



# Cloud NGFW Azure VWAN Lab Guide

Date: Dec, 2023  
Authors: Ravisankar Pegada

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Purpose of This Workshop Guide</b>	<b>2</b>
<b>Lab Activities Overview</b>	<b>2</b>
<b>Part-1 : Build test setup that will be used for this workshop using ARM template</b>	<b>3</b>
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
<b>Part-2 : Create and Configure Cloud NGFW for Azure using Azure portal to secure user traffic</b>	<b>14</b>
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
<b>Part-3 : Secure user traffic using Cloud NGFW for Azure</b>	<b>39</b>
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 Azure VWAN 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 : Configure Routing Intent on Azure VWAN Hub

Part-4 : Test traffic secured through Cloud NGFW. Simulate attack and verify Cloud NGFW in action

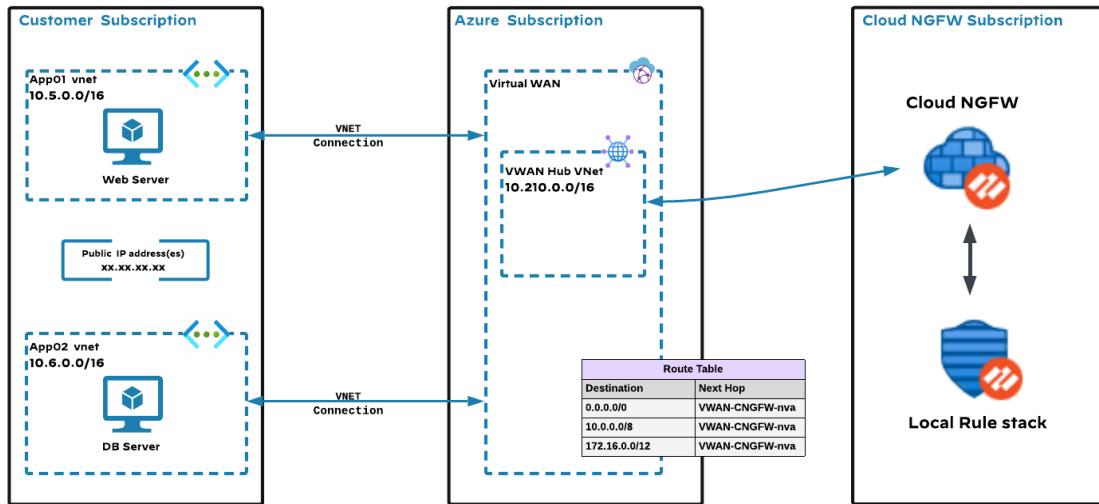
### **Once These Activities Have Been Completed**

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 VWAN 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

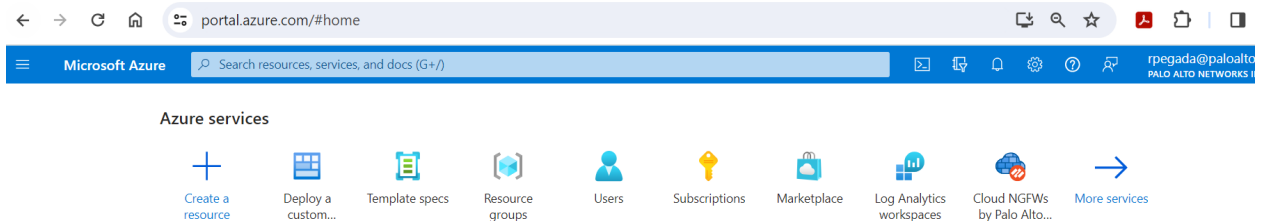


- As part of this workshop we are going to build two spoke VNETs with Web and DB servers created within those VNETs. VWAN Hub will be created and connected to the spoke VNETs
- We will access Web Server within Spoke1 vnet through Cloud NGFW
- Initiate bruteforce attack from web to db and see how cloud NGFW reports the same.
- Validate Outbound Internet access through CNGFW and verify URL filtering

## Activity 0: Log In to the Azure Portal

In this activity, you will:

- Log in to the Azure portal using your own account.



End of Activity-0

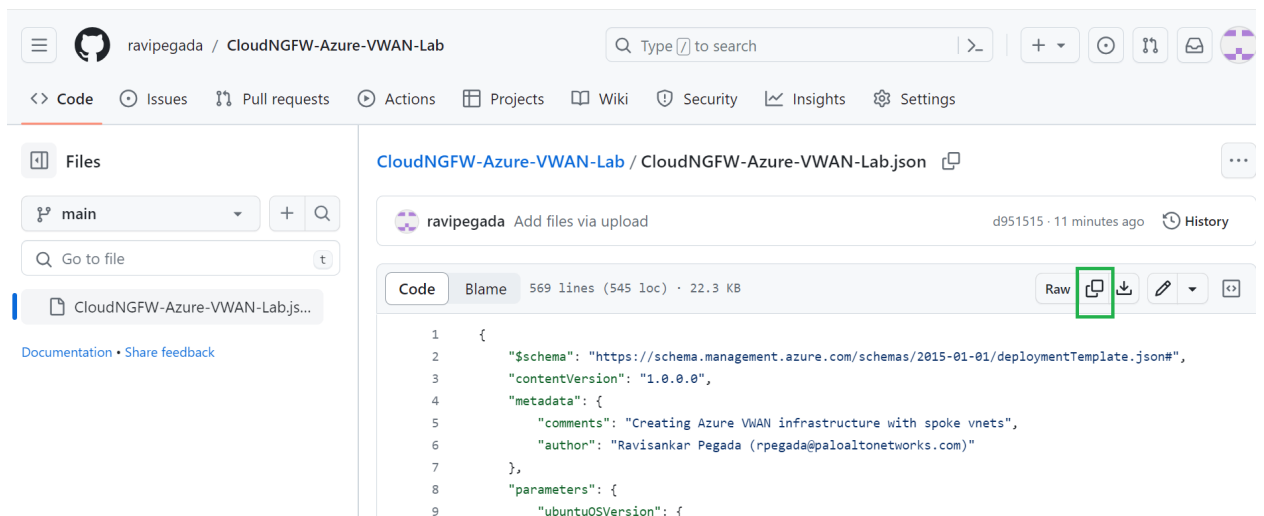
## Activity 1: Deploy Lab Environment with ARM Template

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

- Azure Virtual WAN with a Hub
- Spoke VNet with a Web server and required tools installed
- Spoke VNet with DB server and required tools installed
- Connect Spoke VNets with VWAN Hub
- Log analytics workspace

### Task 1 - Launch ARM Template to deploy lab resources

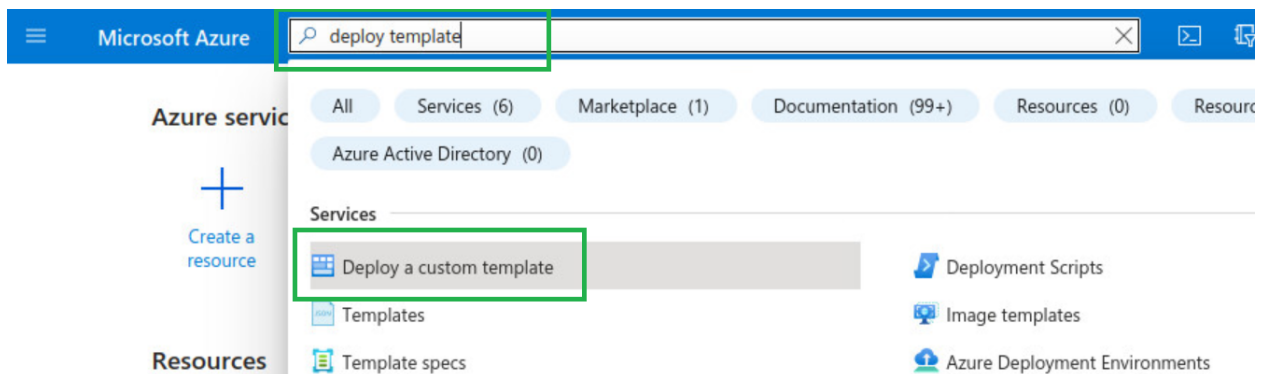
- Copy the template from [Cloud NGFW for Azure VWAN Lab ARM Template](#)



The screenshot shows a GitHub repository for 'ravigegada / CloudNGFW-Azure-VWAN-Lab'. The file 'CloudNGFW-Azure-VWAN-Lab.json' is selected, showing its content in a code editor. The code is an ARM template with the following structure:

```
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "metadata": {
5     "comments": "Creating Azure VWAN infrastructure with spoke vnets",
6     "author": "Ravisankar Pegada (rpegada@paloaltonetworks.com)"
7   },
8   "parameters": {
9     "ubuntuOSVersion": {
```

- 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.

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

Home >

## Custom deployment

Deploy from a custom template

Select a template Basics Review + create

Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started. [Learn more about template deployment](#)

**Build your own template in the editor**

Common templates

- Remove default template content by selecting all and clicking delete

Home > Custom deployment >

## Edit template

Edit your Azure Resource Manager template

+ Add resource ↑ Quickstart template ↶ Load file ↓ Download

Parameters (0)  
Variables (0)  
Resources (0)

```

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 }

```

- Paste the copied ARM template data and click on Save

Home > Custom deployment >

## Edit template

Edit your Azure Resource Manager template

+ Add resource ↑ Quickstart template ↶ Load file ↓ Download

Parameters (2)  
Variables (56)  
Resources (15)

- [variables(nsg\_name\_spoke\_su) (Microsoft.Network/networkSecurityRuleCollection)]
- [variables(inbound\_pip\_name) (Microsoft.Network/publicIPAddresses)]
- [variables(spoke1\_pip\_name) (Microsoft.Network/publicIPAddresses)]
- [variables(spoke2\_pip\_name) (Microsoft.Network/publicIPAddresses)]
- [variables(spoke1\_vnet\_name) (Microsoft.Network/virtualNetworks)]
- [variables(spoke2\_vnet\_name) (Microsoft.Network/virtualNetworks)]
- [variables(vm1\_nic\_name) (Microsoft.Network/networkInterfaces)]

```

1 {
2   "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "metadata": {
5     "comments": "Creating Azure WAN infrastructure with spoke vnets",
6     "author": "Ravisankar Pegada (rpegada@paloaltonetworks.com)"
7   },
8   "parameters": {
9     "ubuntuOSVersion": {
10      "type": "string",
11      "defaultValue": "18.04-LTS",
12      "allowedValues": [
13        "18.04-LTS",
14        "16.04.0-LTS",
15        "14.04.5-LTS"
16      ]
17     },
18     "metadata": {
19       "description": "The Ubuntu version for the VM. This will pick a fully patched image of this given Ubuntu version."
20     }
21   }
22 }

```

Allowed values: 18.04-LTS, 16.04.0-LTS, 14.04.5-LTS.


**Save** Discard

- Now within Basics tab Select the “Resource group” from the drop down or **Create new** and click on “Review + create” as shown below

[Home](#) >

## Custom deployment ...

Deploy from a custom template

 New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Select a template   **Basics**   Review + create

### Template



Customized template [↗](#)  
15 resources

 Edit template

 Edit parameters

 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 \* ⓘ

AzureTME



Resource group \* ⓘ

CloudNGFW-Azure-Demo-Lab

[Create new](#)

### Instance details

Region \* ⓘ

(US) East US

Ubuntu OS Version ⓘ

18.04-LTS

Vm Size ⓘ

Standard\_B1s

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 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.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for

**Create**   < Previous   Next

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

[Home](#) >

### Microsoft.Template-20231214135509 | Overview

Deployment

Search   Delete   Cancel   Redeploy   Download   Refresh

- Overview
- Inputs
- Outputs
- Template

**... Deployment is in progress**

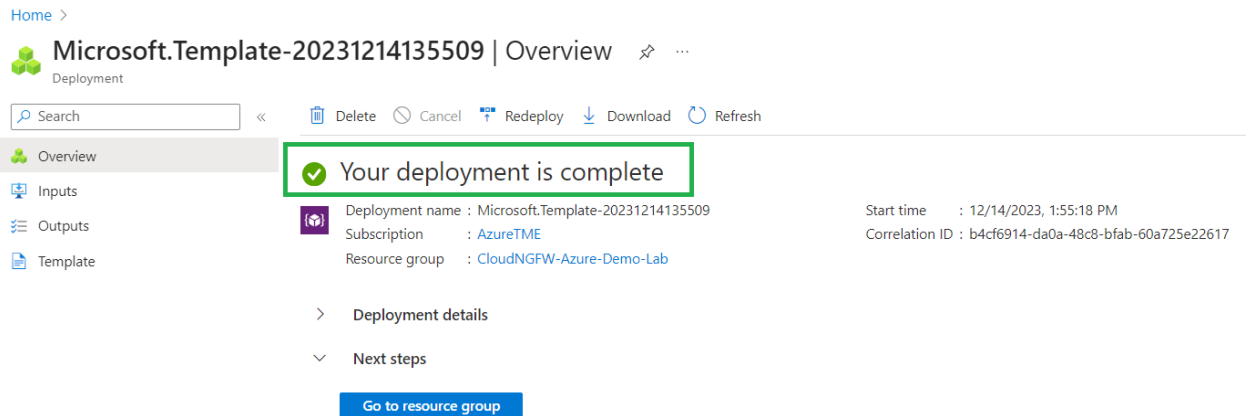
Deployment name : Microsoft.Template-20231214135509   Start time : 12/14/2023, 1:55:18 PM  
Subscription : AzureTME   Correlation ID : b4cf6914-da0a-48c8-bfab-60a725e22617  
Resource group : CloudNGFW-Azure-Demo-Lab

Deployment details

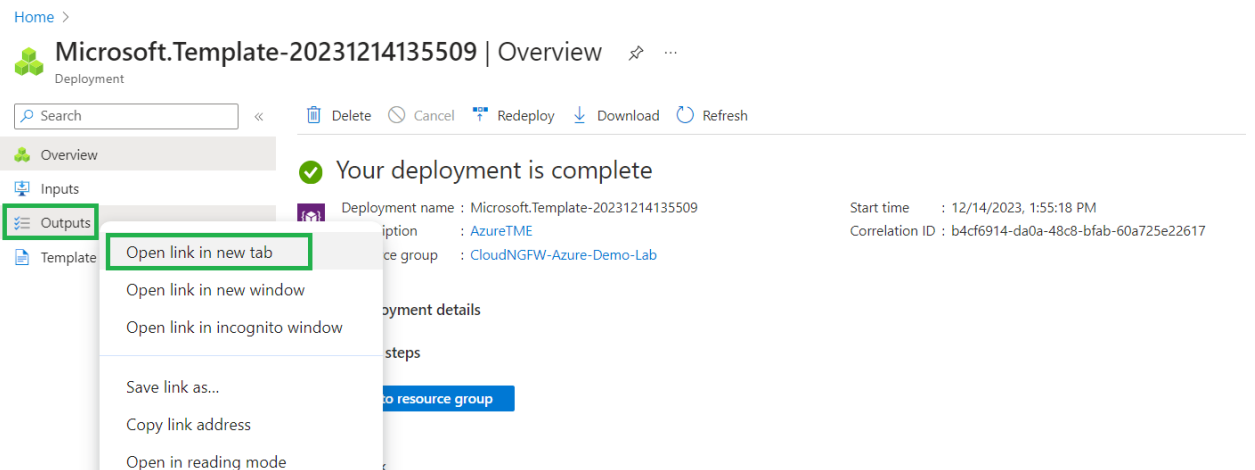
Resource	Type	Status	Operation details
database-vm/installcustomscript	Microsoft.Compute/virtualMachines/extension	Created	<a href="#">Operation details</a>
webserver-vm/installcustomscript	Microsoft.Compute/virtualMachines/extension	Created	<a href="#">Operation details</a>
database-vm	Virtual machine	OK	<a href="#">Operation details</a>
webserver-vm	Virtual machine	OK	<a href="#">Operation details</a>
database-vm-nic0	Network interface	Created	<a href="#">Operation details</a>
webserver-vm-nic0	Network interface	Created	<a href="#">Operation details</a>
CNGFW-Demo-VWAN-Hub01	Microsoft.Network/virtualHub	Created	<a href="#">Operation details</a>



- Wait for the deployment to get completed



- Right click on **Outputs** and open in new tab



- You will be presented with the below screen. We are going to use these URLs in in Part-3 below to showcase securing user traffic using Cloud NGFW

Home > Microsoft.Template-20231214135509

## Microsoft.Template-20231214135509 | Outputs

Deployment

Search

- Overview
- Inputs
- Outputs
- Template

web-server-url  
http://4.156.189.70

web-server-url-wordpress  
http://4.156.189.70/wordpress

web-server-url-sql-attack  
http://4.156.189.70/sql-attack.html

ssh-web-vm  
ssh paloalto@4.156.189.70 -p 221

username  
paloalto

password  
Pa10AlT0@123

frontend-IP  
4.156.189.70

- Go to the resource group to verify all the resources created. Click on “Go to Resource group” within your deployment page as shown below.

Home >

## Microsoft.Template-20231214135509 | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

- Overview
- Inputs
- Outputs
- Template

**Your deployment is complete**

Deployment name : Microsoft.Template-20231214135509  
Subscription : AzureTME  
Resource group : CloudNGFW-Azure-Demo-Lab

Start time : 12/14/2023, 1:55:18 PM  
Correlation ID : b4cf6914-da0a-48c8-bfab-60a725e22617

> Deployment details

∨ Next steps

**Go to resource group**

- You will see all the resources as shown below. Click on “Virtual WAN ” resource created

Home > Microsoft.Template-20231214135509 | Overview

## CloudNGFW-Azure-Demo-Lab

Resource group

Search

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

- Overview
- Activity log
- Access control (IAM)
- Tags
- Resource visualizer
- Events
- Settings
  - Deployments
  - Security
  - Deployment stacks
  - Policies
  - Properties
  - Locks
  - Cost Management

Essentials

Resources Recommendations

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

Showing 1 to 14 of 14 records. Show hidden types No grouping List view

Name	Type	Location
CloudNGFW-Logs	Log Analytics workspace	East US
<b>CNGFW-Demo-VWAN</b>	Virtual WAN	East US
database-vm	Virtual machine	East US
database-vm-nic0	Network Interface	East US
database-vm_OSDisk	Disk	East US
dbserverpip	Public IP address	East US
frontendip	Public IP address	East US
spoke-subnets-nsg	Network security group	East US

- Check for the status of Virtual WAN to be successful and click on “Hubs” as shown below

Home > Microsoft.Template-20231214135509 | Overview > CloudNGFW-Azure-Demo-Lab >

**CNGFW-Demo-VWAN** Virtual WAN

Search << Delete Refresh

**Overview**

- Activity log
- Access control (IAM)
- Tags
- Settings
  - Configuration
  - Properties
  - Locks
- Connectivity
  - Hubs**
  - VPN sites
  - User VPN configurations
  - ExpressRoute circuits
  - Virtual network connections
- Monitor

**Essentials**

Resource group : [CloudNGFW-Azure-Demo-Lab](#)

Location : East US

Subscription : [AzureTME](#)

Subscription ID : 0683d406-4d77-4bb7-b1a6-165c282b5d37

Tags (edit) : [Add tags](#)

World map

Status : **Succeeded**

Branch-to-branch : Enabled

Virtual hubs : 1

Topology : [View Topology](#)

- You will see the Hub status as Updating as shown below

Home > Microsoft.Template-20231120110620 | Overview > CloudNGFW-Azure-Demo-Lab > CNGFW-Demo-VWAN

**CNGFW-Demo-VWAN | Hubs** Virtual WAN

Search << + New Hub Refresh

Search for hubs by name Clear all filters

Add filter

Hub	Hub status	Region	VPN sites	Address Space	Point-to-site	ExpressRoute Circuits
CNGFW-Demo-VWAN-Hub0	Updating	East US	-	10.210.0.0/24	-	-

Overview

- Activity log
- Access control (IAM)
- Tags
- Settings
  - Configuration
  - Properties
  - Locks
- Connectivity
  - Hubs**
  - VPN sites
  - User VPN configurations

- Hub status will be changed to Succeeded in a couple of minutes

Home > Microsoft.Template-20231214135509 | Overview > CloudNGFW-Azure-Demo-Lab > CNGFW-Demo-VWAN

**CNGFW-Demo-VWAN | Hubs** Virtual WAN

Search << + New Hub Refresh

Search for hubs by name Clear all filters

Add filter

Hub	Hub status	Region	VPN sites	Address Space	Point-to-site
CNGFW-Demo-VWAN-Hub0	Succeeded	East US	-	10.210.0.0/24	-

Overview

- Activity log
- Access control (IAM)
- Tags
- Settings
  - Configuration
  - Properties
  - Locks
- Connectivity
  - Hubs**
  - VPN sites
  - User VPN configurations

- Click on the Hub created to verify the Hub and its Routing status. **Make sure that the Routing status is in “Provisioned” state. This will take around 30 Min for the routing status to get updated**

Home > CNGFW-Demo-VWAN | Hubs >

**CNGFW-Demo-VWAN-Hub01** Virtual HUB

Search Edit virtual hub Delete Refresh Reset router Reset Hub

Overview

Connectivity

- VPN (Site to site)
- ExpressRoute
- User VPN (Point to site)

Routing

- Route Maps (Preview)
- Routing Intent and Routing Policies

Essentials

Name : [CNGFW-Demo-VWAN-Hub01](#) Routing status : ✔ Provisioned

Resource group : [CloudNGFW-Azure-Demo-Lab](#) Hub routing preference : ExpressRoute

Tags : [Tags](#) Metrics : [View in Azure Monitor](#)

Hub status : ✔ Succeeded

Private address space : 10.210.0.0/24

[See more](#)

Virtual network connections  
Connect virtual networks to a virtual

VPN (Site to site)  
Connect a VPN Site to a virtual hub VPN

User VPN (Point to site)  
Connect a User VPN Configuration to a

- Now Click on “Home” to go to your Azure portal home page

Home > Microsoft.Template-20231120110620 | Overview > CloudNGFW-Azure-Demo-Lab > CNGFW-Demo-VWAN | Hubs >

**CNGFW-Demo-VWAN-Hub01** Virtual HUB

Search Edit virtual hub Delete Refresh Reset router Reset Hub

Overview

Connectivity

- VPN (Site to site)
- ExpressRoute
- User VPN (Point to site)

Routing

- Route Maps (Preview)
- Routing Intent and Routing Policies
- BGP Peers

Essentials

Name : [CNGFW-Demo-VWAN-Hub01](#) Routing status : ✔ Provisioned

Resource group : [CloudNGFW-Azure-Demo-Lab](#) Hub routing preference : ExpressRoute

Tags : [Tags](#) Metrics : [View in Azure Monitor](#)

Hub status : ✔ Succeeded

Private address space : 10.210.0.0/24

[See more](#)

Virtual network connections  
Connect virtual networks to a virtual hub.  
vNet connections: 2

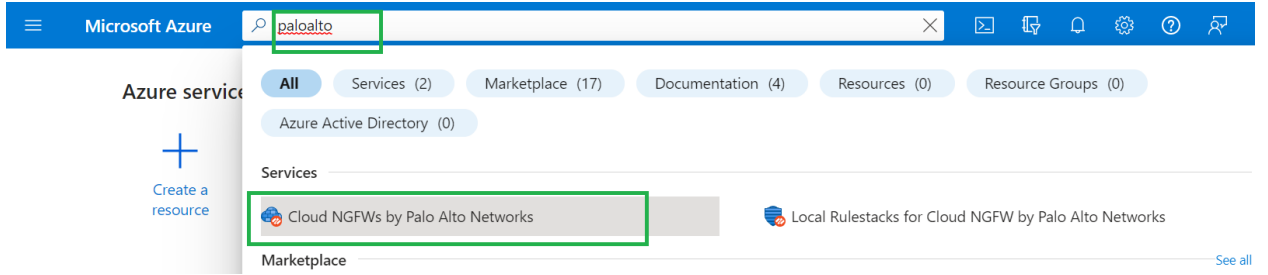
VPN (Site to site)  
Connect a VPN Site to a virtual hub VPN Gateway.  
● No gateway (Create)

User VPN (Point to site)  
Connect a User VPN Configuration to a virtual hub User VPN Gateway.  
● No gateway (Create)

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

### Activity 1: Create Cloud NGFW Service

- Within Azure Home page, 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

[Home](#) >

## Cloud NGFWs by Palo Alto Networks

Cloudshare (azurecloudshare.onmicrosoft.com) | PREVIEW

[+ Create](#) [Manage view](#) [Refresh](#) [Export to CSV](#) [Open query](#)

[Subscription equals all](#) [Resource group equals all](#)

- Within the “**Basics**” tab, select the “**Resource group**” that we have used in Part-1 above to create the resources from the drop down(*CloudNGFW-Azure-Demo-Lab*). Provide a name for “**Firewall Name**”, Ex: *CloudNGFW-Azure-VWAN-Demo* and select “**Marketplace Plan**” by leaving **Region** to default(East US) or select the region where you have created resources in Part-1 as shown in below screenshot.  
Click on “**Next**” to proceed further with creation of Cloud NGFW

# 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.

Subscription \* ⓘ

Resource group \* ⓘ  [Create new](#)

## Firewall Details

Firewall Name \* ⓘ

Region \* ⓘ

Marketplace Plan \* ⓘ

- Within the Networking section select the Network Type as “**Virtual Wan Hub**” and you will be presented with an option to select Virtual Wan Hub Name as shown below. Select the Virtual Hub Name(*CNGFW-Demo-VWAN-Hub01*) that you have created in Part-1 from the drop down.

**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

Click on “**Next**” to proceed further with Security Policies creation

# Create Cloud NGFW by Palo Alto Networks ...

Basics Networking Security Policies DNS Proxy Tags Terms Review + create

Please configure your Firewall deployment with network requirements, i.e., Public IP CIDR and virtual network settings.

## Network Type

Type \*

- Virtual Network  
 Virtual Wan Hub

## Virtual Wan Hub Details

Virtual Hub Name \* ⓘ

CNGFW-Demo-VWAN-Hub01

## Public IP Address Configuration

Public IP Address(es) \* ⓘ

- Create new  
 Use existing

Public IP Address Name(s) \* ⓘ

frontendip

## Additional Prefixes To Private Traffic Range

Additional Prefixes ⓘ

## Source NAT Settings

Enable Source NAT ⓘ

Use the above Public IP Address(es)

Previous

Next

Review + create

**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.

Leave Security Policies settings to default values and click on “**Next**” to proceed further.

[Home](#) > [Cloud NGFWs by Palo Alto Networks](#) >

## Create Cloud NGFW by Palo Alto Networks ...

Basics   Networking   Security Policies   DNS Proxy   Tags   Terms   Review + create

Managed by \* ⓘ

Azure Rulestack  
 Palo Alto Networks Panorama

Choose a Local Rulestack \* ⓘ

Create new  
 Use existing

Local Rulestack \*

CloudNGFW-Azure-VWAN-Demo-Irs

Firewall rules \* ⓘ

Allow all (Enables all security services using best-practices profile to inspect traffic)  
 Deny all

**i** 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.

Previous

Next

Review + create

- 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**”

[Home](#) > [Cloud NGFWs by Palo Alto Networks](#) >

## Create Cloud NGFW by Palo Alto Networks ...

[Basics](#) [Networking](#) [Security Policies](#) [DNS Proxy](#) [Tags](#) [Terms](#) [Review + create](#)

DNS Proxy \* ⓘ

Disabled  
 Enabled

---

[Previous](#) [Next](#) [Review + create](#)

- 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**”

## Create Cloud NGFW by Palo Alto Networks ...

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 <input type="button" value="v"/>

---

- Accept the terms  
Click on check-box to agree for the terms and conditions as shown below and click on “**Next**” to proceed further

## Create Cloud NGFW by Palo Alto Networks ...

[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](#). The [Palo Alto Networks service level agreement](#) applies to the offering.

I Agree \*

[Previous](#)

[Next](#)

[Review + create](#)

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

# Create Cloud NGFW by Palo Alto Networks ...

Basics   Networking   Security Policies   DNS Proxy   Tags   Terms   Review + create

[View automation template](#)

## Basics

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

## Networking

Type	Virtual Wan Hub
Virtual Hub Name	CNGFW-Demo-VWAN-Hub01
Public IP Address(es)	Use existing
Public IP Address Name(s)	frontendip

## Security Policies

Managed by	Azure Rulestack
------------	-----------------

[Previous](#)   [Next](#)   **Create**

- You will be presented with below screen where you the deployment is in progress and we can see the Cloud NGFW resources being created

Home >

### CreateFirewallForm-20231214145212 | Overview

Deployment

Search   Delete   Cancel   Redeploy   Download   Refresh

- Overview
- Inputs
- Outputs
- Template

**Deployment is in progress**

Deployment name : CreateFirewallForm-20231214145212   Start time : 12/14/2023, 2:55:45 PM  
Subscription : AzureTME   Correlation ID : 4574ccb7-abf1-4c03-a42d-add38f7be866  
Resource group : CloudNGFW-Azure-Demo-Lab

Deployment details

Resource	Type	Status	Operation details
CloudNGFW-Azure-VWAN-Demo-Irs	Local Rulestack for Cloud NGFW	Created	<a href="#">Operation details</a>
CloudNGFW-Azure-VWAN-Demo-nva	Microsoft.Network network virtu.	Created	<a href="#">Operation details</a>

## Activity 2: Review Cloud NGFW deployment status

Let us now review the deployment status of Cloud NGFW.

On successful deployment of the service you will be presented with below screen

Home > CreateFirewallForm-20231214145212 | Overview

Deployment

Search << Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

**✓ Your deployment is complete**

Deployment name : CreateFirewallForm-20231214145212  
Subscription : AzureTME  
Resource group : CloudNGFW-Azure-Demo-Lab

Start time : 12/14/2023, 2:55:45 PM  
Correlation ID : 4574ccb7-abf1-4c03-a42d-add38f7be866

> Deployment details

∨ Next steps

**Go to resource group**

- Click on **“Go to resource group”** to review Cloud NGFW and its resources
- Within the resource group, click on **“CloudNGFW-Azure-VWAN-Demo”** resource as shown below

Home > CreateFirewallForm-20231214145212 | Overview

CloudNGFW-Azure-Demo-Lab

Resource group

Search << 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

Settings

Deployments

Security

Deployment stacks

Policies

Properties

Locks

Cost Management

Essentials

Resources Recommendations

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

Showing 1 to 16 of 16 records. Show hidden types No grouping

Name ↑↓	Type ↑↓	Location ↑↓
<b>CloudNGFW-Azure-VWAN-Demo</b>	Cloud NGFW by Palo Alto Networks	East US
CloudNGFW-Azure-VWAN-Demo-Irs	Local Rulestack for Cloud NGFW by Palo Alto Net...	East US
CloudNGFW-Logs	Log Analytics workspace	East US
CNGFW-Demo-VWAN	Virtual WAN	East US
database-vm	Virtual machine	East US
database-vm-nic0	Network interface	East US
database-vm_OSDisk	Disk	East US
dbserverpip	Public IP address	East US

- You should see that Cloud NGFW service was created successfully with Health status as **“Healthy”**, Provisioning state as **“Succeeded”** and Network type as **“VWAN”**.

Home > CreateFirewallForm-20231214145212 | Overview > CloudNGFW-Azure-Demo-Lab >

## CloudNGFW-Azure-VWAN-Demo

Cloud NGFW by Palo Alto Networks

Search Refresh Delete

Overview

- Activity log
- Access control (IAM)
- Tags

Settings

- Networking & NAT
- Security Policies
- Log Settings
- DNS Proxy
- Rules
- Properties
- Locks

Support + troubleshooting

- New Support Request

Monitoring

- Alerts

Automation

- Tasks (manual)

Resource group (move) : CloudNGFW-Azure-Demo-Lab

Location : East US

Subscription (move) : AzureTME

Subscription ID : 0683d406-4d77-4bb7-b1a6-165c282b5d37

Tags (edit) : StoreStatus : DND InstanceLife : 60 office : India userID : rpegada

See more

Get started Properties Recommendations

**Cloud NGFW**

Identity ---

System data View value as JSON

**Properties**

Front end settings ---

Provisioning state Succeeded

**Networking & NAT**

Network type VWAN

V WAN configuration View value as JSON

Resource id : /subscriptions/0683d406-4d77-4bb7-b1a6-165c282b5d37

Health Status Healthy

Type : paloaltonetworks.cloudngfw/firewalls

Public IPs : 4.156.189.70

Private IPs : 10.210.0.228

**DNS Proxy**

Enable DNS proxy DISABLED

Enabled DNS type CUSTOM

DNS servers ---

**Plan data**

Usage type PAYG

Billing cycle MONTHLY

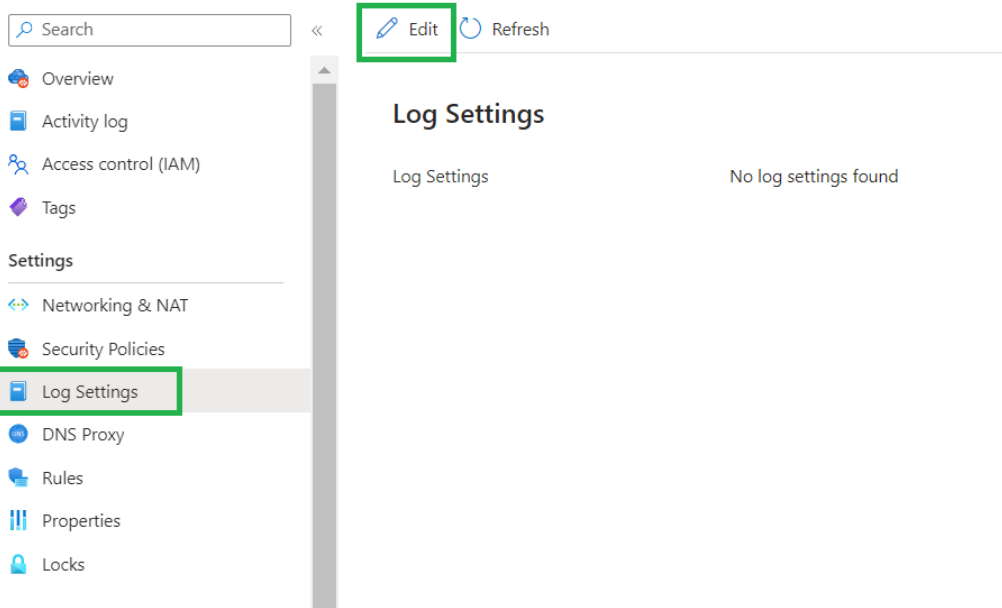
Plan id panw-cloud-ngfw-payg

Effective date 1/1/1, 5:53:28 AM

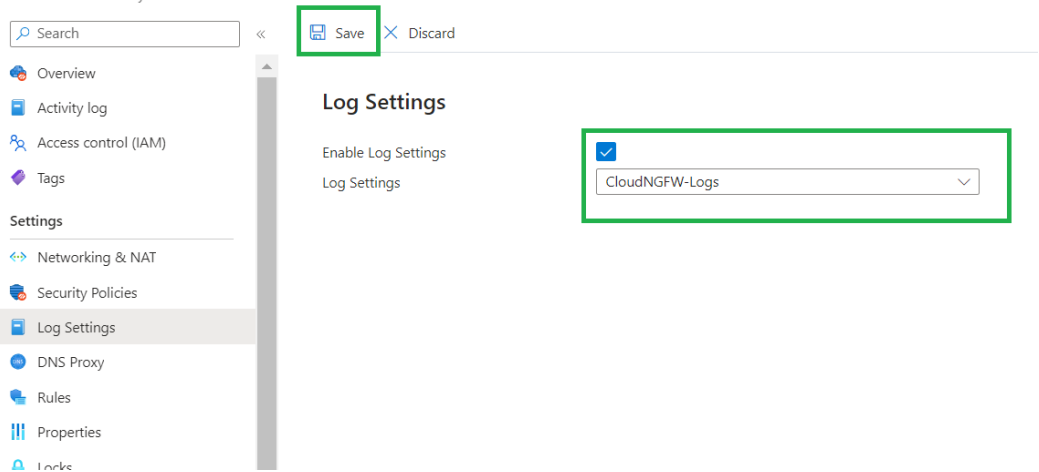
## Activity 3: Create Cloud NGFW Service

### 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

Home > CloudNGFW-Azure-Demo-Lab > CloudNGFW-Azure-VWAN-Demo

CloudNGFW-Azure-VWAN-Demo | Networking & NAT ☆ ...

Cloud NGFW by Palo Alto Networks

Search << Edit Refresh

Overview  
Activity log  
Access control (IAM)  
Tags

Settings

Networking & NAT

Security Policies  
Log Settings  
DNS Proxy  
Rules  
Properties  
Locks

Support + troubleshooting

New Support Request

Monitoring

### Networking

Type

Virtual Network

Virtual WAN Hub

Virtual Hub

CNGFW-Demo-VWAN-Hub01

NVA Id

CloudNGFW-Azure-VWAN-Demo-nva

### Source Network Address Translation (SNAT)

Public IP Addresses 20,241,255,169

Enable Source NAT

Use the above Public IP addresses

- 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



Search << Save Discard

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
  - Networking & NAT**
  - Security Policies
  - Log Settings
  - DNS Proxy
  - Rules
  - Properties
  - Locks
- Support + troubleshooting
  - New Support Request
- Monitoring
  - Alerts

### Source Network Address Translation (SNAT)

Public IP Addresses: frontendip

Enable Source NAT

Use the above Public IP addresses

### Destination Network Address Translation (DNAT)

Search

+ Add Delete

Name	Protocol	Frontend IP	Frontend Port	Backend IP	Backend Port
No data is available					

- 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 \*

SSHAccessToWeb

Protocol \*

TCP

UDP

Frontend IP \*

frontendip

Frontend Port \*

221

Backend IP \*

10.5.0.5

Backend Port \*

22

Add

Cancel

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

Home > CloudNGFW-Azure-Demo-Lab > CloudNGFW-Azure-VWAN-Demo

CloudNGFW-Azure-VWAN-Demo | Networking & NAT ☆ ...

Cloud NGFW by Palo Alto Networks

Search << Save Discard

Overview  
Activity log  
Access control (IAM)  
Tags

Settings

Networking & NAT  
Security Policies  
Log Settings  
DNS Proxy  
Rules  
Properties  
Locks

Support + troubleshooting  
New Support Request

Monitoring  
Alerts

### Source Network Address Translation (SNAT)

Public IP Addresses: frontendip

Enable Source NAT

Use the above Public IP addresses

### Destination Network Address Translation (DNAT)

Search

+ Add Delete

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

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

Home > CloudNGFW-Azure-Demo-Lab > CloudNGFW-Azure-VWAN-Demo

CloudNGFW-Azure-VWAN-Demo | Networking & NAT ☆ ...

Cloud NGFW by Palo Alto Networks

Search << Save Discard

Overview  
Activity log  
Access control (IAM)  
Tags

Settings

Networking & NAT  
Security Policies  
Log Settings

### Networking

Saving...

- 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
SSHAccessToWeb	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.

Home > CloudNGFW-Azure-Demo-Lab > CloudNGFW-Azure-VWAN-Demo

CloudNGFW-Azure-VWAN-Demo | Rules ☆ ...

Cloud NGFW by Palo Alto Networks

Search Refresh

Search

Priority	Name	Source	Destination	Constraints	Action	Logging	Egress Decry..
1000000	cloud-ngfw-default-rule	any	any	Default	Allow	yes	Disabled

Local Rules (1)

Rules

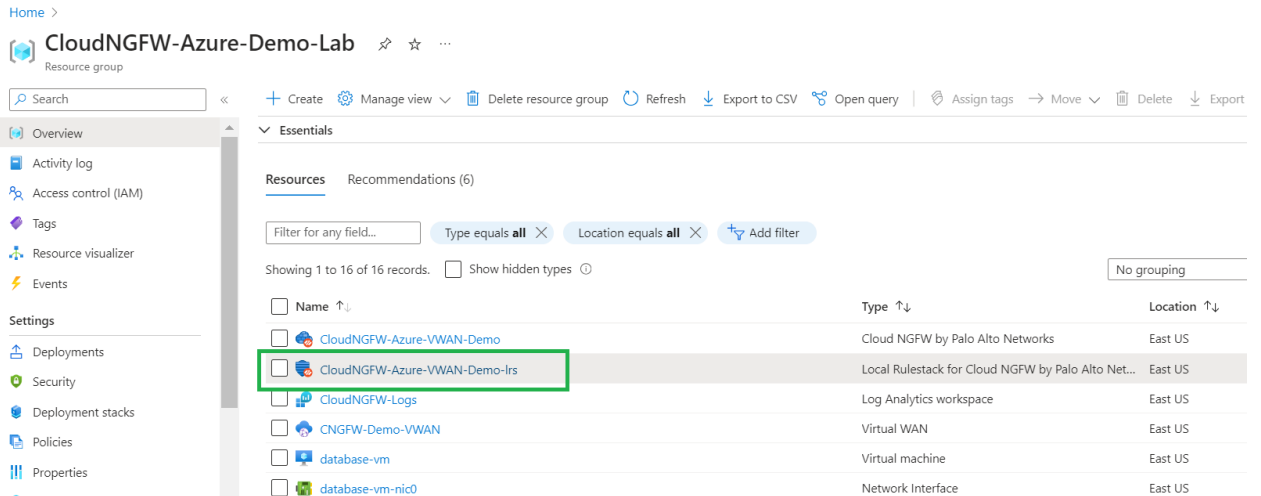
### Task 4 - Configure Firewall Policies using Local Rulestack

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

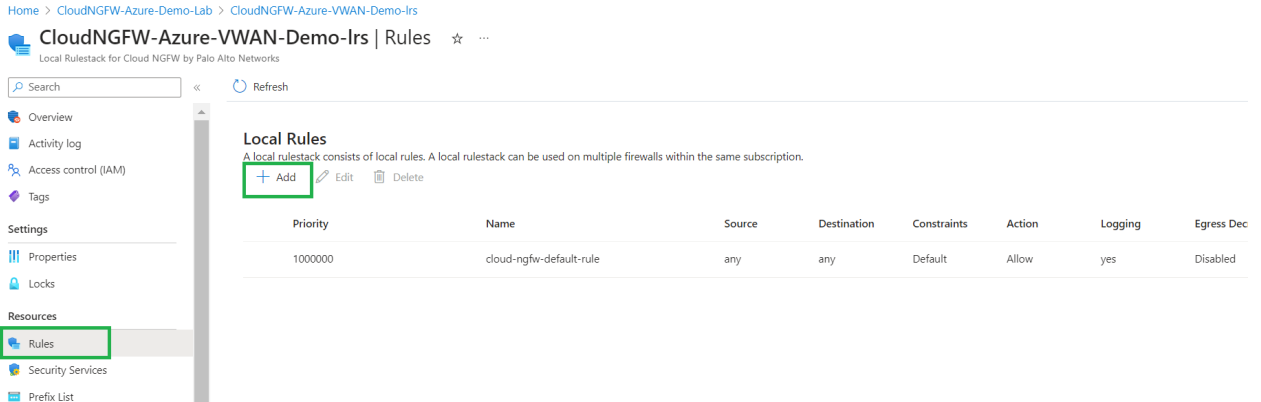
- Add rule to allow Mysql from web to db servers
- Add a rule to block Social networking category

#### Add rule to allow Mysql from web to db servers

- Go to your resource group and right-click on “**CloudNGFW-Demo-Irs**” 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(BlockMySQLFromWebToDB), priority, Source(Web) and destination(DB) subnet match as per the deployment topology. From Application match criteria, select “mysql” application from the dropdown(you will be able to search the application) with action as **allow** and **enable logging** as shown below.

# Add Rule

Define Rule Parameters

## General

Name \*

AllowMySQLFromWebtoDB

Description

Priority \*

500

Enabled



## Source

Match Criteria

Any

Match

IP Address (CIDR Format)

10.5.0.0/24

Countries

Prefix List

Exclude



## Destination

Match Criteria

Any

Match

IP Address (CIDR Format)

10.6.0.0/24

Countries	<input type="text"/>
Prefix List	<input type="text" value=""/>
FQDN List	<input type="text" value=""/>
Destination Exclude	<input type="checkbox"/>
<b>Granular Controls</b>	
Application	
Match Criteria	<input type="radio"/> Any
	<input checked="" type="radio"/> Select
Applications	<input type="text" value="mysql"/>
URL Category	
Match Criteria	<input checked="" type="radio"/> Any
	<input type="radio"/> Select
Protocol & Port	
Match Criteria	<input type="radio"/> Application Default
	<input checked="" type="radio"/> Any
	<input type="radio"/> Select
<b>Actions</b>	
Actions	<input checked="" type="radio"/> Allow
	<input type="radio"/> Drop
	<input type="radio"/> Reset Server
	<input type="radio"/> Reset Both
Egress Decryption ⓘ	<input type="checkbox"/>
Logging	<input checked="" type="checkbox"/>

---

<input checked="" type="button" value="Save"/>	<input type="button" value="Cancel"/>
--	---------------------------------------

### Add rule to block Social Networking

Within the Rules page, click on “Add” to add a new rule.

Provide the Name(BlockSocialNetworking), select the URL Category as ‘social-networking’, action as **drop** and enable logging as shown below.



Click on **Validate** and then **Save** 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

social-networking

Categories \*  
Protocol & Port  
Match Criteria

Application Default

Any

Select

Actions

Actions

Allow

Drop

Reset Server

Reset Both

Egress Decryption

Logging

Newly added policies would look as shown below

CloudNGFW-Azure-VWAN-Demo-Irs | 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  
Prefix List

**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 D
400	BlockSocialNetworking	any	any	Custom	Drop	yes	Disabled
500	AllowMySQLFromWebtoDB	match	match	Custom	Allow	yes	Disabled
1000000	cloud-ngfw-default-rule	any	any	Default	Allow	yes	Disabled

## Deploy configuration

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

CloudNGFW-Azure-VWAN-Demo-Irs | 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	<b>Pending Deployment:</b> LocalRule, Rulestack	<b>Deploy Configuration</b> Revert

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

## Deploy ×

Push your configured rulestacks to your firewalls.

**The following firewall(s) will be deployed with the changes made to the rulestack.**

CloudNGFW-Azure-VWAN-Demo(CloudNGFW-Azure-Demo-Lab)

**Deploy** Cancel

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

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 : Configure Routing Intent on Azure VWAN Hub

Routing Intent simplifies routing and configuration by managing route associations and propagations of all connections in a hub

### Activity 1: Configure Routing Intent.

Open Azure Virtual WAN within your resource group

CloudNGFW-Azure-Demo-Lab ☆ ...

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

Essentials  
Subscription (move) : AzureTME  
Subscription ID : 0683d406-4d77-4bb7-b1a6-165c282b5d37  
Deployments : 2 Succeeded  
Location : East US  
Tags (edit) : Add tags

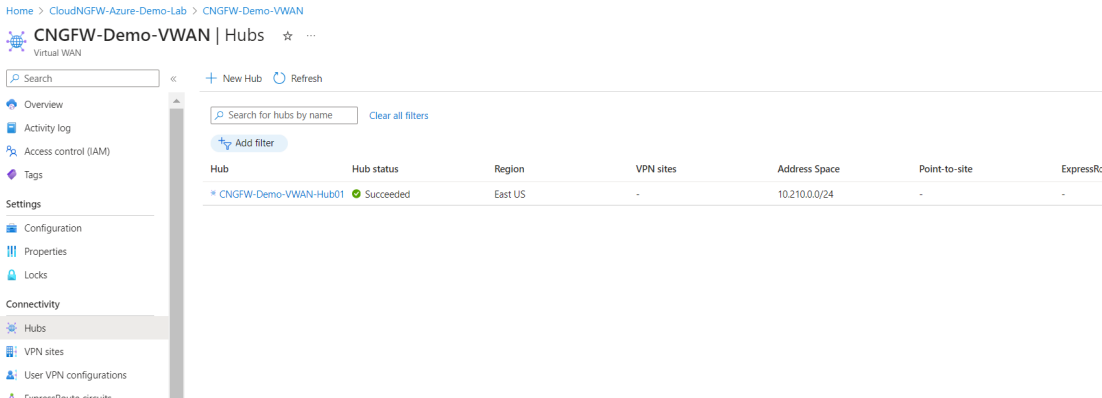
Resources Recommendations (6)

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

Showing 1 to 16 of 16 records. Show hidden types No grouping List view

Name	Type	Location
CloudNGFW-Azure-VWAN-Demo	Cloud NGFW by Palo Alto Networks	East US
CloudNGFW-Azure-VWAN-Demo-Irs	Local Rulestack for Cloud NGFW by Palo Alto Networks	East US
CloudNGFW-Logs	Log Analytics workspace	East US
CNGFW-Demo-VWAN	Virtual WAN	East US
database-vm	Virtual machine	East US
database-vm-nic0	Network Interface	East US

Go to Hubs within the virtual wan selected.

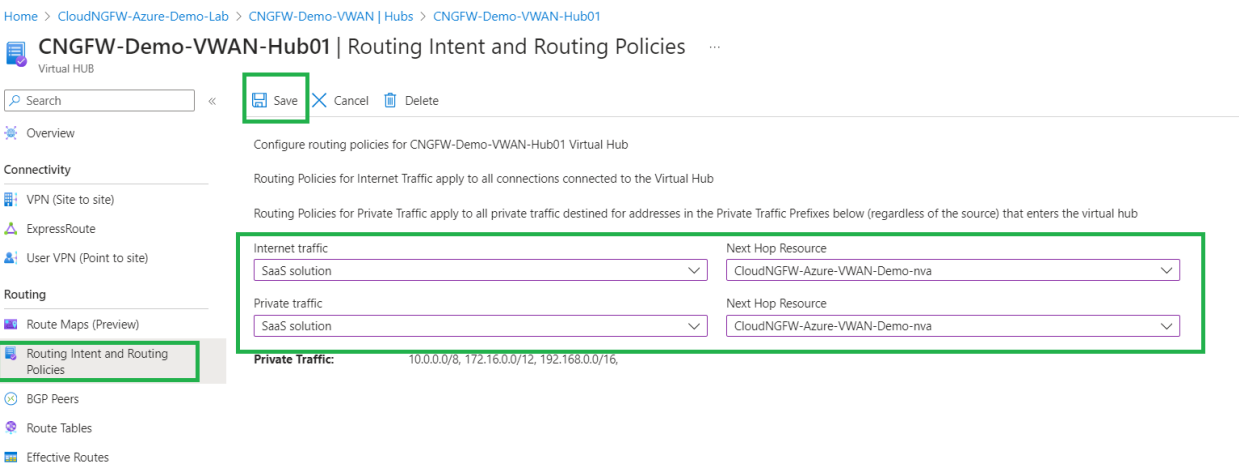


Configure Routing Intent as shown below.

Select “**SaaS solution**” from the drop down of **Internet traffic** and Next Hop Resource as Cloud NGFW service created, in order to secure Internet inbound and outbound traffic using Cloud NGFW

Similarly to secure private traffic(Spoke to Spoke and Spoke to On-prem) select “**SaaS solution**” from the drop down of **Private traffic** and Next Hop Resource as Cloud NGFW service created

Click on **Save** to save the configuration



## Part-4 : 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**”. You can also go to your “Resource Group > Deployments” and select Microsoft.Template.XXXXX deployment.

Home > CloudNGFW-Azure-Demo-Lab

## CloudNGFW-Azure-Demo-Lab | Deployments

Resource group

Search

Refresh Cancel Redeploy Delete View template

- Overview
- Activity log
- Access control (IAM)
- Tags
- Resource visualizer
- Events
- Settings
  - Deployments
  - Security
  - Deployment stacks
  - Policies

Filter by deployment name or resources in the deployment...

<input type="checkbox"/>	Deployment name	Status
<input type="checkbox"/>	CreateFirewallForm-20231214145212	✔ Succeeded
<input checked="" type="checkbox"/>	Microsoft.Template-20231214135509	✔ Succeeded

Home > CloudNGFW-Azure-Demo-Lab | Deployments > Microsoft.Template-20231214135509

### Microsoft.Template-20231214135509 | Outputs

Deployment

Search

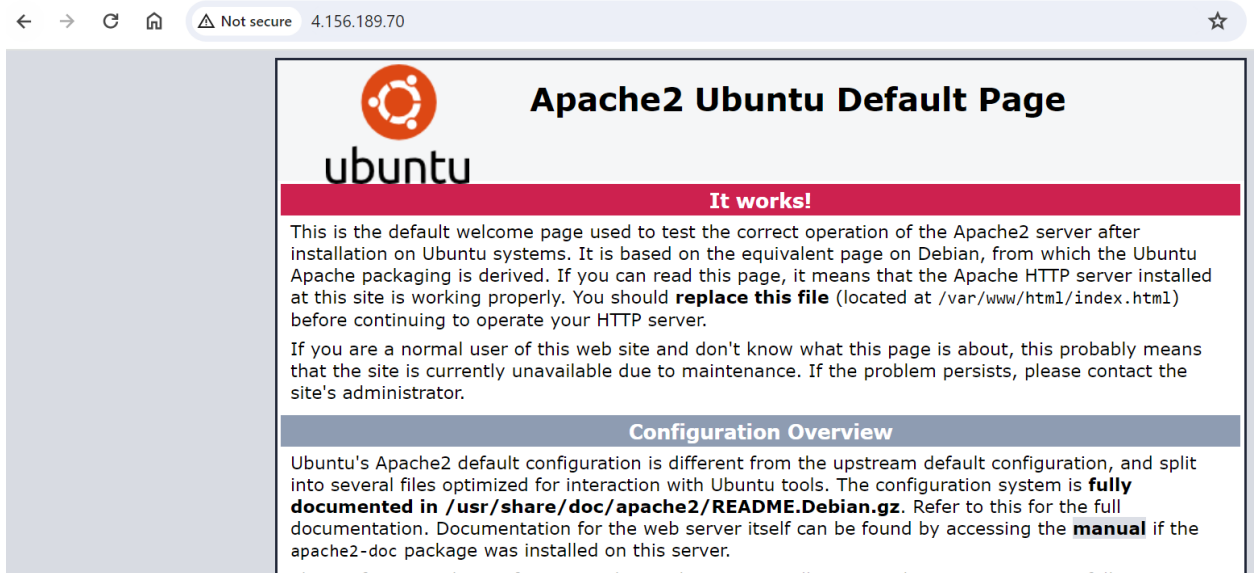
- Overview
- Inputs
- Outputs
- Template

web-server-url	<a href="http://4.156.189.70">http://4.156.189.70</a>
web-server-url-wordpress	<a href="http://4.156.189.70/wordpress">http://4.156.189.70/wordpress</a>
web-server-url-sql-attack	<a href="http://4.156.189.70/sql-attack.html">http://4.156.189.70/sql-attack.html</a>
ssh-web-vm	<a href="ssh://palalto@4.156.189.70-p-221">ssh://palalto@4.156.189.70-p-221</a>
username	palalto
password	Pal0Alt0@123
frontend-ip	4.156.189.70

From within this output, copy the web-server-url as shown below.

web-server-url	<a href="http://4.156.189.70">http://4.156.189.70</a>
web-server-url-wordpress	<a href="http://4.156.189.70/wordpress">http://4.156.189.70/wordpress</a>
web-server-url-sql-attack	<a href="http://4.156.189.70/sql-attack.html">http://4.156.189.70/sql-attack.html</a>

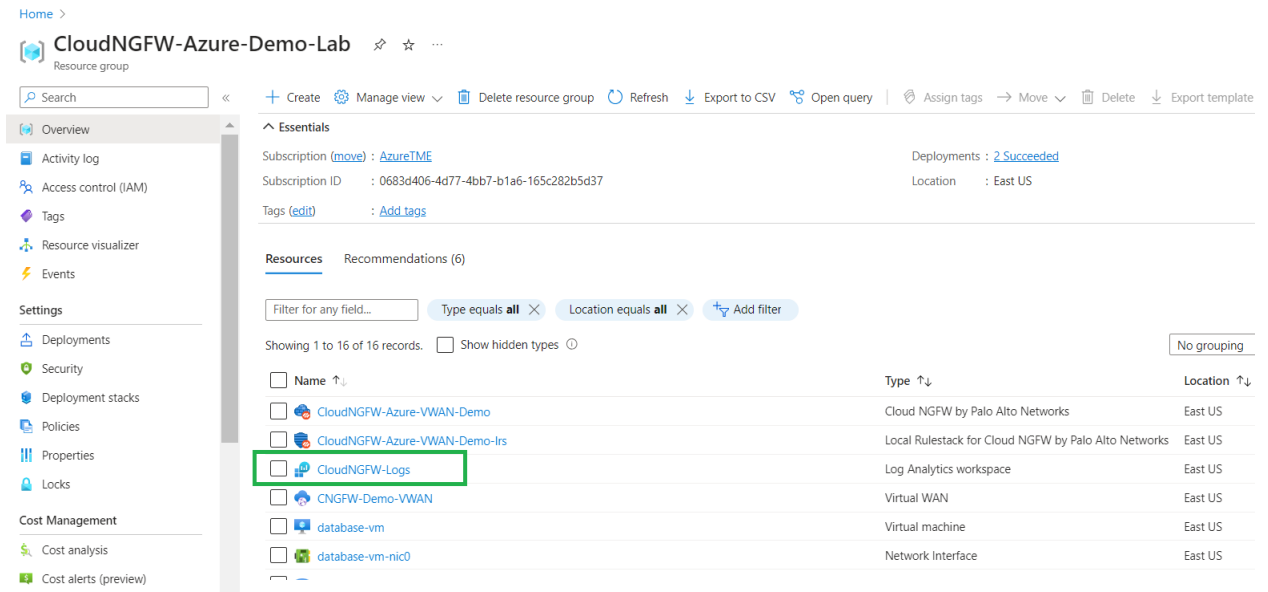
- Use the copied url and access the web server from your browser or from the browser within the student desktop. You should see the web page as shown below.



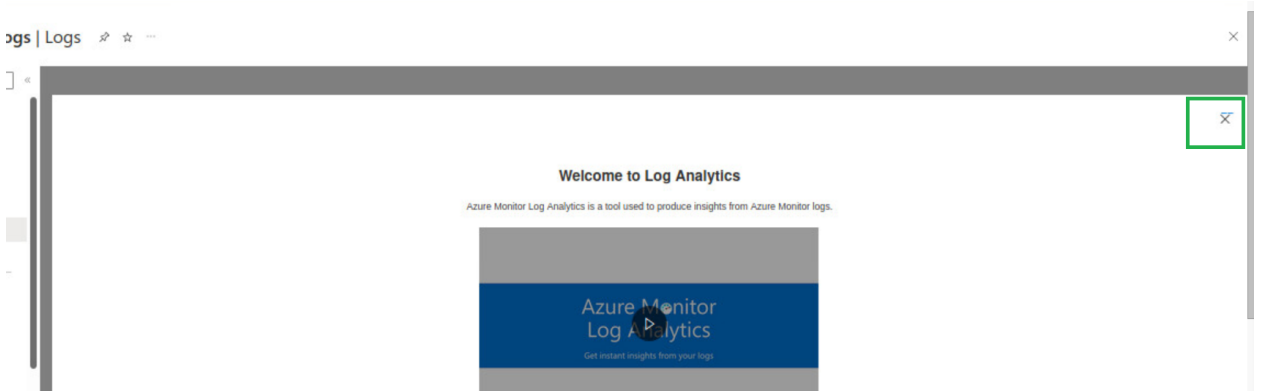
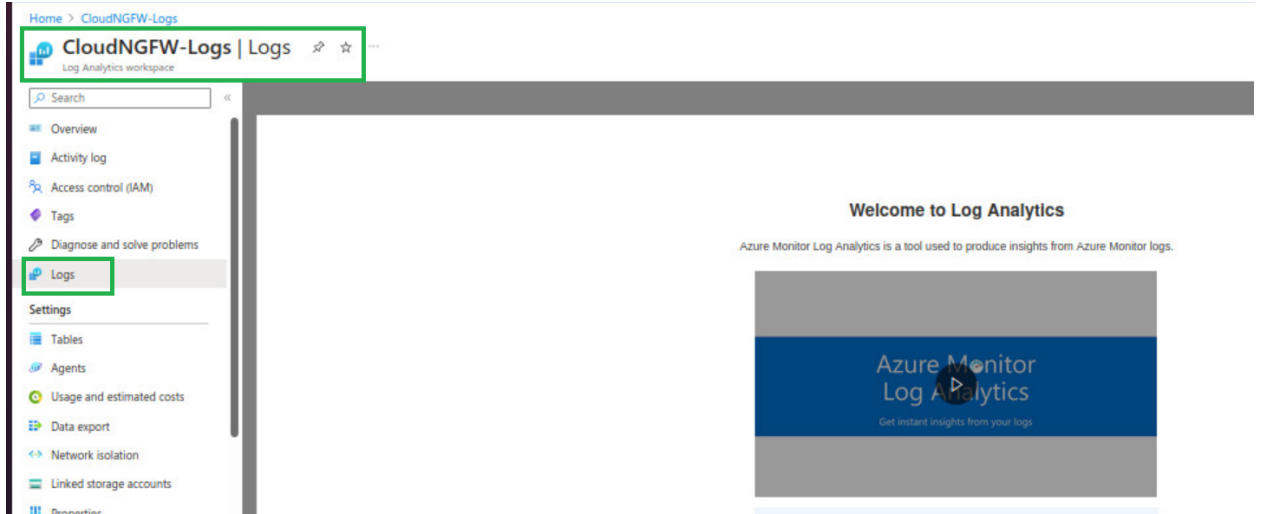
- This indicates that the web server is accessible from internet

## Task 2 - Verify Cloud NGFW logs using Log Analytics workspace

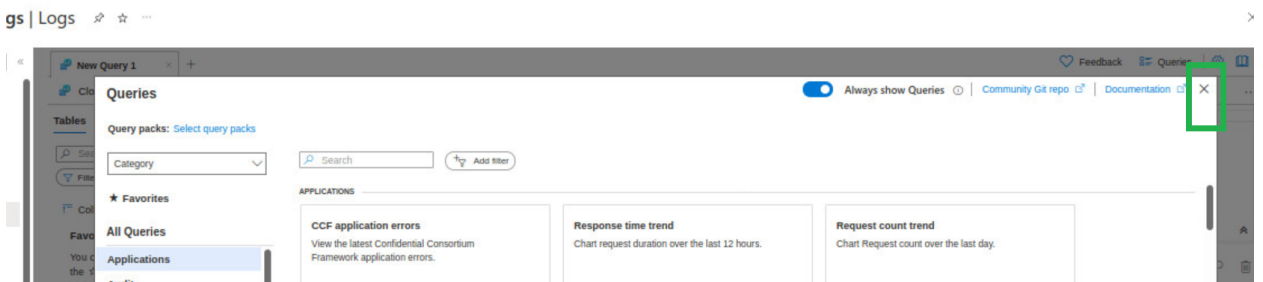
- Click on “CloudNGFW-Logs” to open Log Analytics Workspace by going to the resource group as shown below.



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

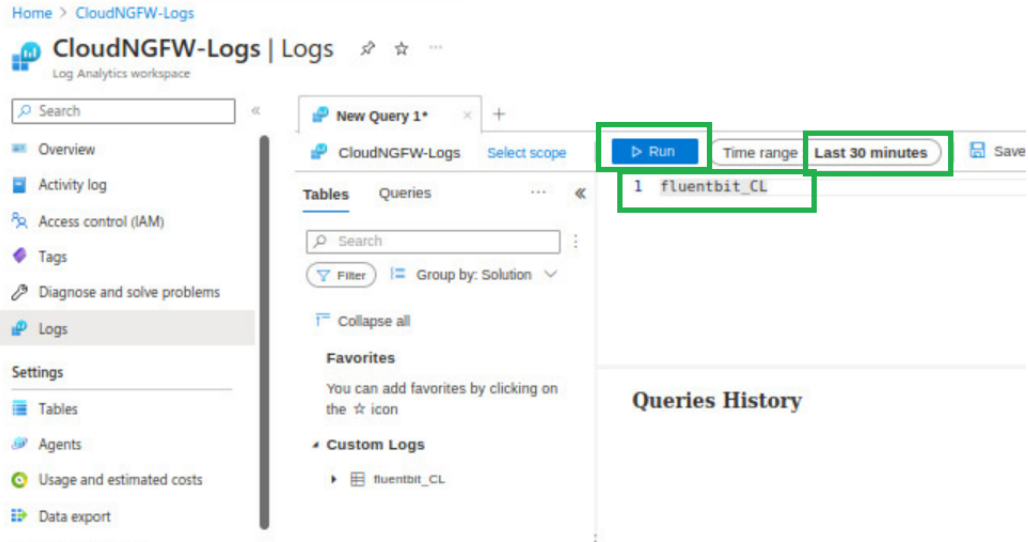


- Close the Queries page as shown below

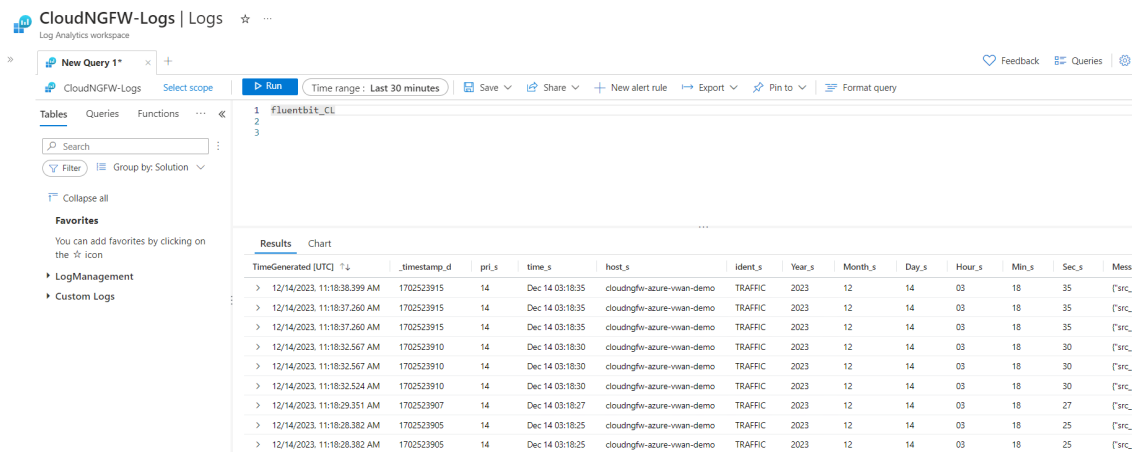


- After going to Log Analytics workspace(CloungFW-Logs), navigate to **Logs** on the left menu
- In order to view Cloud NGFW logs we will be using custom query “**fluentbit\_CL**”
- Select **Local Time** from the **Display time** at the left bottom of the page to view the logs in your local time.
- Select 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.



Change the display time to "Local Time" as shown below



## What's my IP ⋮

134.238.236.250

Your public IP address

→ [Learn more about IP addresses](#)

- 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.

The screenshot shows the CloudNGFW-Logs interface. The main area displays a list of log messages with columns for TimeGenerated and Message. Several messages are highlighted with a green box, showing source IP addresses like 134.238.236.250 and 10.6.0.5. Below the main interface, a detailed view of log messages is shown, with the same IP addresses highlighted in green boxes.

TimeGenerated [Local Time]	Message
12/14/2023, 4:44:44.204 PM	["src_ip":"134.238.236.250", "sport":"40383", "dst_ip":"4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"allow", "bytes_recv":"12039", "bytes_sent":...
12/14/2023, 4:44:43.119 PM	["src_ip":"65.154.226.167", "sport":"30740", "dst_ip":"4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"allow", "bytes_recv":"11141", "bytes_sent":...
12/14/2023, 4:44:33.803 PM	["src_ip":"10.5.0.5", "sport":"53786", "dst_ip":"20.42.73.216", "dport":"443", "proto":"tcp", "app":"azure-log-analytics", "rule":"cloud-ngfw-default-rule", "action":"allow", "bytes_recv":"5110", "bytes_sent":3...
12/14/2023, 4:44:33.075 PM	["src_ip":"10.6.0.5", "sport":"39676", "dst_ip":"40.71.12.254", "dport":"443", "proto":"tcp", "app":"azure-log-analytics", "rule":"cloud-ngfw-default-rule", "action":"allow", "bytes_recv":"5110", "bytes_sent":3...
12/14/2023, 4:44:29.083 PM	["src_ip":"134.238.236.250", "sport":"40383", "dst_ip":"4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"alert", "url_idx":"3", "url_category_list":"me...
12/14/2023, 4:44:28.401 PM	["src_ip":"65.154.226.167", "sport":"30740", "dst_ip":"4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"alert", "url_idx":"1", "url_category_list":"medi...
12/14/2023, 4:44:24.959 PM	["src_ip":"134.238.236.250", "sport":"40383", "dst_ip":"4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"alert", "url_idx":"1", "url_category_list":"me...
12/14/2023, 4:39:24.534 PM	["src_ip":"185.224.128.184", "sport":"535", "dst_ip":"4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"allow", "bytes_recv":"0", "bytes_sent":"103"]
12/14/2023, 4:39:19.207 PM	["src_ip":"185.224.128.184", "sport":"535", "dst_ip":"4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"block-url", "url_idx":"11", "url_category_list":"a...

12/14/2023, 4:44:33.075 PM	["src_ip":"10.6.0.5", "sport":"39676", "dst_ip":"40.71.12.254", "dport":"443", "proto":"tcp", "app":"azure-log-analytics", "rule":"cloud-ngfw-default-rule", "action":"allow", "bytes_recv":"5110", "bytes_sent":"3...
12/14/2023, 4:44:29.083 PM	["src_ip":"134.238.236.250", "sport":"40383", "dst_ip":"4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"alert", "url_idx":"3", "url_category_list":"me...
12/14/2023, 4:44:28.401 PM	["src_ip":"65.154.226.167", "sport":"30740", "dst_ip":"4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"alert", "url_idx":"1", "url_category_list":"medi...
12/14/2023, 4:44:24.959 PM	["src_ip":"134.238.236.250", "sport":"40383", "dst_ip":"4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"alert", "url_idx":"1", "url_category_list":"me...

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

## Activity 2: 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 rule stack as shown below

The screenshot shows the Palo Alto Networks Security Services configuration page. The breadcrumb navigation is: Home > CloudNGFW-Azure-Demo-Lab > CloudNGFW-Azure-VWAN-Demo-Irs. The page title is "CloudNGFW-Azure-VWAN-Demo-Irs | Security Services" with a star icon and a refresh button. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Settings (Properties, Locks), Resources (Rules, Security Services, Prefix List, FQDN List, Certificates, Deployment, Managed Identity), Support + troubleshooting (New Support Request), Monitoring (Alerts), and Automation. The "Security Services" option is highlighted with a green box. The main content area features a warning message: "To use Palo Alto Networks Advanced Cloud-Delivered Security Services (such as Advanced Threat Prevention, Advanced URL Filtering, Wildfire, and...) Without registering your Azure Tenant, only the standard Cloud-Delivered Security Services (such as Threat Prevention, and URL Filtering) will be o... Learn more about various Security Services Best Practice profiles." Below this, several security services are listed with their status and profile:

- Advanced Threat Prevention**: Enabled (checked), Profile: Best Practice
- Vulnerability Protection Profiles**: An Intrusion Prevention System (IPS) is a network security and threat prevention technology that examines traffic flow to detect and prevent v... Enable: checked, Profile: Best Practice
- Anti-Spyware Profiles**: Anti-spyware protection zeroes in on outbound threats, especially command-and-control (C2) activity, where an infected client is being leverage... Enable: unchecked, Profile: Best Practice
- Antivirus Profiles**: Antivirus protects against viruses, worms, and trojans as well as spyware downloads. Enable: checked, Profile: Best Practice
- File Blocking Profiles**: Use file blocking to prevent the transmission of specific file types sent over your network.

### Task 1 - Access Sql attack URL

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

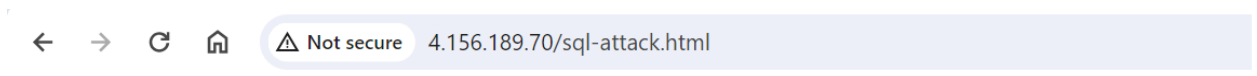
The screenshot shows the ARM Template deployment outputs page. The breadcrumb navigation is: Home > CloudNGFW-Azure-Demo-Lab > Deployments > Microsoft.Template-20231214135509. The page title is "Microsoft.Template-20231214135509 | Outputs". The left sidebar contains navigation options: Overview, Inputs, Outputs, and Template. The "Outputs" option is highlighted with a green box. The main content area displays a list of outputs:

- web-server-url: http://4.156.189.70
- web-server-url-wordpress: http://4.156.189.70/wordpress
- web-server-url-sql-attack: http://4.156.189.70/sql-attack.html

The "web-server-url-sql-attack" output is highlighted with a green box, and its value is also highlighted with a green box.

## Task 2 - Launch Brute Force attack on DB Server

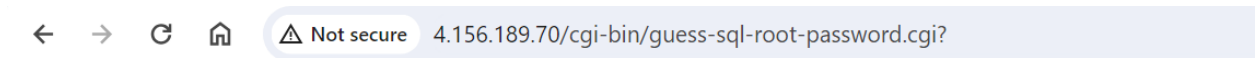
- Click on “LAUNCH BRUTE FORCE SQL ROOT PASSWORD GUESSING” to initiate brute force attack from web server to DB server



### Attack the database

**LAUNCH BRUTE FORCE SQL ROOT PASSWORD GUESSING**

- You will be presented with below mentioned screen



**Brute force MySQL root password attempt launched.**

**RETURN TO ATTACK LAUNCH PAGE**

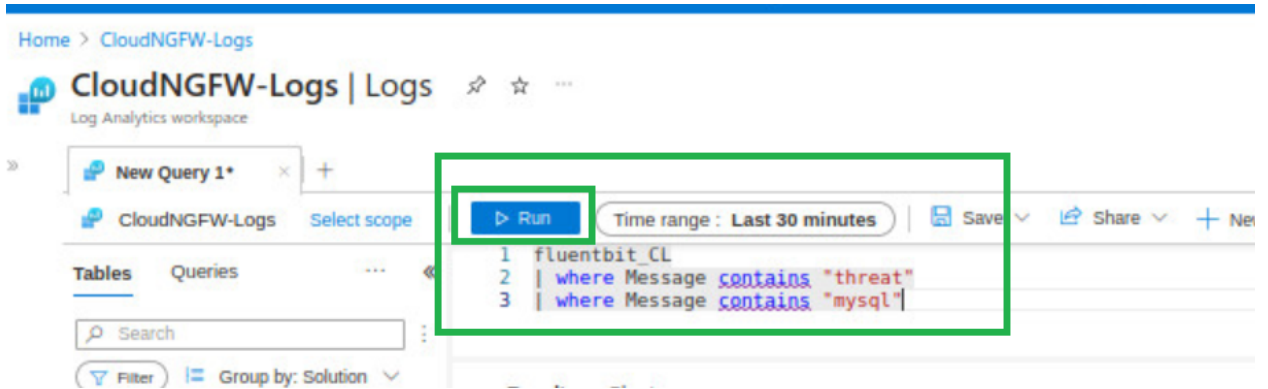
## Task 3 - Verify THREAT logs on Log Analytics workspace

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

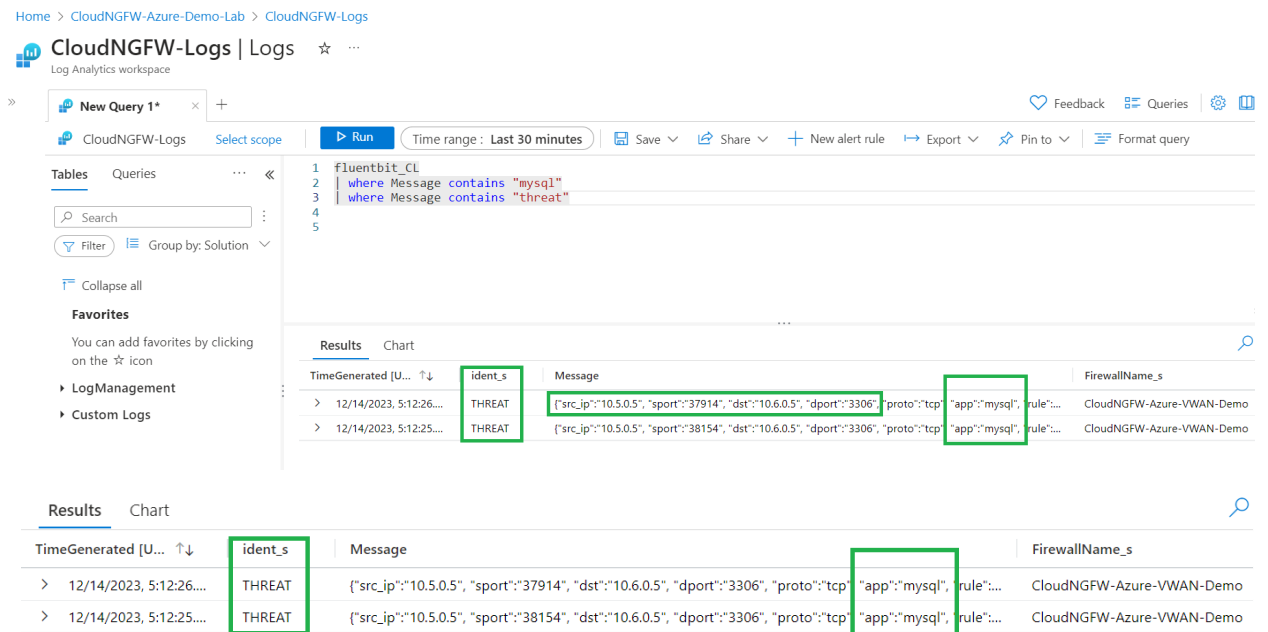
*fluentbit\_CL*

*| 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 3: Validate secure outbound internet access through Cloud NGFW

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

web-server-url

web-server-url-wordpress

web-server-url-sql-attack

ssh-web-vm

username

password

- Use the SSH command copied along with the password as shown in above screenshot and login to the Web server terminal
- If you using VPN on your laptop, it might prevent SSH to the webserver-vm. Please disconnect VPN and then try to connect to web server using SSH
- 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

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_re...
> 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_re...
> 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":"ssl", "rule":"cloud-nfw-default-rule", "action":"allow", "bytes_recv":"11999...
> 5/31/2023, 2:55:51.964 PM	TRAFFIC	["src_ip":"10.5.0.5", "sport":"56758", "dst_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_recv":"548", "bytes_sent":"344", "pkts_received":"3", "pkts_sent":"3", "start_time":"2023/05/31 02:27:13", "elapsed_time":"0", "repeat_count":"1", "category":"social-networking", "src_country":"10.0.0-10.255.255.255", "dst_country":"United States", "session_end_reason":"policy-deny", "xff_ip":""]
> 5/31/2023, 2:55:51.947 PM	DECRYPTION	["src_ip":"10.5.0.5", "sport":"56758", "dst_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_recv":"548", "bytes_sent":"344", "pkts_received":"3", "pkts_sent":"3", "start_time":"2023/05/31 02:27:13", "elapsed_time":"0", "repeat_count":"1", "category":"social-networking", "src_country":"10.0.0-10.255.255.255", "dst_country":"United States", "session_end_reason":"policy-deny", "xff_ip":""]
> 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":"unknown-tcp", "rule":"cloud-nfw-default-rule", "action":"allow", "byte...
> 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":"unknown-tcp", "rule":"cloud-nfw-default-rule", "action":"allow", "byte...

END of LAB