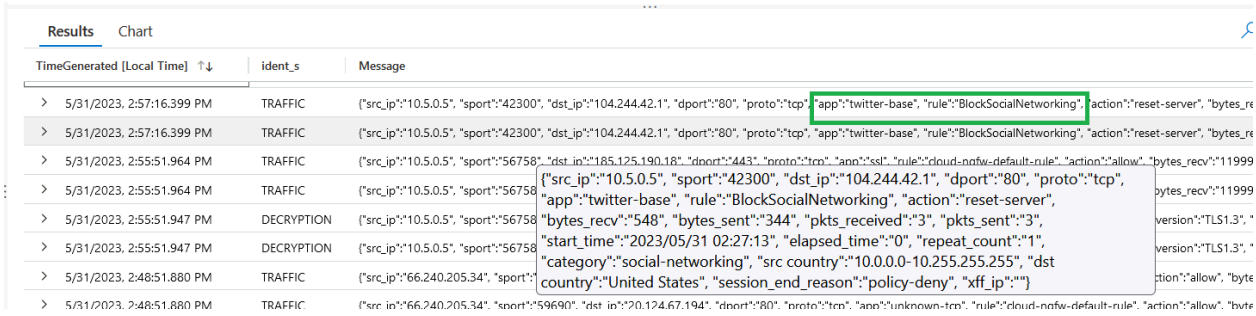


- Use the SSH command copied along with the password as shown in above screenshot and login to the Web server terminal



- After log into the web server try to access twitter.com which is part of the social networking category. You will not be able to access the website. Connection will get stuck and eventually time out.

- Verify logs by going to log analytics to confirm that Twitter website was blocked due to the rule we have added in above steps



END of LAB