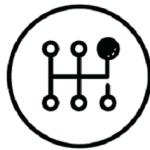


Cloud NGFW for Azure UTD Lab Guide



ULTIMATE
TEST DRIVE

Table of Contents

Table of Contents	1
Purpose of This Workshop Guide	2
Lab Activities Overview	2
Part-1 : Build test setup that will be used for this workshop using ARM template	3
Lab Topology	3
Activity 0: Log In to the UTD Workshop	3
Task 1 - Login to Your Ultimate Test Drive Class Environment	3
Task 2 : Log in to the Azure portal using the account provided.	5
Activity 1: Deploy Lab Environment with ARM Template	9
Task 1 - Launch ARM Template to deploy lab resources	9
Part-2 : Create and Configure Cloud NGFW for Azure using Azure portal to secure user traffic	14
Activity 1: Create Cloud NGFW Service	14
Activity 2: Review ARM template and Cloud NGFW deployment status	23
Task 1 - Review ARM Template deployment status	23
Task 2 - Review Cloud NGFW deployment status	25
Activity 3: Create Cloud NGFW Service	27
Task 1 - Configure Logging	27
Task 2 - Configure Destination NAT	29
Task 3 - Review default rule configured	34
Task 4 - Configure Firewall Policies using Local Rulestack	34
Add rule to block Mysql from web to db servers	34
Add rule to block Social Networking	36
Deploy configuration	38
Part-3 : Secure user traffic using Cloud NGFW for Azure	39
Activity 1: Verify secure inbound access to Web Server	39

Task 1 - Access Web Server through Cloud NGFW	39
Task 2 - Verify Cloud NGFW logs using Log Analytics workspace	40
Activity 2: Verify dynamic content on Web Server	44
Task 1 - Access Wordpress through Cloud NGFW	44
Task 2 - Update Localrustack to Allow Mysql traffic from Web to DB Servers	45
Deploy configuration	46
Task 3 - Re-verify Dynamic Content on Web Server	48
Activity 3: Protect your application from Threats using default security profiles	49
Task 1 - Access Sql attack URL	50
Task 2 - Launch Brute Force attack on DB Server	50
Task 3 - Verify THREAT logs on Log Analytics workspace	51
Activity 4: Validate secure outbound internet access through Cloud NGFW	52

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

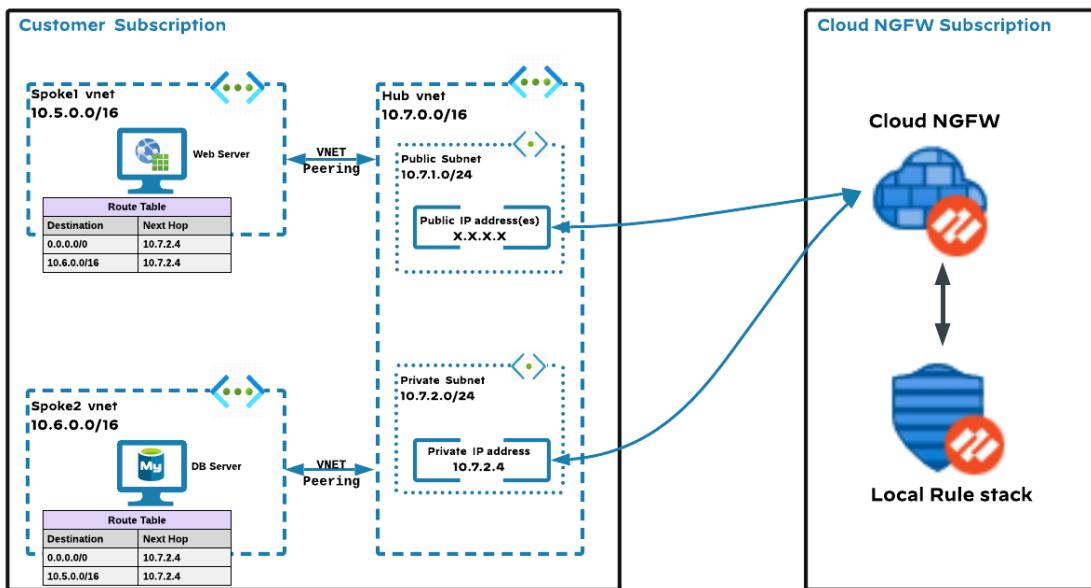
Once These Activities Have Been Completed

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

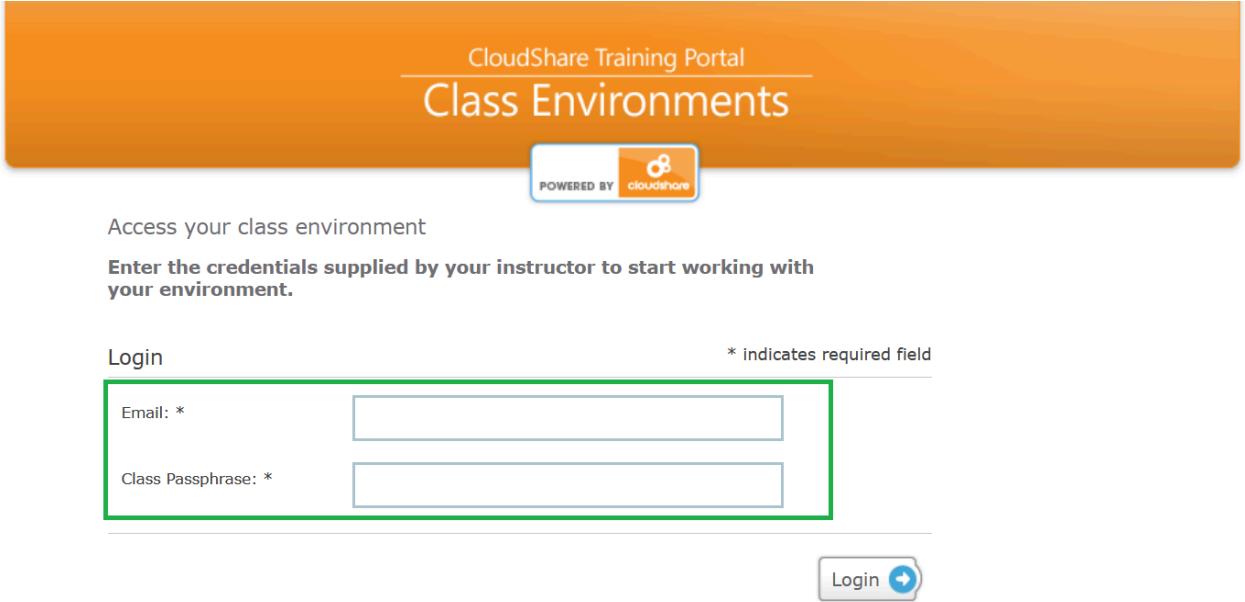
In this activity, you will:

- 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.

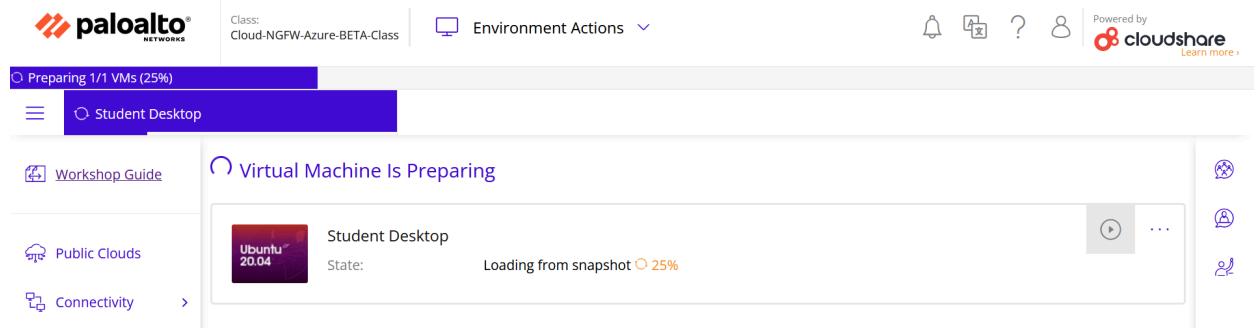
Enter your email address and the class passphrase.



The screenshot shows the CloudShare Training Portal Class Environments login page. At the top, it says "CloudShare Training Portal" and "Class Environments". Below that is a "POWERED BY cloudshare" logo. The main area has a green header with the text "Access your class environment" and "Enter the credentials supplied by your instructor to start working with your environment." Below this is a "Login" form with fields for "Email: *" and "Class Passphrase: *". A note at the top right says "* indicates required field". At the bottom right is a "Login" button with a blue arrow icon.

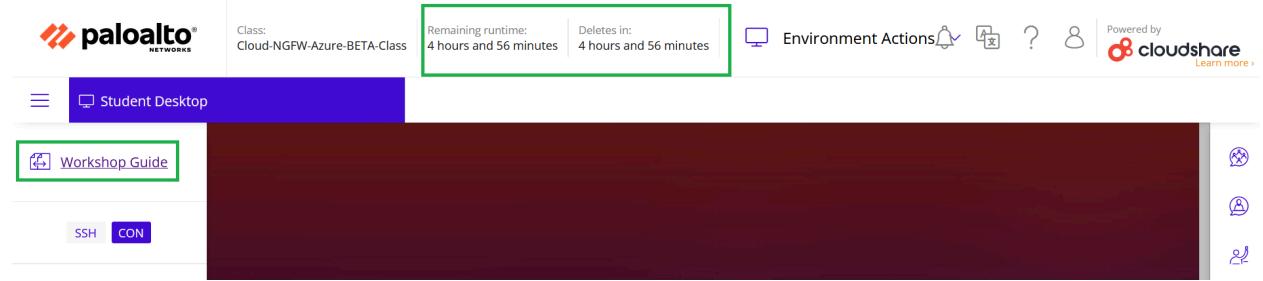
- Complete the registration process by providing your name and click the **Register and Login** option that you will get at the bottom.
- Make a note of your email and password to login to the UTD lab environment. You might need email and password to re-login in the lab environment in case you logged 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



The screenshot shows the CloudShare Training Portal dashboard. At the top, there's a navigation bar with the Palo Alto Networks logo, the class name "Cloud-NGFW-Azure-BETA-Class", and "Environment Actions". To the right are icons for notifications, user profile, and help, followed by the "Powered by cloudshare" logo. Below the navigation is a progress bar indicating "Preparing 1/1 VMs (25%)". Underneath, there are tabs for "Student Desktop" (which is selected) and "Workshop Guide". A message "Virtual Machine Is Preparing" is displayed. On the left, there are sections for "Public Clouds" (Ubuntu 20.04) and "Connectivity". On the right, there are additional icons for monitoring and connectivity.

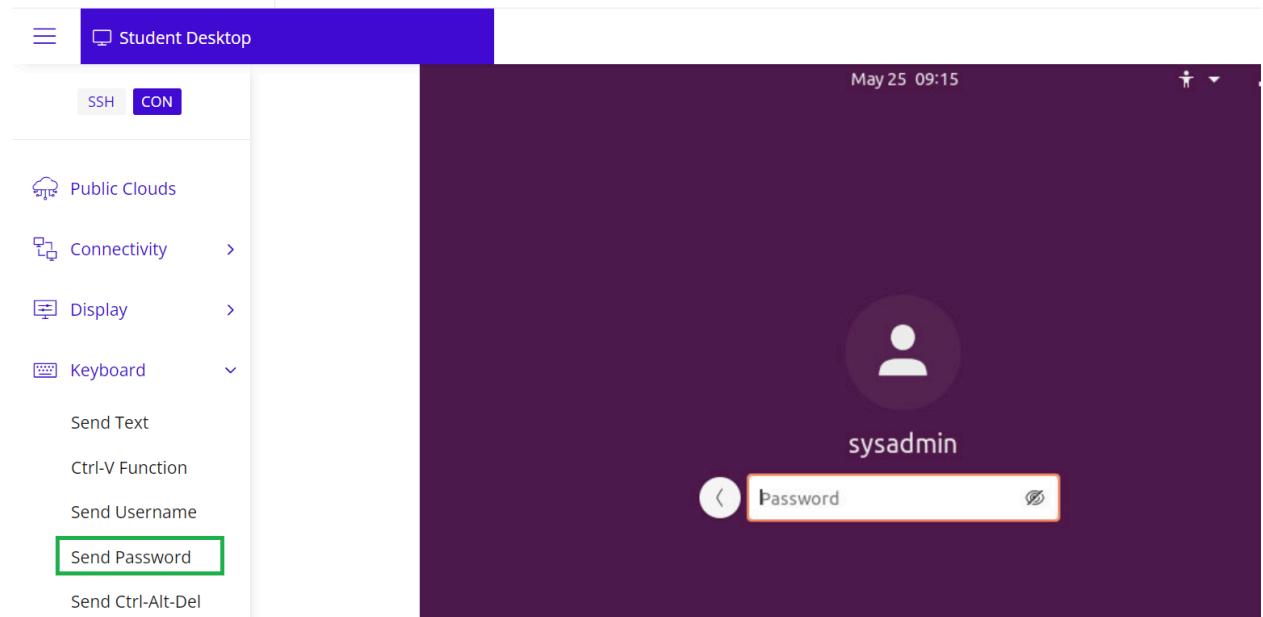
- On Successful creation of the lab, you will see the lab runtime as shown in the below screenshot. Click on the Workshop Guide tab to open the lab guide in a new tab and follow the instructions as per the guide to complete the workshop.



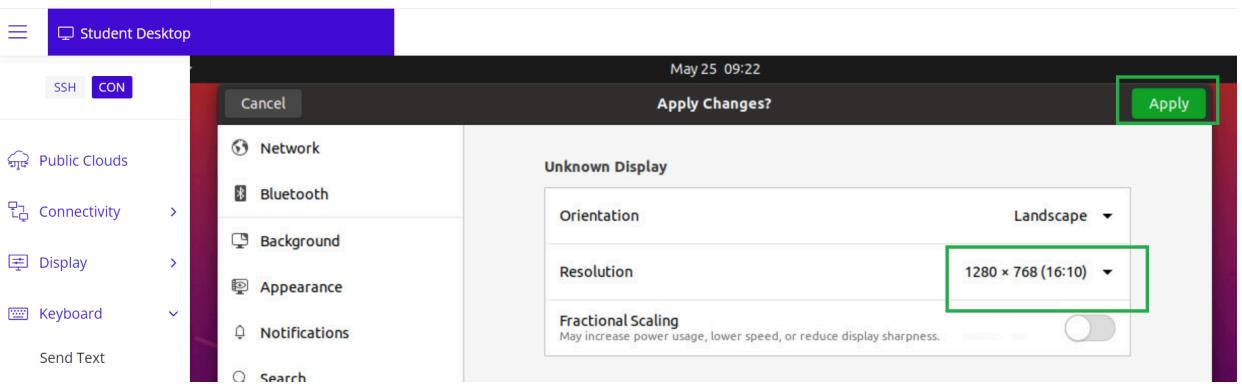
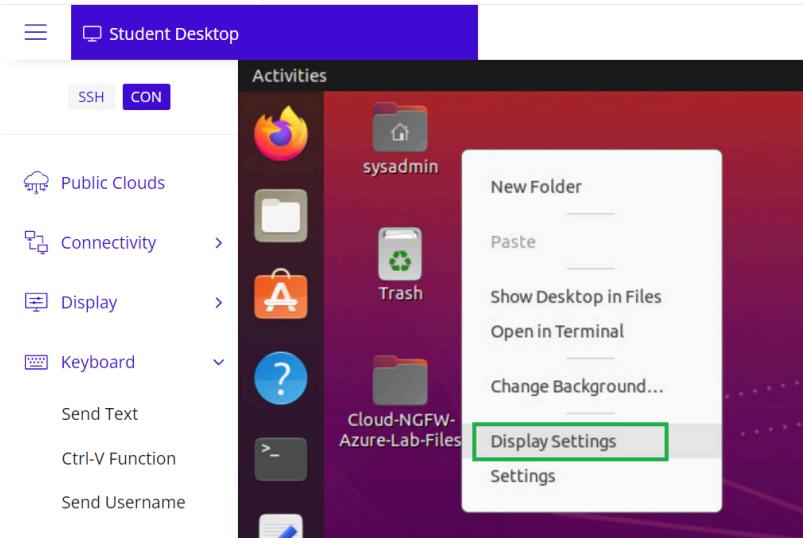
Task 2 : Log in to the Azure portal using the account provided.

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.

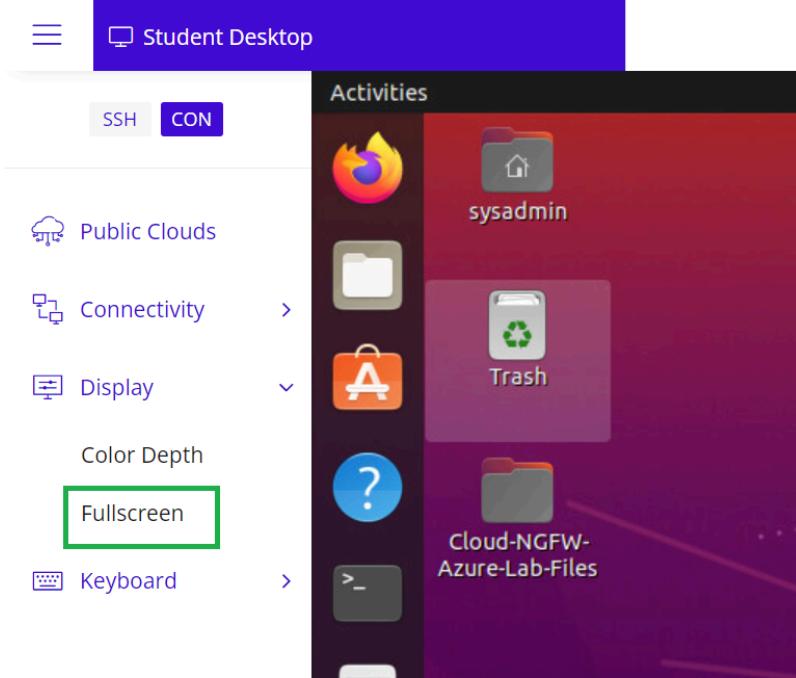
- Go to the CloudShare lab environment and click on the Student Desktop tab at the top of the page.
- In the left-hand side Action panel under the Keyboard, click on the Send Password to log in on Student Desktop.



- 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 down. The recommended resolution is 1280 x 768 (16:10).



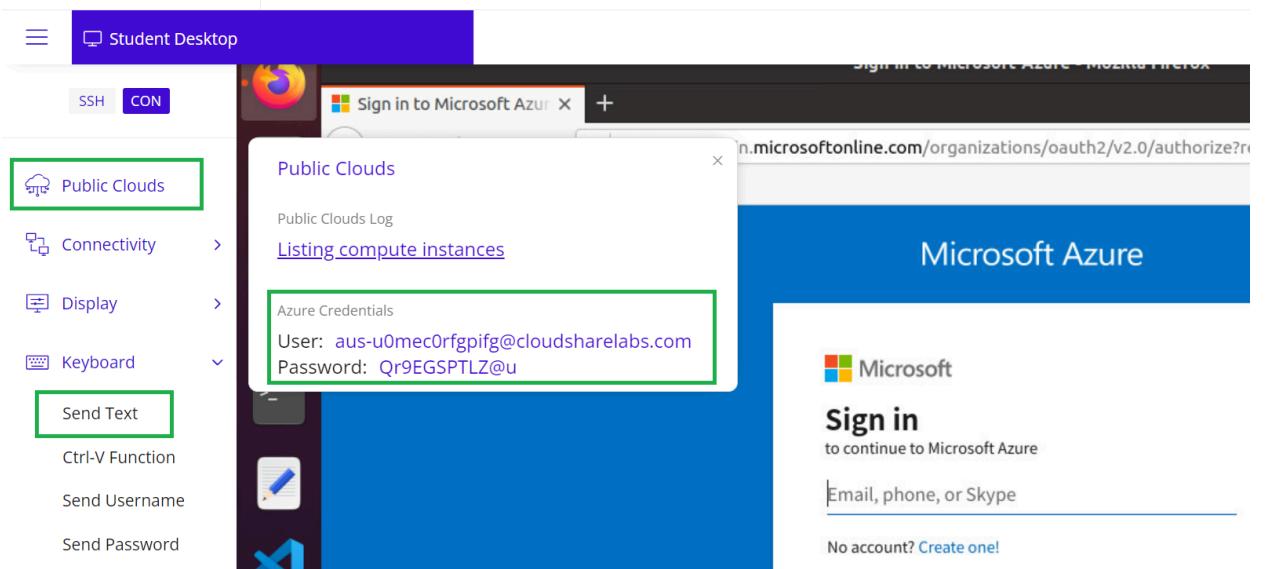
- From the left-hand Action panel. You can also click the Full screen icon to maximize the display.



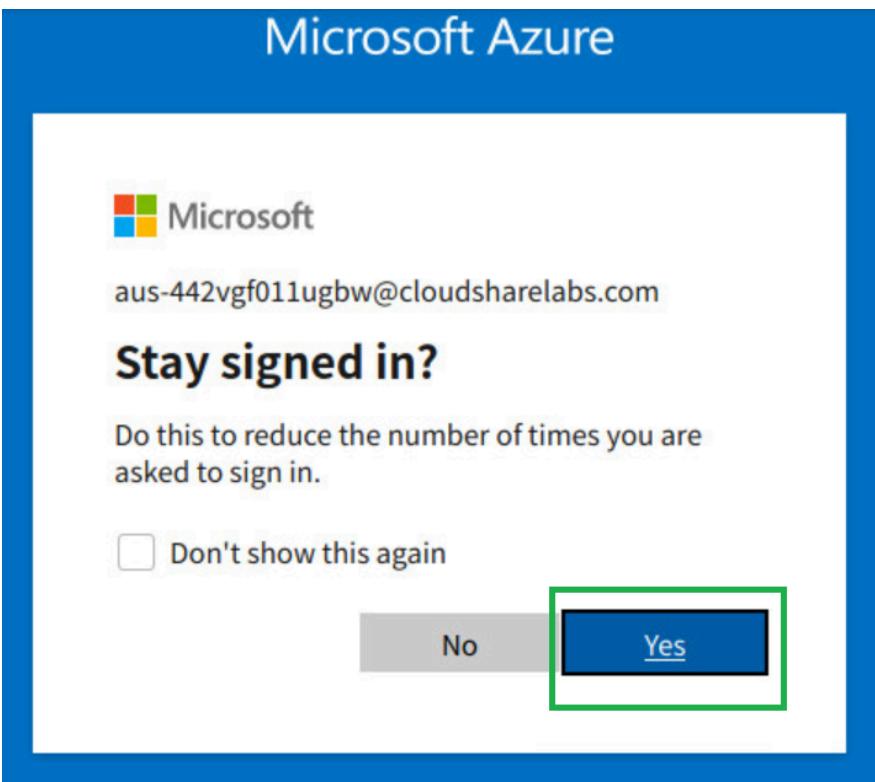
- To exit the full-screen mode, use the esc key on our keyboard or click the black arrow at the top of the window to open the dropdown menu; then click **Exit**.
- In the **Student Desktop** window click on the **Firefox Web browser** icon.
- Click on **Azure Portal** bookmark tab to open a Azure portal 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**.



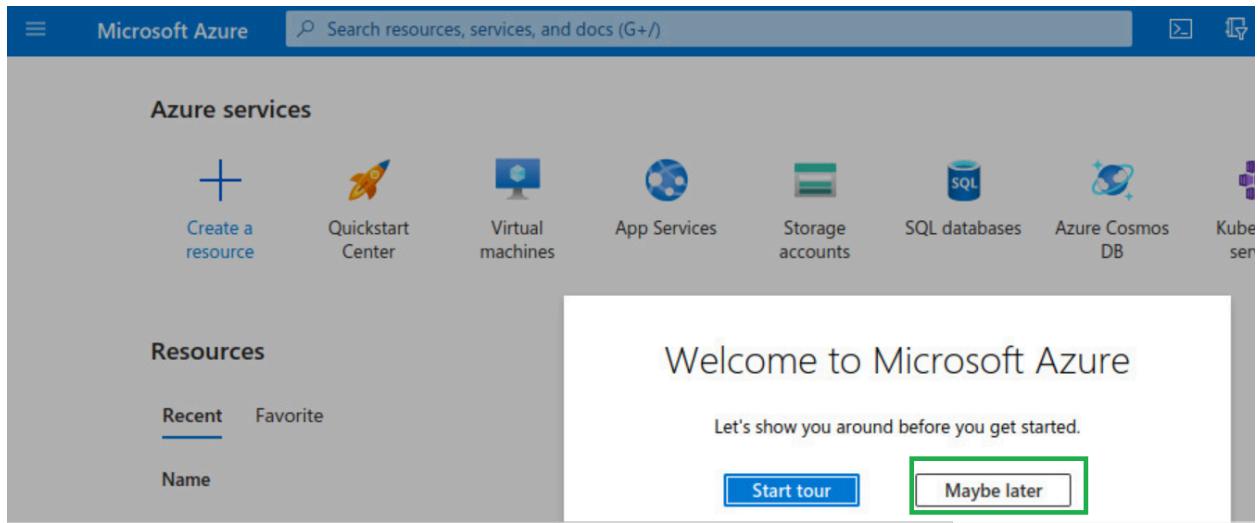
You can also access the Azure portal from your laptop browser and login using the credentials provided by the Cloudshare lab environment.



- 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

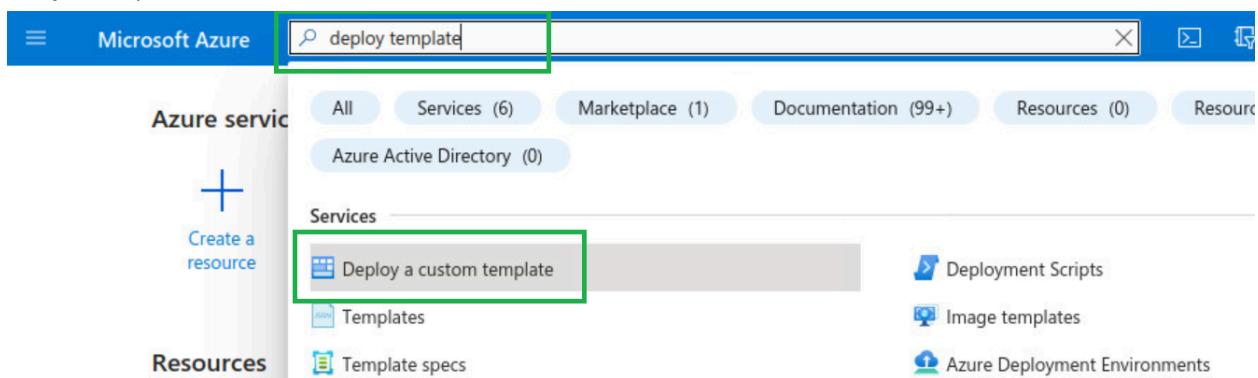
Activity 1: Deploy Lab Environment with ARM Template

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.

The screenshot shows the Microsoft Azure 'Custom deployment' page. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the title 'Custom deployment' and a sub-header 'Deploy from a custom template'. Underneath, there are tabs: 'Select a template' (which is underlined and bolded), 'Basics', and 'Review + create'. A descriptive text follows: 'Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started.' Below this, there's a button labeled 'Build your own template in the editor' with a pencil icon, which is highlighted with a green box. Further down, there's a section titled 'Common templates'.

- Use Load file option to load custom ARM template

The screenshot shows the Microsoft Azure 'Edit template' page. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the title 'Edit template' and a sub-header 'Edit your Azure Resource Manager template'. There are buttons for '+ Add resource', 'Quickstart template', 'Load file' (which is highlighted with a green box), and 'Download'. On the left, there are sections for 'Parameters (0)', 'Variables (0)', and 'Resources (0)'. On the right, there's a code editor window showing the beginning of an ARM template:

```

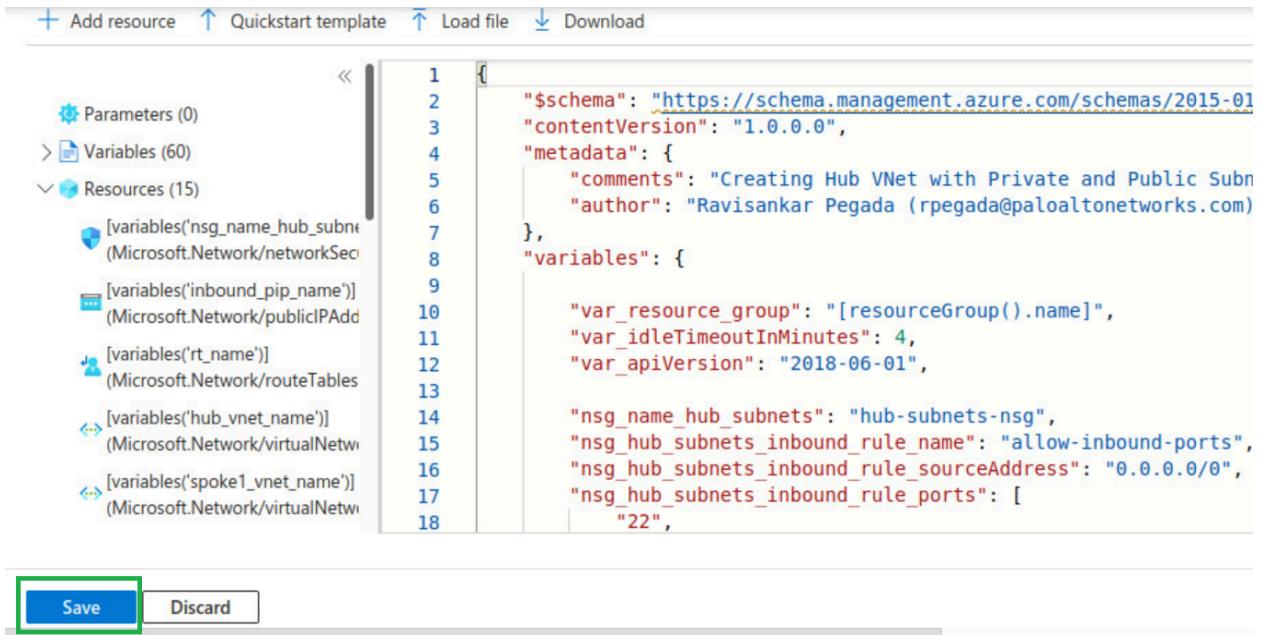
1  {
2    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
3    "contentVersion": "1.0.0.0",
4    "parameters": {},
5    "resources": []
6  }

```

- 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

The screenshot shows a 'File Upload' dialog box. At the top, there's a 'Cancel' button and a 'File Upload' title. Below that is a file selection interface with a 'Recent' section and a 'Cloud-NGFW-Azure-Lab-Files' folder. In the 'Name' field, the file 'CloudNGFW-Azure-VNet-2023-05-23.json' is selected, indicated by a green box around the file name.

- Click on “Save” to save the template



The screenshot shows the Azure Resource Manager template editor interface. On the left, there's a navigation pane with options: 'Parameters (0)', 'Variables (60)', and 'Resources (15)'. Under 'Resources', several items are listed with their types and names: '[variables('nsg_name_hub_subnets')]' (Microsoft.Network/networkSecurityGroups), '[variables('inbound_pip_name')]' (Microsoft.Network/publicIPAddresses), '[variables('rt_name')]' (Microsoft.Network/routeTables), '[variables('hub_vnet_name')]' (Microsoft.Network/virtualNetworks), and '[variables('spoke1_vnet_name')]' (Microsoft.Network/virtualNetworks). The main area displays the JSON template code with line numbers from 1 to 18. The 'Save' button at the bottom left is highlighted with a green box.

```

1  {
2    "$schema": "https://schema.management.azure.com/schemas/2015-01
3    "contentVersion": "1.0.0.0",
4    "metadata": {
5      "comments": "Creating Hub VNet with Private and Public Subn
6      "author": "Ravisankar Pegada (rpegada@paloaltonetworks.com)
7    },
8    "variables": {
9
10       "var_resource_group": "[resourceGroup().name]",
11       "var_idleTimeoutInMinutes": 4,
12       "var_apiVersion": "2018-06-01",
13
14       "nsg_name_hub_subnets": "hub-subnets-nsg",
15       "nsg_hub_subnets_inbound_rule_name": "allow-inbound-ports",
16       "nsg_hub_subnets_inbound_rule_sourceAddress": "0.0.0.0/0",
17       "nsg_hub_subnets_inbound_rule_ports": [
18         "22",

```

- 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

Select a template Basics Review + create

Template

Customized template 15 resources

Edit template Visualize

Project details

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

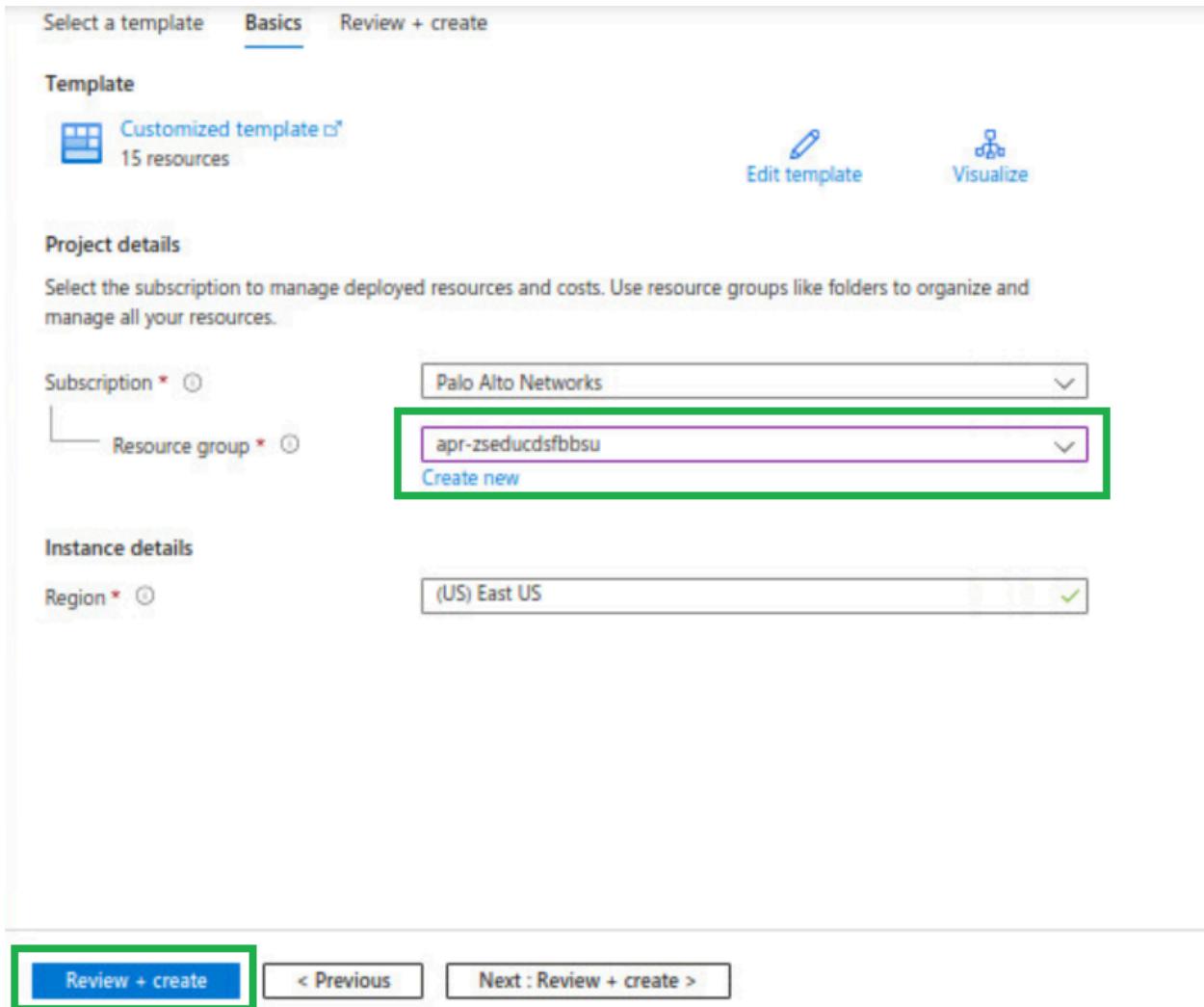
Subscription * (Palo Alto Networks)

Resource group * (apr-zseducdsfbbsu) [Create new](#)

Instance details

Region * (US) East US

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



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

Home >

Custom deployment

Deploy from a custom template

 Validation Passed

Select a template Basics Review + create

Summary



Customized template
15 resources

Terms

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

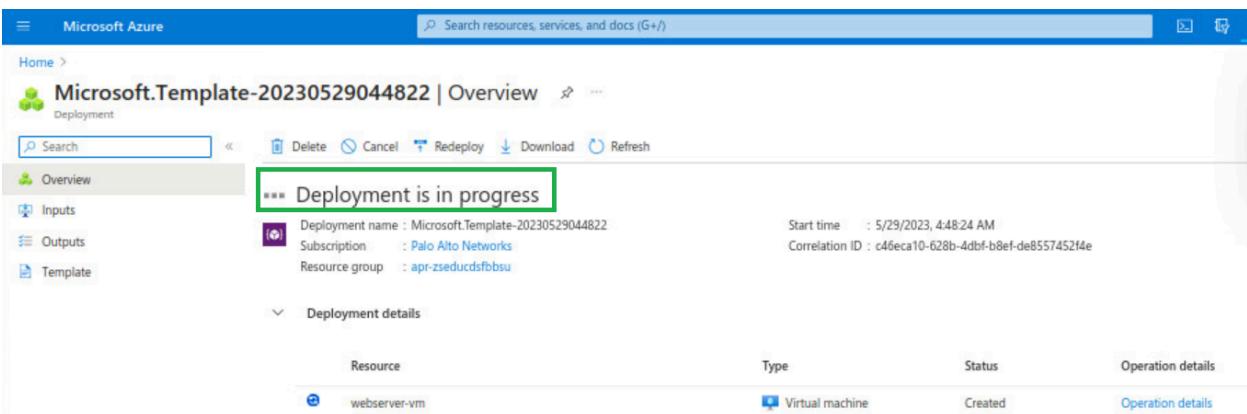
By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Create

< Previous

Next >

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



Microsoft Azure

Microsoft.Template-20230529044822 | Overview

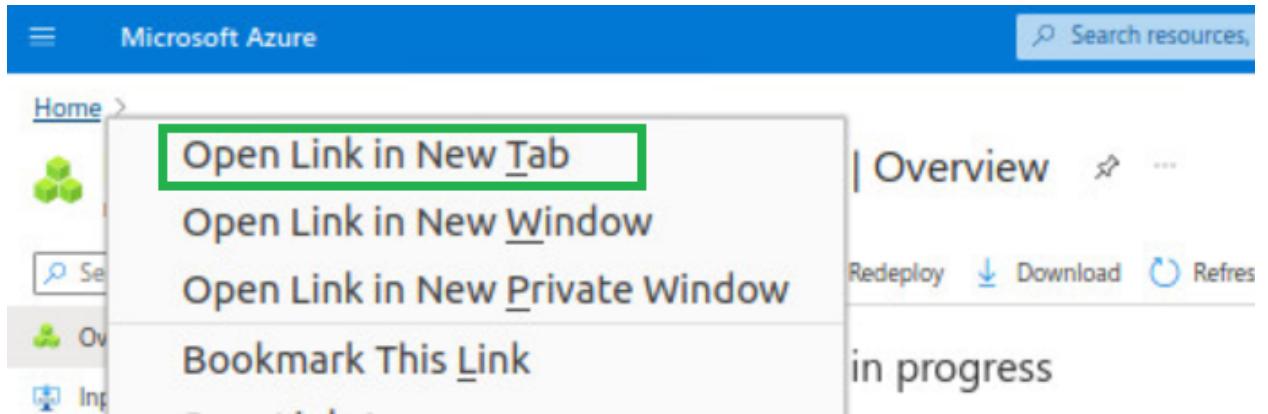
Deployment

Deployment is in progress

Resource	Type	Status	Operation details
webserver-vm	Virtual machine	Created	Operation details

You can wait for the deployment to complete or

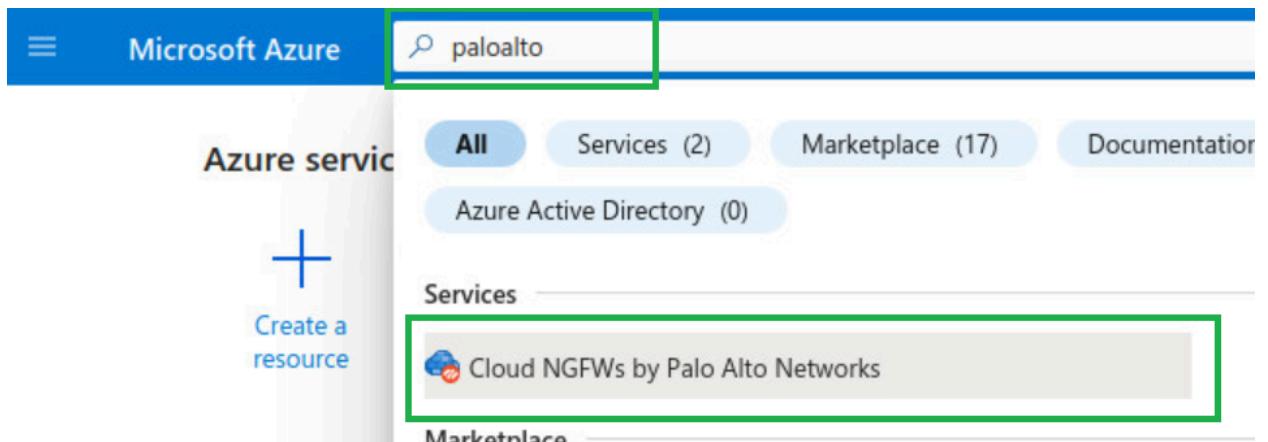
While the deployment is in progress, right click on "**Home**" and open Azure portal in another tab.



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

Microsoft Azure

Search resources, services, and docs (C)

Home >

Cloud NGFWs by Palo Alto Networks

Cloudshare (azurecloudshare.onmicrosoft.com) | PREVIEW

+ Create Manage view Refresh Export to CSV

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

Microsoft Azure

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

Home > Cloud NGFWs by Palo Alto Networks >

Create Cloud NGFW by Palo Alto Networks

Basics Networking Security Policies DNS Proxy Tags Terms Review + create

Creating a Cloud NGFW resource (by Palo Alto Networks) in Azure enables you to quickly and easily secure network traffic in your Azure VNets and Azure VWANs from the most advanced cyber-threats. This Azure Native ISV service harnesses the power of AI and ML to stop the most advanced cyber-threats. As an Azure-native ISV managed service, it deploys in minutes and scales automatically with your network traffic, so you can focus on security, not managing infrastructure. [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.

- 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

Basics Networking Security Policies DNS Proxy Tags Terms Review + create

Creating a Cloud NGFW resource (by Palo Alto Networks) in Azure enables you to quickly and easily secure network traffic in your Azure VNets and Azure VWANs from the most advanced cyber-threats. This Azure Native ISV service harnesses the power of AI and ML to stop the most advanced cyber-threats. As an Azure-native ISV managed service, it deploys in minutes and scales automatically with your network traffic, so you can focus on security, not managing infrastructure. [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 * ○ Palo Alto Networks

Resource group * ○ apr-zseducdsfbbsu [Create new](#)

Firewall Details

Firewall Name * ○ CloudNGFW-Demo

Region * ○ East US

Marketplace Plan * ○ Cloud Next-Generation Firewall by Palo Alto Networks - An Azure Native ISV Service Pay-as-you-go

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

- 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

Basics Networking Security Policies DNS Proxy Tags Terms Review + create

ORK settings.

Network Type

Type *

Virtual Network
 Virtual Wan Hub

Configure virtual networks

Virtual Network *

hub-vnet

Private Subnet *

hub-private-subnet (10.7.2.0/24)

Public Subnet *

hub-public-subnet (10.7.1.0/24)

Public IP Address Configuration

Public IP Address(es) *

Create new
 Use existing

Public IP Address Name(s) *

frontendip

Source NAT Settings

Enable Source NAT

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

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.

The screenshot shows the configuration steps for creating a Cloud NGFW. The current step is "Security Policies".

Managed by *: Options are "Azure Portal Rulestack" (selected) and "Palo Alto Networks Panorama".

Choose a Local Rulestack *: Options are "Create new" (selected) and "Use existing".

Local Rulestack *: A text input field contains "CloudNGFW-Demo-lrs".

Firewall rules *: Options are "Allow all (Enables all security services using best-practices profile to inspect traffic)" (selected) and "Deny all".

A callout box provides information about using Palo Alto Networks Advanced Cloud-Delivered Security Services:

- To use Palo Alto Networks Advanced Cloud-Delivered Security Services (such as Advanced Threat Prevention, Advanced URL Filtering, Wildfire, and DNS Security), you must register your Azure Tenant at the Palo Alto Networks Customer Support Portal after the firewall creation.
- Without registering your Azure Tenant, only the standard Cloud-Delivered Security Services (such as Threat Prevention, and URL Filtering) will be offered, if enabled.

At the bottom, the navigation buttons are: "Review + create" (disabled), "< Previous", and "Next : DNS Proxy >" (highlighted with a green box).

- 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 >**”

DNS Proxy *

Disabled

Enabled

[Review + create](#)

[< Previous](#)

[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 >**"

Basics Networking Security Policies DNS Proxy Tags Terms Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ	Value ⓘ	Resource
<input type="text"/>	:	<input type="text"/> 5 selected ▾

[Review + create](#)

[< Previous](#)

[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

[Basics](#)[Networking](#)[Security Policies](#)[DNS Proxy](#)[Tags](#)[Terms](#)[Review + create](#)[Terms of use](#) | [Privacy Policy](#)

By clicking Create I agree to the legal terms and privacy statement associated with the Marketplace offering (licensed by Palo Alto Networks by the [End User Agreement](#)) and authorize Microsoft to bill my current payment method for the fees associated with the offerings with the same billing frequency as my Azure subscription and agree that Microsoft may share my contact usage and transactional information with the provider of the offerings for support billing and other transactional activities. Microsoft does not provide rights for third-party offerings. For additional details refer to [Azure Marketplace Terms](#)

I Agree *

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

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

Basics Networking Security Policies DNS Proxy Tags Terms **Review + create**

Basics

Subscription	Palo Alto Networks
Resource group	apr-zseducdsfbbsu
Firewall Name	CloudNGFW-Demo
Region	East US
Marketplace Plan	Cloud Next-Generation Firewall by Palo Alto Networks - An Azure Native ISV ...

Networking

Type	Virtual Network
Virtual network	hub-vnet
Private Subnet	hub-private-subnet
Address prefix (Private Subnet)	10.7.2.0/24
Public Subnet	hub-public-subnet
Address prefix (Public Subnet)	10.7.1.0/24
Public IP Address(es)	Use existing
Public IP Address Name(s)	frontendip

Security Policies

Managed by	Azure Portal Rulestack
Choose a Local Rulestack	Create new
Local Rulestack	CloudNGFW-Demo-lrs
Firewall rules	Allow all (Enables all security services using best-practices profile to inspect t...)

Create < Previous Next

- You will be presented with below screen

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named 'CreateFirewallForm-20230529045125'. The status bar at the top indicates 'Deployment is in progress'. The deployment details show the following information:

Deployment name	Subscription	Resource group
CreateFirewallForm-20230529045125	Palo Alto Networks	apr-zseducdsfbusu

Deployment details also include start time (5/29/2023, 5:03:55 AM) and correlation ID (7a7aeff4-66ed-4ff6-b549-c7737878d530). A table below lists the resources deployed:

Resource	Type	Status
CloudNGFW-Demo-Irs	Local Rulestack for Cloud NGFW	Created

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.

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named "Microsoft.Template-20230529044822". The "Overview" tab is selected. A prominent message box states "Your deployment is complete" with a green checkmark icon. Below it, deployment details are listed: Deployment name: Microsoft.Template-20230529044822, Subscription: Palo Alto Networks, Resource group: apr-zseducdsfbsu. Navigation links include "Deployment details" and "Next steps". A blue button at the bottom right says "Go to resource group".

- 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 screenshot shows the Microsoft Azure Deployment Overview page for the same deployment. The "Outputs" tab in the left menu is highlighted with a green box. A context menu is open over the "Outputs" tab, with the top item "Open Link in New Tab" highlighted with a green box. Other options in the menu are "Open Link in New Window" and "Open Link in New Private Window". The deployment details are visible in the background.

- 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

Microsoft.Template-20230529044822 | Outputs

Deployment

<input type="text"/> Search	<
 Overview	
 Inputs	
 Outputs	
 Template	

web-server-url

<http://20.119.121.126>

web-server-url-wordpress

<http://20.119.121.126/wordpress>

web-server-url-sql-attack

<http://20.119.121.126/sql-attack.html>

ssh-web-vm

<ssh paloalto@20.119.121.126 -p 221>

username

paloalto

password

PaloAlt0@123

frontend-IP

20.119.121.126

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

Your deployment is complete

Deployment name : CreateFirewallForm-20230529045125
Subscription : Palo Alto Networks
Resource group : apr-zseducdsfbsu

Deployment details

Next steps

Go to resource group

- Within the resource group, click on “CloudNGFW-Demo” resource as shown below

apr-442vgf011ugbw

Resource group

Overview

Essentials

Subscriptions (move) : Palo Alto Networks
Subscription ID : c5cb9492-bf76-4231-88e7-17b9c0117bc0
Tags (edit) : Name : Ravisankar Pegada Class : Cloud-NGFW-Azure-BETA-Class

Deployments : 2 Succeeded
Location : East US

Resources Recommendations

Name	Type	Description
CloudNGFW-Demo	Cloud NGFW by Palo Alto Networks	Local Rulestack for Cloud NGFW by Palo Alto Network
CloudNGFW-Demo-1rs	Public IP address	
CloudNGFW-Demo-public-ip	Log Analytics workspace	
CloudNGFW-Logs		

- 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

Essentials

- Resource group (move) : [apr-zseductsfbsu](#)
- Location : East US
- Subscription (move) : [Palo Alto Networks](#)
- Subscription ID : c5cb9492-bf76-4231-88e7-17b9c0117bc0

Tags

Properties

Front end settings (edit)	...
Provisioning state (edit)	Succeeded

Networking & NAT

Network type (edit)	VNET
---------------------	------

DNS Proxy

- Enable DNS proxy (edit) : DISABLED
- Enabled DNS type (edit) : CUSTOM
- DNS servers (edit) : ---

Plan data

- Usage type (edit) : PAYG
- Billing cycle (edit) : MONTHLY
- Plan id (edit) : panw-cloud-ngfw-pa
- Effective date (edit) : 12/31/1, 7:03:58 PM

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

Microsoft Azure

Home > CloudNGFW-Demo

CloudNGFW-Demo | Log Settings

Cloud NGFW by Palo Alto Networks

Search Edit Refresh

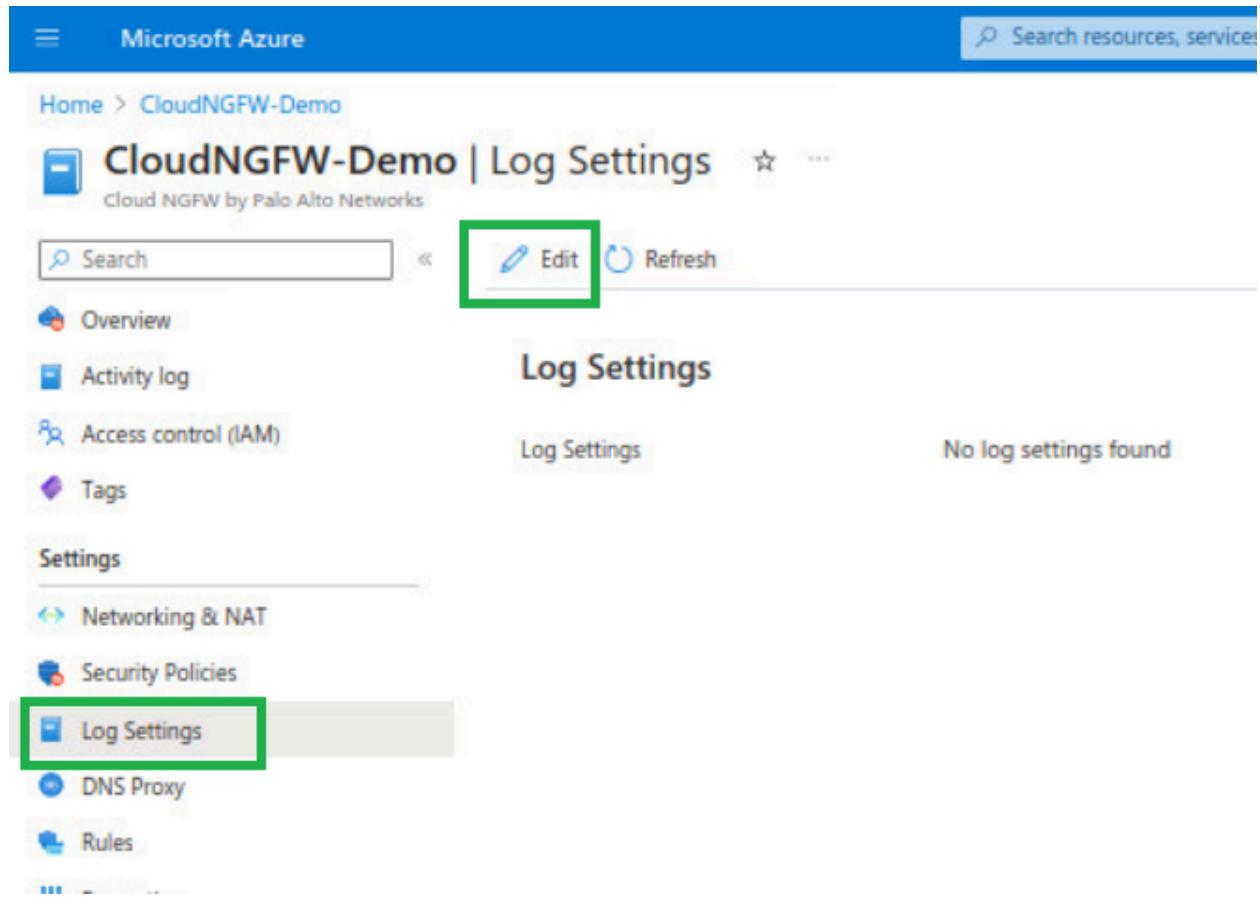
Overview Activity log Access control (IAM) Tags

Log Settings

No log settings found

Settings

Networking & NAT Security Policies Log Settings DNS Proxy Rules



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

Microsoft Azure

Home > CloudNGFW-Demo

CloudNGFW-Demo | Log Settings

Cloud NGFW by Palo Alto Networks

Search Save Discard

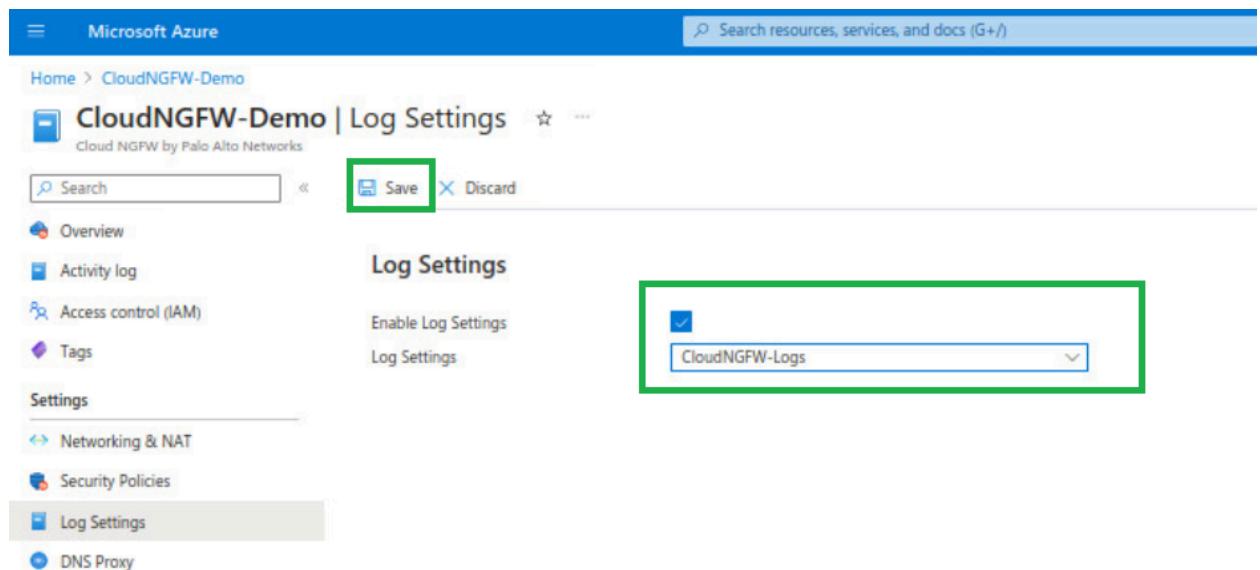
Overview Activity log Access control (IAM) Tags

Log Settings

Enable Log Settings

Log Settings

CloudNGFW-Logs



CloudNGFW-Demo | Log Settings

Cloud NGFW by Palo Alto Networks

Search

Overview

Activity log

Access control (IAM)

Tags

Log Settings

Networking & NAT

Security Policies

Log Settings

DNS Proxy

Rules

Properties

Log Settings

Updated log settings successfully

Log Settings

CloudNGFW-Logs

Workspace Id

812da118-65a0-4a33-9cb9-975f0775d930

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

The screenshot shows the Microsoft Azure portal interface for a CloudNGFW-Demo resource. The top navigation bar includes the Microsoft Azure logo, a search bar, and a 'Search resources, services, and docs (G+ /)' field. Below the navigation bar, the breadcrumb path 'Home > CloudNGFW-Demo' is shown, followed by the title 'CloudNGFW-Demo | Networking & NAT' and a subtitle 'Cloud NGFW by Palo Alto Networks'. A 'Edit' button is highlighted with a green box. The main content area is titled 'Networking' and shows a 'Virtual Network' configuration. The 'Type' is set to 'Virtual Network' (radio button selected). The 'Virtual Network' dropdown shows 'hub-vnet'. Below this, there are sections for 'Private subnet' (showing 'hub-private-subnet') and 'Public subnet' (showing 'hub-public-subnet'). On the left sidebar, under 'Settings', the 'Networking & NAT' tab is also highlighted with a green box. Other settings listed include 'Security Policies', 'Log Settings', and 'DNS Proxy'.

- 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

Home > CloudNGFW-Demo

CloudNGFW-Demo | Networking & NAT

Cloud NGFW by Palo Alto Networks

Search Save Discard

Virtual Network	hub-vnet
Private subnet	hub-private-subnet
Public subnet	hub-public-subnet

Settings

- Networking & NAT** (selected)
- Security Policies
- Log Settings
- DNS Proxy
- Rules
- Properties
- Locks

Support + troubleshooting

New Support Request

Monitoring

Alerts

Automation

Source Network Address Translation (SNAT)

Public IP Addresses: CloudNGFW-Demo-public-ip

Enable Source NAT:

Use the above Public IP addresses:

Destination Network Address Translation (DNAT)

Search

Add

- 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 Frontend Setting

Provide Configuration for Frontend Setting

Name *

AccessToWeb

Protocol *

TCP

UDP

Frontend IP *

frontendip

Frontend Port *

80

Backend IP *

10.5.0.5

Backend Port *

80

Add

Cancel

- 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
 -

Add Frontend Setting

Provide Configuration for Frontend Setting

Name *

SSHAccesstoWebServer

Protocol *

TCP

UDP

Frontend IP *

frontendip

Frontend Port *

221

Backend IP *

10.5.0.5

Backend Port *

22

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

The screenshot shows the CloudNGFW-Demo Networking & NAT interface. At the top right, there are 'Save' and 'Discard' buttons. The 'Save' button is highlighted with a green box. Below the buttons, there are sections for 'Private subnet' and 'Public subnet'. On the left, there's a sidebar with 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', and 'Settings' (with 'Networking & NAT' selected). On the right, there's a section titled 'Source Network Address Translation (SNAT)' with fields for 'Public IP Addresses' (set to 'frontendip') and a progress bar labeled 'Saving...'. A 'Networking' section is also visible.

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

This screenshot shows the same interface as above, but the 'Networking' section is highlighted with a green box and has a circular progress icon with the text 'Saving...' next to it, indicating the configuration is being saved.

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

Destination Network Address Translation (DNAT)

Name	Protocol	Frontend IP	Frontend Port	Backend IP	Backend Port
AccessToWeb	TCP	frontendip	80	10.5.0.5	80
SSHAcessToWe...	TCP	frontendip	221	10.5.0.5	22

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.

The screenshot shows the CloudNGFW-Demo Rules interface. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Networking & NAT, Security Policies, Log Settings, DNS Proxy, and Rules. The Rules option is highlighted with a red box. The main area has two search bars at the top. Below them is a table with columns: Priority, Name, Source, Destination, Constraints, Action, Logging, and Egress Decr. A single row is listed under 'Local Rules (1)'. The row details are: Priority 1000000, Name 'cloud-ngfw-default-rule', Source 'any', Destination 'any', Constraints 'Default', Action 'Allow', Logging 'yes', and Egress Decr 'Disabled'. This row is also highlighted with a green box.

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

The screenshot shows the Azure Resource Group 'apr-dgon2lsekypsm' overview page. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Deployments, Security, and Policies. The Overview section is selected. In the center, there's a table titled 'Resources' with columns: Name, Type, Location, and Status. One item is highlighted with a red box: 'CloudNGFW-Demo-lrs' (Type: Local Rulestack for Cloud NGFW by ...). Other items include 'CloudNGFW-Demo' (Type: Cloud NGFW by Palo Alto Networks, Location: East US), 'CloudNGFW-Logs' (Type: Log Analytics workspace, Location: East US), and 'database-1' (Type: Virtual machine, Location: East US).

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

CloudNGFW-Demo-lrs | Rules star ...

Local Rulestack for Cloud NGFW by Palo Alto Networks

Search
Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags

Settings

- Properties
- Locks

Resources

- Rules
- Security Services

Local Rules

A local rulestack consists of local rules. A local rulestack can contain up to 100 rules.

+ Add	Edit	Delete

Priority	Name
1000000	cloud-ngfw-default-rule

- 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

Define Rule Parameters

General

Name *

Description

Enabled



Source

Any

Match

IP Address (CIDR Format)

Countries

Prefix List

Exclude



Destination

Any

Match

IP Address (CIDR Format)

Countries

URL Category

Match Criteria

Any

Select

Protocol & Port

Match Criteria

Application Default

Any

Select

TCP ▾ 3306

Actions

Actions

Allow

Deny

Drop

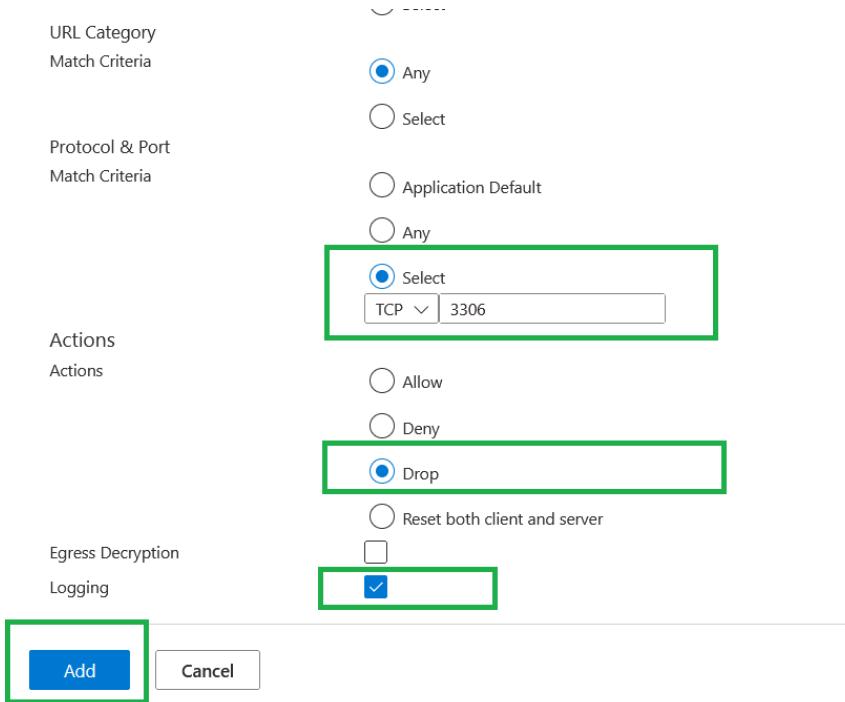
Reset both client and server

Egress Decryption

Logging

Add

Cancel



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 *

Description

Priority *

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 *

Protocol & Port

Match Criteria



Any



Select

Categories *

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

The screenshot shows the CloudNGFW-Demo-lrs | Deployment page. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Settings (Properties, Locks), Resources (Rules, Security Services, Prefix List, FQDN List, Certificates, Deployment, Managed Identity). The Deployment section is highlighted with a green box. It shows a table with columns: Config (Candidate Configuration), Status (Pending Deployment: LocalRule, Rulestack), and Action (Deploy Configuration, Revert). The Deploy Configuration button is also highlighted with a green box.

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

Deployment

The screenshot shows a Deploy dialog box. It has tabs for Config (Candidate Configuration) and Status. The Status tab is active, showing the text: Push your configured rulestacks to your firewalls. The Action section contains the text: The following firewall(s) will be deployed with the changes made to the rulestack. Below that, it lists: CloudNGFW-Demo(apr-dgon2lsekypsm). At the bottom are two buttons: Deploy (highlighted with a green box) and Cancel.

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

CloudNGFW-Demo-lrs | Deployment

Local Rulestack for Cloud NGFW by Palo Alto Networks

Search Refresh

Overview Activity log Access control (IAM) Tags

Settings Properties Locks

Resources Rules Security Services Prefix List FQDN List Certificates Deployment Managed Identity

Deployment

Config	Status	Action
Candidate Configuration	Deployed	Deploy Configuration Revert

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”

Microsoft Azure

Home > Microsoft.Template-20230529044822

Microsoft.Template-20230529044822 | Outputs

Deployment

Search

Overview Inputs Outputs Template

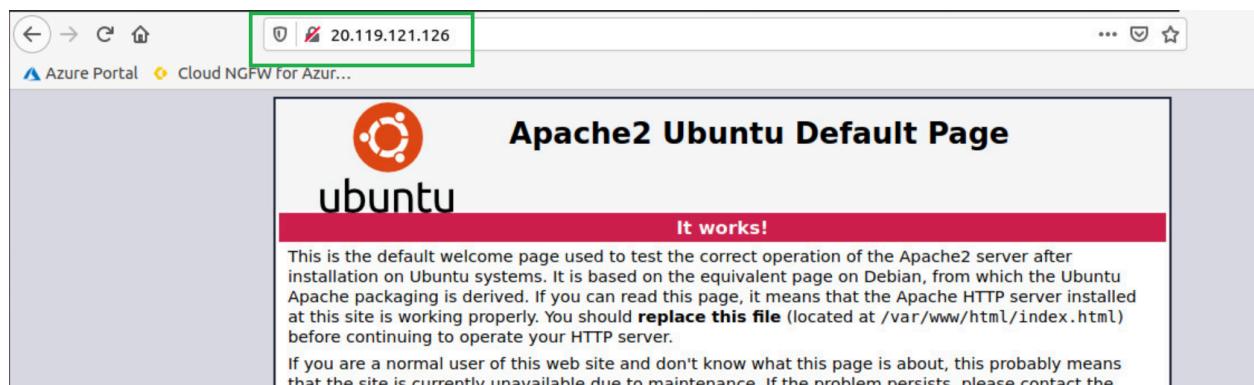
web-server-url
http://20.119.121.126

web-server-url-wordpress
http://20.119.121.126/wordpress

-20230529044822 | Outputs ...

web-server-url	http://20.119.121.126	
web-server-url-wordpress	http://20.119.121.126/wordpress	
web-server-url-sql-attack	http://20.119.121.126/sql-attack.html	

- 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.

Home >

apr-zseducdsfbbsu Resource group

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

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

Essentials

Subscription (move) : Palo Alto Networks Deployments : 2 Succeeded
Subscription ID : c5cb9492-bf76-4231-88e7-17b9c0117bc0 Location : East US
Tags (edit) : Name : Ravishankar Pegada Class : Cloud-NGFW-Azure-BETA-Class

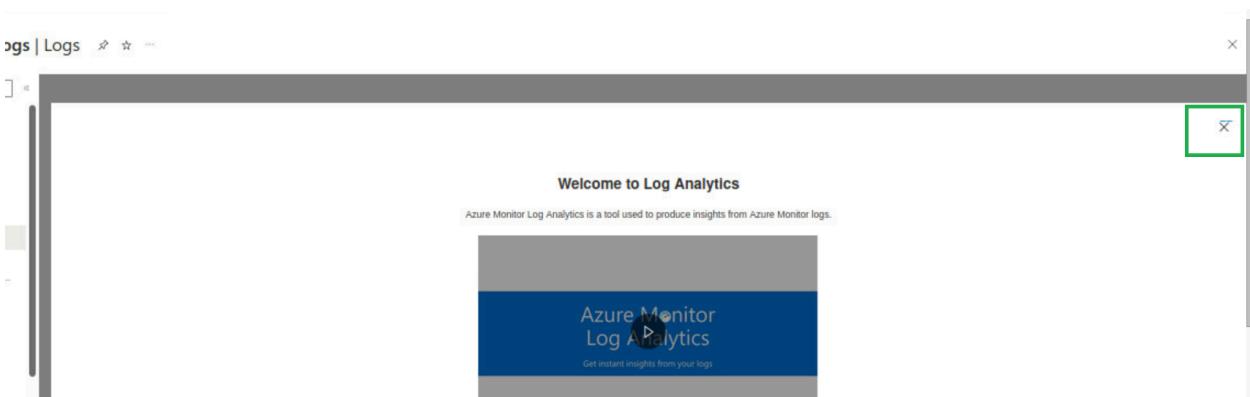
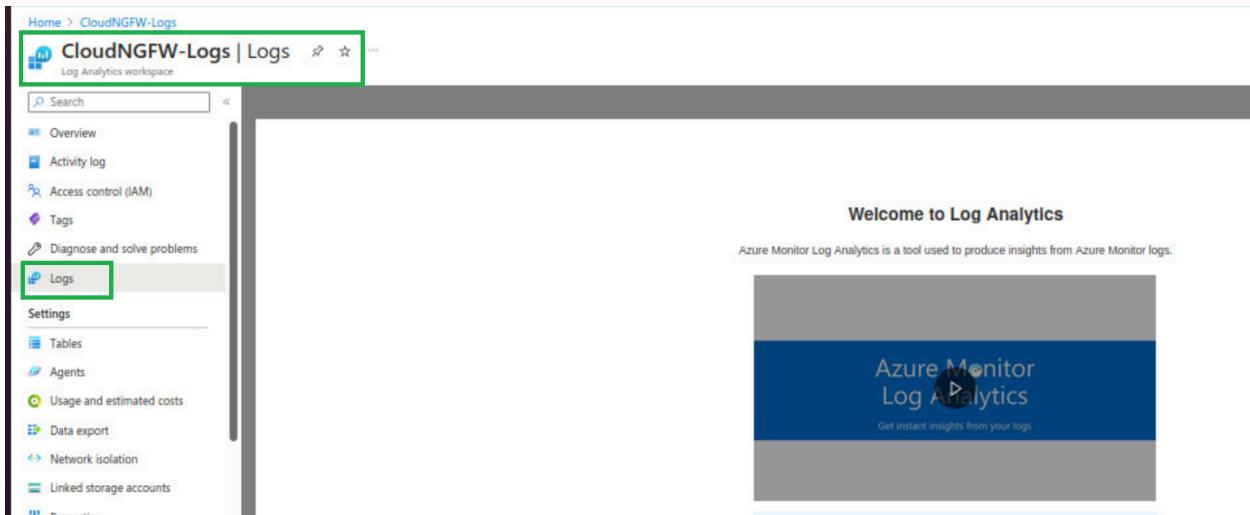
Resources Recommendations

Filter for any field... Type equals all Location equals all Add filter

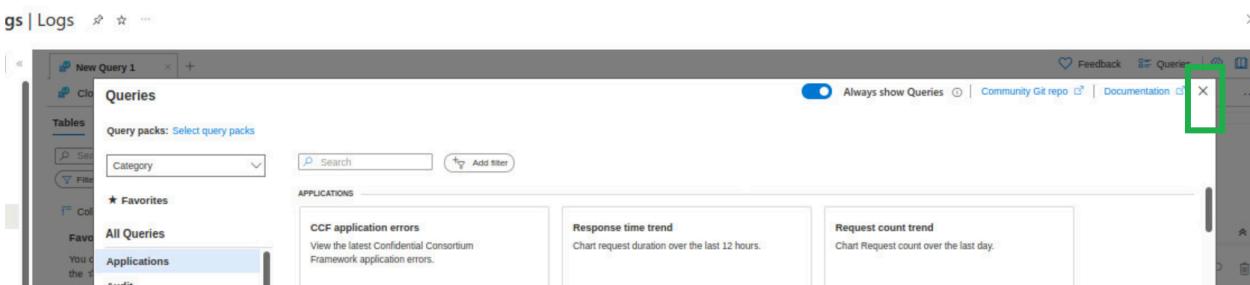
Showing 1 to 15 of 15 records. Show hidden types

Name	Type	Description
CloudNGFW-Demo	Cloud NGFW by Palo Alto Networks	Cloud NGFW-Demo
CloudNGFW-Demo-lrs	Local Rulestack for Cloud NGFW by Palo Alto Network	CloudNGFW-Demo-lrs
CloudNGFW-Logs	Log Analytics workspace	CloudNGFW-Logs

- Close “Welcome to Log Analytics” pop-up window



- Close the Queries page as shown below



- After going to Log Analytics workspace(CloudNGFW-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

Home > CloudNGFW-Logs

CloudNGFW-Logs | Logs

Log Analytics workspace

Search

New Query 1*

CloudNGFW-Logs Select scope

Run Time range Last 30 minutes Save

Tables Queries ...

1 fluentbit_CL

Search Filter Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the star icon

Custom Logs

fluentbit_CL

Queries History

- 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

The screenshot shows the Log Analytics workspace interface for the 'CloudNGFW-Logs' workspace. The top navigation bar includes the workspace name, a 'New Query 1+' button, and various action icons like Run, Save, Share, and Export. Below the navigation is a search bar and a 'Tables' tab selected. A query editor window is open with the title '1 fluentbit_CL'. The query results table displays log entries with columns: TimeGenerated [Local], _timestamp_d, pri_s, time_s, host_s, ident_s, Year_s, Month_s, Day_s, and H. The first four rows of the table are highlighted with green boxes.

TimeGenerated [Local]	_timestamp_d	pri_s	time_s	host_s	ident_s	Year_s	Month_s	Day_s	H
> 5/29/2023, 5:47:39.451 AM	1685328457	14	May 29 02:47:37	cloudngfw-demo	TRAFFIC	2023	05	29	0
> 5/29/2023, 5:47:39.451 AM	1685328457	14	May 29 02:47:37	cloudngfw-demo	TRAFFIC	2023	05	29	0
> 5/29/2023, 5:47:04.515 AM	1685328422	14	May 29 02:47:02	cloudngfw-demo	TRAFFIC	2023	05	29	0
> 5/29/2023, 5:47:04.515 AM	1685328422	14	May 29 02:47:02	cloudngfw-demo	TRAFFIC	2023	05	29	0

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

The screenshot shows a Google search interface. The search bar contains the query "what is my ip address". Below the search bar are several filter buttons: WiFi, VPN, For my router, And port, Of my computer, Ip4, and Images. A note indicates there are about 1,230,000,000 results found in 0.31 seconds. The main result is a card titled "What's my IP" which displays the IP address "38.87.199.134" in a large font, with the entire number highlighted by a green box. Below the IP address, it says "Your public IP address".

- 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.

Results		Chart
TimeGenerated [Local Time]	ident_s	Message
> 5/29/2023, 5:47:39.451 AM	TRAFFIC	["src_ip":"89.248.105.84","sport":53638,"dst_ip":"20.119.121.120","dport":80,"proto":"tcp","app":"incomplete","rule":"cloud-ngfw-default-rule","action":"allow","bytes_recv":58,"bytes_sent":180,"pkts_recv":1,"pkts_sent":1}
> 5/29/2023, 5:47:39.451 AM	TRAFFIC	["src_ip":"89.248.105.84","sport":53638,"dst_ip":"20.119.121.120","dport":80,"proto":"tcp","app":"incomplete","rule":"cloud-ngfw-default-rule","action":"allow","bytes_recv":58,"bytes_sent":180,"pkts_recv":1,"pkts_sent":1}
> 5/29/2023, 5:47:40.515 AM	TRAFFIC	["src_ip":"38.87.199.134","sport":44996,"dst_ip":"20.119.121.120","dport":80,"proto":"tcp","app":"web-browsing","rule":"cloud-ngfw-default-rule","action":"allow","bytes_recv":8320,"bytes_sent":1903,"pkts_recv":1,"pkts_sent":1}
> 5/29/2023, 5:47:40.515 AM	TRAFFIC	["src_ip":"38.87.199.134","sport":44996,"dst_ip":"20.119.121.120","dport":80,"proto":"tcp","app":"web-browsing","rule":"cloud-ngfw-default-rule","action":"allow","bytes_recv":8320,"bytes_sent":1903,"pkts_recv":1,"pkts_sent":1]
> 5/29/2023, 5:46:44.458 AM	THREAT	["src_ip":"38.87.199.134","sport":44996,"dst_ip":"20.119.121.120","dport":80,"proto":"tcp","app":"web-browsing","rule":"cloud-ngfw-default-rule","action":"alert","url_idx":1,"url_category_list":"medium-risk,ur..."]

TRAFFIC	{"src_ip":"38.87.199.134", "sport":44990, "dst_ip":"20.119.121.126", "dport":80, "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"allow", "log":true}
TRAFFIC	{"src_ip":"38.87.199.134", "sport":44990, "dst_ip":"20.119.121.126", "dport":80, "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"allow", "log":true}

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.



Error establishing a database connection

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.

Home > CloudNGFW-Demo-lrs

CloudNGFW-Demo-lrs | Rules

Local Rulestack for Cloud NGFW by Palo Alto Networks

Search Refresh

Overview Activity log Access control (IAM) Tags

Settings Properties Locks

Resources Rules Security Services

Local Rules

A local rulestack consists of local rules. A local rulestack can be used on multiple firewalls within the same subscription.

Add Edit Delete

Priority	Name	Source	Destination	Constraints	Action	Logging	Egress Decay...
400	BlockSocialNetworking	any	any	Custom	DenyResetS...	yes	Disabled
500	BlockMySQLFromWebToDB	match	match	Custom	DenyResetS...	yes	Disabled
1000000	cloud-ngfw-default-rule	any	any	Default	Allow	yes	Disabled

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

View Rule

Configured Parameters for the rule

Application

Match Criteria

Any

Select

URL Category

Match Criteria

Any

Select

Protocol & Port

Match Criteria

Application Default

Any

Select

TCP ▾ 3306

Actions

Actions

Allow

Deny

Drop

Reset both client and server

Egress Decryption

Logging

Validate

Cancel

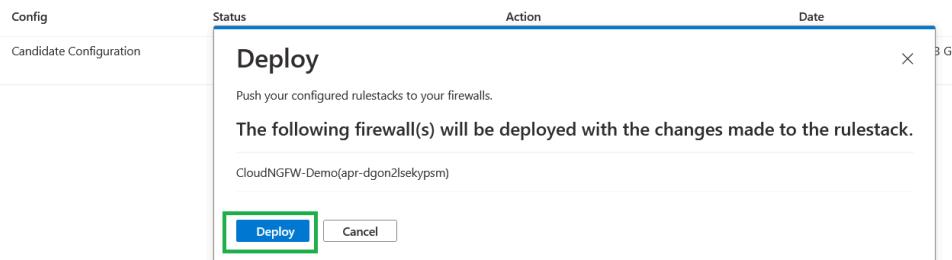
Deploy configuration

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

The screenshot shows the deployment interface for the CloudNGFW-Demo-Irs rulestack. The main title is "CloudNGFW-Demo-Irs | Deployment". On the left, there's a sidebar with "Overview", "Activity log", "Access control (IAM)", "Tags", "Settings" (selected), "Properties", "Locks", "Resources" (with "Rules", "Security Services", "Prefix List", "FQDN List", "Certificates"), and "Deployment" (selected). The main area has tabs for "Config" (selected) and "Status" (Candidate Configuration). The status bar says "Pending Deployment: LocalRule, Rulestack". Below it are "Action" buttons: "Deploy Configuration" (highlighted with a green box) and "Revert".

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

Deployment

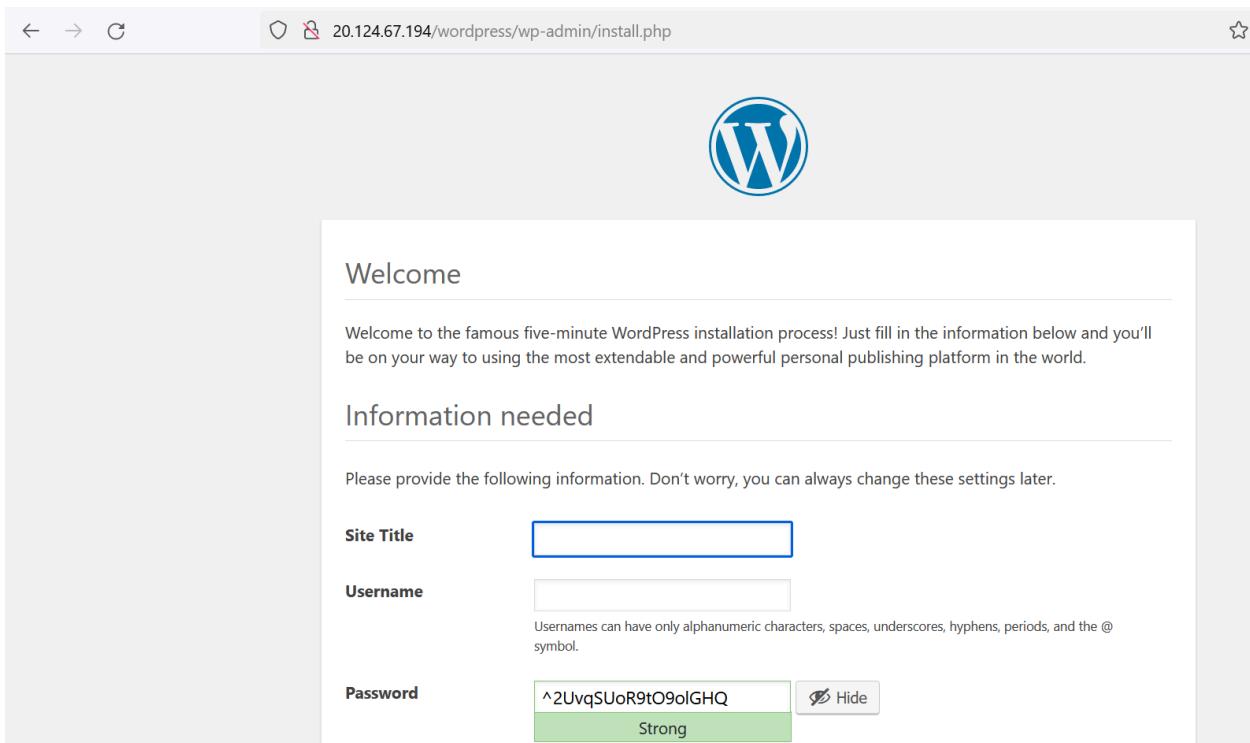


On Successful deployment, you should see the status as “**Deployed**” as shown below

The deployment interface shows the "Status" column with "Deployed" highlighted with a green box. The "Action" column still has the "Deploy Configuration" and "Revert" buttons.

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

A screenshot of the Microsoft Log Analytics workspace titled 'CloudNGFW-Logs | Logs'. The workspace is described as a 'Log Analytics workspace'. At the top, there's a search bar with 'New Query 1*' and a '+' button. Below the search bar, there are tabs for 'CloudNGFW-Logs' and 'Select scope'. A prominent blue 'Run' button is highlighted with a green rectangular box. To the right of the Run button, it says 'Time range : Last 30 minutes'. Further to the right are 'Save' and 'Log' buttons. Below the top navigation, there are two tabs: 'Tables' (which is selected) and 'Queries'. Under the 'Tables' tab, there is a single table named 'fluentbit_CL'. At the bottom of the interface is a search bar with a magnifying glass icon and a three-dot ellipsis button.

Results		
TimeGenerated [Local Time] ↑↓	ident_s	Message
> 5/31/2023, 2:25:36.157 PM	TRAFFIC	{"src_ip":"134.238.14.79", "sport":24837, "dst_ip":"20.124.67.194", "dport":80, "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"allow", "bytes_
> 5/31/2023, 2:25:36.157 PM	TRAFFIC	{"src_ip":"134.238.14.78", "sport":50213, "dst_ip":"20.124.67.194", "dport":80, "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"allow", "bytes_
> 5/31/2023, 2:25:36.157 PM	TRAFFIC	{"src_ip":"134.238.14.78", "sport":50213, "dst_ip":"20.124.67.194", "dport":80, "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"allow", "bytes_
> 5/31/2023, 2:25:36.157 PM	TRAFFIC	{"src_ip":"134.238.14.79", "sport":50213, "dst_ip":"20.124.67.194", "dport":80, "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"allow", "bytes_
> 5/31/2023, 2:25:36.157 PM	TRAFFIC	{"src_ip":"134.238.14.79", "sport":62148, "dst_ip":"20.124.67.194", "dport":80, "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"allow", "bytes_
> 5/31/2023, 2:25:31.589 PM	TRAFFIC	{"src_ip":"10.5.0.5", "sport":41974, "dst_ip":"10.6.0.5", "dport":3306, "proto":"tcp", "app":"mysql", "rule":"BlockMySQLFromWebToDB", "action":"allow", "bytes_recv":11091, "b
> 5/31/2023, 2:25:31.589 PM	TRAFFIC	{"src_ip":"10.5.0.5", "sport":41974, "dst_ip":"10.6.0.5", "dport":3306, "proto":"tcp", "app":"mysql", "rule":"BlockMySQLFromWebToDB", "action":"allow", "bytes_recv":11091, "b
> 5/31/2023, 2:25:26.820 PM	TRAFFIC	{"src_ip":"10.5.0.5", "sport":41972, "dst_ip":"10.6.0.5", "dport":3306, "proto":"tcp", "app":"mysql", "rule":"BlockMySQLFromWebToDB", "action":"allow", "bytes_recv":2894, "b

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

Home > CloudNGFW-Demo-Irs

CloudNGFW-Demo-Irs | Security Services ☆ ...

Local Rulestack for Cloud NGFW by Palo Alto Networks

Search Save Refresh

Overview Activity log Access control (IAM) Tags

Properties Locks

Rules Security Services Prefix List FQDN List Certificates Deployment Managed Identity

Support + troubleshooting New Support Request

IPS and Spyware Threats Protection

IPS Vulnerability

An Intrusion Prevention System (IPS) is a network security and threat prevention technology that examines traffic flow to detect and prevent malicious activity. It uses signature-based detection to identify known threats and behavioral analysis to detect new or emerging threats.

Enable Profile Best Practice

Anti-Spyware

Anti-spyware protection zeroes in on outbound threats, especially command-and-control (C2) activity, where an infected client attempts to communicate with a remote server. It uses behavioral analysis to detect and block such activity.

Enable Profile Best Practice

Malware and File-based Threat Protection

Antivirus

Antivirus protects against viruses, worms, and trojans as well as spyware downloads.

Task 1 - Access Sql attack URL

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

The screenshot shows the Azure portal's Outputs blade for a deployment named '-20230529044822'. It lists several outputs, including 'web-server-url', 'web-server-url-wordpress', and 'web-server-url-sql-attack'. The 'web-server-url-sql-attack' output is highlighted with a green box. The URL value is 'http://20.119.121.126/sql-attack.html'.

- 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

A screenshot of a browser window. The address bar shows the URL '20.124.67.194/sql-attack.html'. Below the address bar, there are two prominent pink buttons with white text: 'LAUNCH WEB TO DB SSH ATTEMPT' and 'LAUNCH BRUTE FORCE SQL ROOT PASSWORD GUESSING'. The 'LAUNCH BRUTE FORCE SQL ROOT PASSWORD GUESSING' button is enclosed in a green box.

- You will be presented with below mentioned screen

A screenshot of a browser window. The address bar shows the URL '20.124.67.194/cgi-bin/guess-sql-root-password.cgi?'. The page content is not visible in the screenshot.

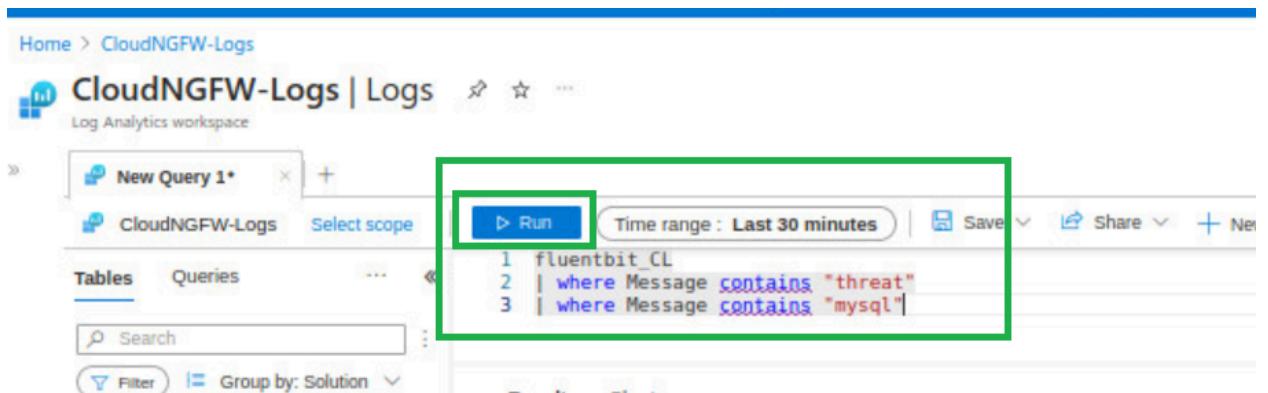
Brute force MySQL root password attempt launched.

Task 3 - Verify THREAT logs on Log Analytics workspace

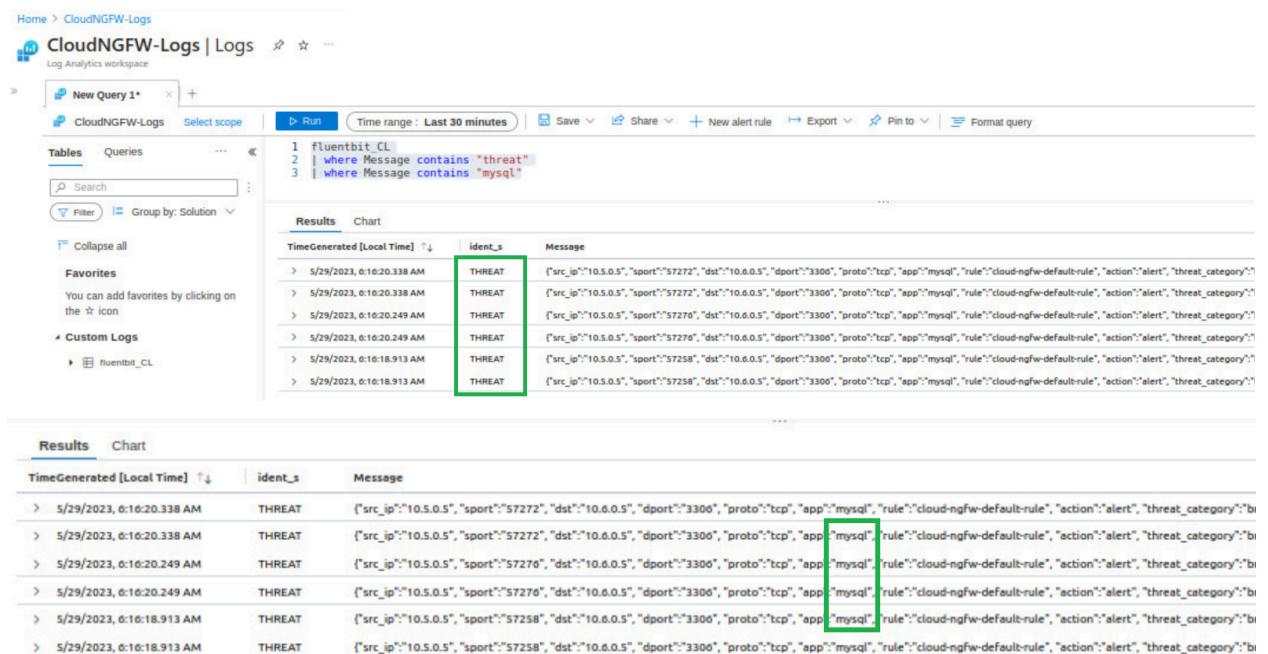
- To verify the threat logs, go to log analytics workspace and run the below mentioned query. This query will filter threat logs that include mysql traffic.

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.

The screenshot displays two separate Azure ARM template output sections, each titled "-20230529044822 | Outputs".

Output 1 (Top):

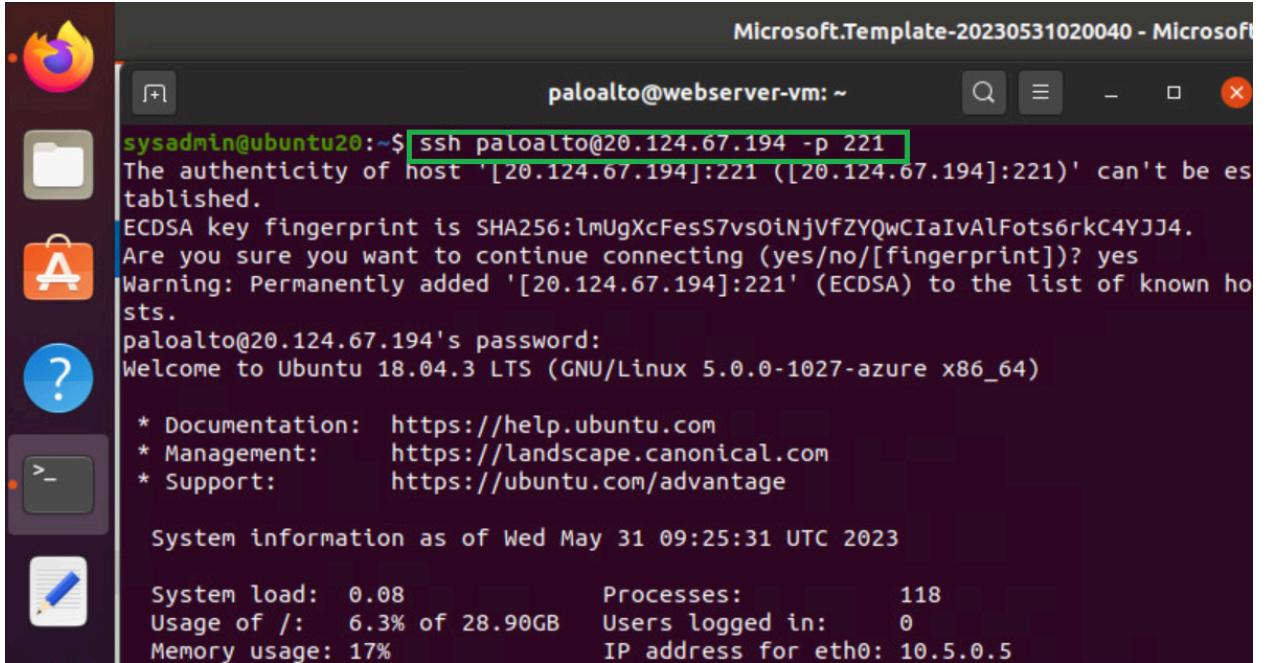
- web-server-url: http://20.119.121.126
- web-server-url-wordpress: http://20.119.121.126/wordpress
- web-server-url-sql-attack: http://20.119.121.126/sql-attack.html
- ssh-web-vm:** ssh paloalto@20.119.121.126 -p 221
- username: paloalto

Output 2 (Bottom):

- web-server-url: http://20.119.121.126
- web-server-url-wordpress: http://20.119.121.126/wordpress
- web-server-url-sql-attack: http://20.119.121.126/sql-attack.html
- ssh-web-vm:** ssh paloalto@20.119.121.126 -p 221
- username: paloalto
- password:** Pal0Alt0@123
- frontend-IP: (This field is partially visible at the bottom right)

In both outputs, the "ssh-web-vm" and "password" fields are highlighted with green boxes.

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



```

paloalto@webserver-vm: ~
sysadmin@ubuntu20:~$ ssh paloalto@20.124.67.194 -p 221
The authenticity of host '[20.124.67.194]:221 ([20.124.67.194]:221)' can't be established.
ECDSA key fingerprint is SHA256:lmUgXcFesS7vs0iNjVfZYQwCIAiVAlFots6rkC4YJJ4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[20.124.67.194]:221' (ECDSA) to the list of known hosts.
paloalto@20.124.67.194's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.0.0-1027-azure x86_64)

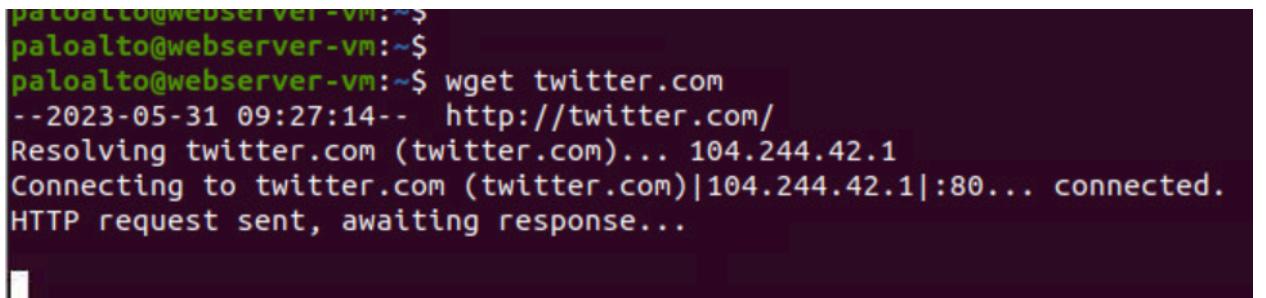
 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

 System information as of Wed May 31 09:25:31 UTC 2023

 System load: 0.08          Processes:           118
 Usage of /: 6.3% of 28.90GB   Users logged in:     0
 Memory usage: 17%          IP address for eth0: 10.5.0.5

```

- 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.



```

paloalto@webserver-vm:~$ 
paloalto@webserver-vm:~$ 
paloalto@webserver-vm:~$ wget twitter.com
--2023-05-31 09:27:14-- http://twitter.com/
Resolving twitter.com (twitter.com)... 104.244.42.1
Connecting to twitter.com (twitter.com)|104.244.42.1|:80... connected.
HTTP request sent, awaiting response...

```

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

Results	Chart	
TimeGenerated [Local Time] ↑↓	ident_s	Message
> 5/31/2023, 2:57:16.399 PM	TRAFFIC	{"src_ip":"10.5.0.5", "sport":42300, "dst_ip":"104.244.42.1", "dport":80, "proto":"tcp", "app":"twitter-base", "rule":"BlockSocialNetworking", "action":"reset-server", "bytes_rec":11999, "bytes_sent":11999, "start_time":2023/05/31 02:27:13, "elapsed_time":0, "repeat_count":1, "category":"social-networking", "src_country":10.0.0.0-10.255.255.255, "dst_country":United States, "session_end_reason":"policy-deny", "xff_ip":null}
> 5/31/2023, 2:57:16.399 PM	TRAFFIC	{"src_ip":"10.5.0.5", "sport":42300, "dst_ip":"104.244.42.1", "dport":80, "proto":"tcp", "app":"twitter-base", "rule":"BlockSocialNetworking", "action":"reset-server", "bytes_rec":11999, "bytes_sent":11999, "start_time":2023/05/31 02:27:13, "elapsed_time":0, "repeat_count":1, "category":"social-networking", "src_country":10.0.0.0-10.255.255.255, "dst_country":United States, "session_end_reason":"policy-deny", "xff_ip":null}
> 5/31/2023, 2:55:51.964 PM	TRAFFIC	{"src_ip":"10.5.0.5", "sport":56758, "dst_ip":"185.125.190.18", "dport":443, "proto":"tcp", "app":null, "rule":"cloud-natfw-default-rule", "action":"allow", "bytes_rec":11999, "bytes_sent":11999, "start_time":2023/05/31 02:27:13, "elapsed_time":0, "repeat_count":1, "category":null, "src_country":null, "dst_country":null, "session_end_reason":null, "xff_ip":null}
> 5/31/2023, 2:55:51.964 PM	TRAFFIC	{"src_ip":"10.5.0.5", "sport":56758, "dst_ip":"104.244.42.1", "dport":80, "proto":"tcp", "app":"twitter-base", "rule":"BlockSocialNetworking", "action":"reset-server", "bytes_rec":11999, "bytes_sent":11999, "start_time":2023/05/31 02:27:13, "elapsed_time":0, "repeat_count":1, "category":"social-networking", "src_country":10.0.0.0-10.255.255.255, "dst_country":United States, "session_end_reason":"policy-deny", "xff_ip":null}
> 5/31/2023, 2:55:51.947 PM	DECRYPTION	{"src_ip":"10.5.0.5", "sport":56758, "bytes_rec":548, "bytes_sent":344, "pkts_received":2, "pkts_sent":2, "start_time":2023/05/31 02:27:13, "elapsed_time":0, "repeat_count":1, "category":null, "src_country":null, "dst_country":null, "session_end_reason":null, "xff_ip":null}
> 5/31/2023, 2:55:51.947 PM	DECRYPTION	{"src_ip":"10.5.0.5", "sport":56758, "bytes_rec":548, "bytes_sent":344, "pkts_received":2, "pkts_sent":2, "start_time":2023/05/31 02:27:13, "elapsed_time":0, "repeat_count":1, "category":null, "src_country":null, "dst_country":null, "session_end_reason":null, "xff_ip":null}
> 5/31/2023, 2:48:51.880 PM	TRAFFIC	{"src_ip":"66.240.205.34", "sport":59690, "dst_ip":"20.124.67.194", "dport":80, "proto":"tcp", "app":null, "rule":"cloud-natfw-default-rule", "action":"allow", "bytes_rec":11999, "bytes_sent":11999, "start_time":2023/05/31 02:27:13, "elapsed_time":0, "repeat_count":1, "category":null, "src_country":null, "dst_country":null, "session_end_reason":null, "xff_ip":null}
> 5/31/2023, 2:48:51.880 PM	TRAFFIC	{"src_ip":"66.240.205.34", "sport":59690, "dst_ip":"20.124.67.194", "dport":80, "proto":"tcp", "app":null, "rule":"cloud-natfw-default-rule", "action":"allow", "bytes_rec":11999, "bytes_sent":11999, "start_time":2023/05/31 02:27:13, "elapsed_time":0, "repeat_count":1, "category":null, "src_country":null, "dst_country":null, "session_end_reason":null, "xff_ip":null}

END of LAB