



## **Cloud NGFW Azure VWAN Lab Guide**

Date: Dec, 2023 Authors: Ravisankar Pegada

## **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 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.

÷	→ C @ .	portal.azur	e.com/#home	e						C e		Ď   □
=	Microsoft Azure	₽ Search re	sources, services	s, and docs (G+/)						₽ Q @	ଡ ନ ୍ମ	pegada@paloalto alo alto networks ii
	Az	ure services										
		+			[]	2	+				$\rightarrow$	
		Create a resource	Deploy a custom	Template specs	Resource groups	Users	Subscriptions	Marketplace	Log Analytics workspaces	Cloud NGFWs by Palo Alto	More services	



### **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 <u>Cloud NGFW for Azure VWAN Lab ARM Template</u>

= 🔘 ravipegada / CloudNGFW-Azu	e-VWAN-Lab	o search	
<> Code 📀 Issues 🕅 Pull requests	🕑 Actions 🗄 Projects 🕮 Wiki 🕛 Se	curity 🗠 Insights 🕸 Setti	ngs
<li>Files</li>	CloudNGFW-Azure-VWAN-Lab / CloudN	GFW-Azure-VWAN-Lab.json	<i>с</i>
<u>₿</u> main • + Q	😨 ravipegada Add files via upload		d951515 · 11 minutes ago 🛛 History
Q Go to file t			
CloudNGFW-Azure-VWAN-Lab.js	Code Blame 569 lines (545 loc) · 2	2.3 KB	Raw 🗘 🗶 💌 👀
	1 {		
Documentation • Share feedback	2 "\$schema": "https://schema	.management.azure.com/schemas/20 "	15-01-01/deploymentTemplate.json#",
	4 "metadata": {	,	
	5 "comments": "Creating	Azure VWAN infrastructure with s	poke 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.

Microsoft Azure				×	D G
Azure servic	All Services (6) Azure Active Directory (0)	Marketplace (1)	Documentation (99+)	Resources (0)	Resource
Create a resource	Services	2	5 Depl	loyment Scripts	
Resources	Templates  Template specs		👰 Imag 👥 Azur	ge templates re Deployment Enviror	Iments

• Select Build your own template in the editor.



• Remove default template content by selecting all and clicking delete



• Paste the copied ARM template data and click on Save



• 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 mana	ge the lifecycle of your deployments. Try it now $  ightarrow $	
Select a template <b>Basics</b> Review	+ create	
Template		
Customized template 15 resources	Edit template Edit parameters Visualize	
Project details		
Select the subscription to manage deploy manage all your resources.	ed resources and costs. Use resource groups like folders to organize and	
Subscription * 🛈	AzureTME	/
Resource group * 🛈	CloudNGFW-Azure-Demo-Lab Create new	<u>~</u>
Instance details		
Region * 🤃	(US) East US	<u>~</u>

Region * 🗊	(US) East US	$\checkmark$
Ubuntu OS Version ①	18.04-LTS	$\sim$
Vm Size ①	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 <b>Review + create</b>					
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



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

Home >							
A Microsoft.Templar	te-202	31214	135509   Overview 🖈				
₽ Search	« 🧻 I	Delete (	🛇 Cancel 🚏 Redeploy 🛓 Downlo	ad 💍 Refresh			
👶 Overview		Denla	ovment is in progress	1			
🛓 Inputs		Depr	byment is in progress				
j≡ Outputs	<b>{\$</b> }	Deployn	nent name : Microsoft.Template-2023121	4135509	Start time : 12/	14/2023, 1:55:18 PM f6914_da0a_49c9_bfab_60a729	5022617
📄 Template		Resourc	e group : CloudNGFW-Azure-Demo-La	ab	conclution by . byc		1022017
	~	Deplo	yment details Resource	Туре		Status	Operation details
		Θ	database-vm/installcustomscript	🨝 Microsoft.Compute/virtu	alMachines/extensio	Created	Operation details
		Θ	webserver-vm/installcustomscript	🤿 Microsoft.Compute/virtu	alMachines/extensio	Created	Operation details
		0	database-vm	💶 Virtual machine		ОК	Operation details
		0	webserver-vm	📮 Virtual machine		ОК	Operation details
		0	database-vm-nic0	Retwork interface		Created	Operation details
		0	webserver-vm-nic0	📳 Network interface		Created	Operation details
		•	CNGFW-Demo-VWAN-Hub01	👾 Microsoft.Network/virtua	lHub	Created	Operation details

• Wait for the deployment to get completed

Microsoft.Template	e-20231214135509   Overview 🛷 …	
₽ Search «	📋 Delete 🚫 Cancel 🚏 Redeploy 🛓 Download 🖒 Refresh	
👶 Overview	Your deployment is complete	
Inputs	Deployment name : Microsoft.Template-20231214135509	Start time : 12/14/2023, 1:55:18 PM
i Outputs	Subscription : AzureTME	Correlation ID: b4cf6914-da0a-48c8-bfab-60a725e22617
iemplate	Resource group : Clouding-rw-Azure-Demo-Lab	
	> Deployment details	
	✓ Next steps	
	Go to resource group	

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

Home >			
A Micro	osoft.Template-202312	14135509   Overview 🛷 …	
🔎 Search	« 🗎 Delet	e 🛇 Cancel 👬 Redeploy 🛓 Download 💍 Refresh	
👶 Overview	🔗 You	ir deployment is complete	
😫 Inputs		ar deployment is complete	
×= 0.4.4.4	Dep	loyment name:Microsoft.Template-20231214135509	Start time : 12/14/2023, 1:55:18 PM
s Outputs		iption : AzureTME	Correlation ID: b4cf6914-da0a-48c8-bfab-60a725e22617
📄 Template	Open link in new tab	ce group : CloudNGFW-Azure-Demo-Lab	
	Open link in new window		
	Open link in incognito window	pyment details	
	open link in neoginto window	steps	
	Save link as	to resource group	
	Copy link address		
	Open in reading mode	c	

• 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.Tem	nplate-2023121	4135509	
Microsoft.Ten	nplate-2	0231214135509   Outputs	
🔎 Search	~		
👶 Overview		web-server-url http://4.156.189.70	Ð
🔄 Inputs			
š≡ Outputs		web-server-url-wordpress	
📄 Template		http://4.156.189.70/wordpress	D
		web-server-url-sql-attack	
		http://4.156.189.70/sql-attack.html	D
		ssh-web-vm	
		ssh paloalto@4.156.189.70 -p 221	Ð
		username	
		paloalto	Ð
		password	
		Pal0Alt0@123	Ð
		frontend-IP	
		4 156 189 70	<b>N</b>

• 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 Deployment	-20231214135509   Overview 🖈 …	
₽ Search «	📋 Delete 🚫 Cancel 🃫 Redeploy 👱 Download 🖒 Refresh	
👶 Overview	Your deployment is complete	
📮 Inputs		
š≡ Outputs	Deployment name : Microsoft.Template-20231214135509 Subscription : AzureTME	Start time : 12/14/2023, 1:55:18 PM Correlation ID : b4cf6914-da0a-48c8-bfab-60a725e22617
📄 Template	Resource group : CloudNGFW-Azure-Demo-Lab	
	> Deployment details	
	V Next steps	
	Go to resource group	

• You will see all the resources as shown below. Click on "Virtual WAN" resource created

Home > Microsoft.Template-2023121413	35509   Overview >		
CloudNGFW-Azure-	Demo-Lab 🖈 ☆ …		
₽ Search «	🕂 Create 🕲 Manage view 🗸 📋 Delete resource group 🖒 Refresh 🞍 Export to CSV 😤	Open query $\mid \ \oslash$ Assign tags $ ightarrow$ Move $ ightarrow$	🗸 🗓 Delete 🚽 Export template 🚺 Ope
() Overview	✓ Essentials		
Activity log	December December define		
Access control (IAM)	Resources Recommendations		
🔷 Tags	Filter for any field Type equals all X Location equals all X + Add filter		
🛧 Resource visualizer	Shawing 1 to 14 of 14 or and Shaw bidden turner		
🗲 Events	Showing I to 14 of 14 records.		No grouping V == List
Settings	Name 14	Туре ↑↓	Location $\uparrow\downarrow$
Settings	Name ↑↓ PloudNGFW-Logs	Type ↑↓ Log Analytics workspace	Location ↑↓ East US
Settings  Deployments  Security	Name ↑↓ Provide CoudNGFW-Logs CNGFW-Demo-VWAN	Type ↑↓ Log Analytics workspace Virtual WAN	Location 14 East US East US
Settings   Deployments  Security  Deployment stacks	Name ↑↓	Type ↑↓ Log Analytics workspace Virtual WAN Virtual machine	Location 14 East US East US East US
Settings    Deployments  Security  Deployment stacks  Policies	Name ↑↓	Type ↑↓ Log Analytics workspace Virtual WAN Virtual machine Network Interface	Location 14 East US East US East US East US
Settings    Deployments  Security  Deployment stacks  Policies  UP properties	Name ↑↓	Type ↑↓ Log Analytics workspace Virtual WAN Virtual machine Network Interface Disk	Location 14 East US East US East US East US East US
Settings  Deployments  Security  Deployment stacks  Policies  Properties Construction Constructi	Name ↑↓	Type ↑↓ Log Analytics workspace Virtual WAN Virtual machine Network Interface Disk Public IP address	Location 14 East US East US East US East US East US East US East US
Settings	Name ↑↓	Type ↑↓ Log Analytics workspace Virtual WAN Virtual machine Network Interface Disk Public IP address Public IP address	Location 14 East US East US East US East US East US East US East US East US

• Check for the status of Virtual WAN to be successful and click on "Hubs" as shown below

Overview     ▲     ► Essentials       ■     Activity log     Resource group : CloudN       %     Access control (IAM)     Location : East US       ✓     Taqs     Subscription : AzureTN	GEW-Azure-Demo-Lab	Status Branch-to-brand	: 🕑 Succeeded ch : Enabled
Activity log     Resource group : CloudN       Sp. Access control (IAM)     Location : East US       Subscription : AzureTN	GFW-Azure-Demo-Lab	Status Branch-to-brand	: ✔ Succeeded ch : Enabled
Access control (IAM) Location : East US Tags Subscription : AzureTh	AE	Branch-to-brand	ch : Enabled
Tags Subscription : AzureTN	AE		
	<u></u>	Virtual hubs	: 1
Subscription ID : 0683d4	)6-4d77-4bb7-b1a6-165c282b5d37	Topology	: <u>View Topology</u>
Tags ( <u>edit</u> ) : <u>Add tag</u>	<u>§</u>		
Configuration World map			
Properties			
Locks			
Connectivity			
Hubs		a series	
VPN sites		G AV S	
VPN sites			
VPN sites User VPN configurations	24		

Home > Microsoft.Template-20231120110620 | Overview > CloudNGFW-Azure-Demo-Lab > CNGFW-Demo-VWAN ₩ CNGFW-Demo-VWAN | Hubs ★ ··· × \*\* ₽ Search 🕂 New Hub 💍 Refresh 📀 Overview Search for hubs by name Clear all filters Activity log ⁺<sub>▼</sub> Add filter Access control (IAM) Hub Hub status VPN sites Region Address Space Point-to-site ExpressRoute Circuits 🇳 Tags 10.210.0.0/24 CNGFW-Demo-VWAN-Hu 😌 Updating East US ... Settings Configuration Properties 🔒 Locks Connectivity 👾 Hubs

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

•

Home > Microsoft.Template-202312141355 CNGFW-Demo-VWAN Virtual WAN Search «	509   Overview > CloudNGFV <b>V</b>   Hubs ☆ … + New Hub () Refresh	N-Azure-Demo-Lab ≻ CNG	FW-Demo-VWAN			
Overview     Activity log     Access control (IAM)		Clear all filters				
🗳 Tags	Hub	Hub status	Region	VPN sites	Address Space	Point-to-site
Settings	CNGFW-Demo-VWAN-Hub0	Succeeded	East US	-	10.210.0.0/24	
Configuration						
Properties						
Locks						
Connectivity           Hubs           If 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	, AN-Hub01 ጵ …		
	🖉 Edit virtual hub 📋 Delete 🖒 Refresh 🖒 Reset router 🖒 Reset Hub		
👾 Overview 🔺	↑ Essentials		
Connectivity	Name : CNGFW-Demo-VWAN-Hub01	Routing status	: 🕑 Provisioned
· V/DN (Cite to cite)	Resource group : <u>CloudNGFW-Azure-Demo-Lab</u>	Hub routing preferer	nce : ExpressRoute
VPN (Site to site)	Tags : <u>Tags</u>	Metrics	: View in Azure Monitor
A ExpressRoute	Hub status : 📀 Succeeded		
🛃 User VPN (Point to site)	Private address space : 10.210.0.0/24		
Routing	See more		
Route Maps (Preview)	8		
Routing Intent and Routing	Virtual network connections VPN (Site to site)	User VPN (P	oint to site)
Policies	Connect virtual networks to a virtual Connect a VPN Site to a virtual hub VPN	Connect a User VPN	Configuration to a

• Now Click on "Home" to go to your Azure portal home page

,



# 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

≡	Microsoft Azure	Q	paloalto					$\times$	$\geq$	Ŗ	Q	ŝ	?	ନ
	Azure service		All Services (2)	Marketplace (17)	Documentatio	on (4)	Resources	(0)	Res	ource (	Groups	(0)		
	+	s	Azure Active Directory (0)											
create a resource		¢	b Cloud NGFWs by Palo Alto	o Networks		🧓 Loc	al Rulestacks f	for Clou	ıd NGFV	/ by Pa	lo Alto	Netwoi	rks	
		Ν	/larketplace		_									See all

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



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

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.

Subscription * 🛈	AzureTME 🗸
Resource group * 🛈	CloudNGFW-Azure-Demo-Lab
Firewall Details	
Firewall Name * 🛈	CloudNGFW-Azure-VWAN-Demo
Region * 🕡	East US 🗸
Marketplace Plan *	Cloud Next-Generation Firewall by Palo Alto Networks - An Azure N $\checkmark$
Previous Next Revie	w + create

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

Home > Cloud NGFWs by Palo Alto N	Vetworks >
Create Cloud NGFW k	y Palo Alto Networks
Basics Networking Security Po	olicies DNS Proxy Tags Terms Review + create
Please configure your Firewall deploym	ent with network requirements, i.e., Public IP CIDR and virtual network settings.
Network Type	
Type *	Virtual Network
Virtual Wan Hub Details	
Virtual Hub Name * 🛈	CNGFW-Demo-VWAN-Hub01
Public IP Address Configuration	
Public IP Address(es) * 🔋	Create new
	<ul> <li>Use existing</li> </ul>
Public IP Address Name(s) * i	frontendip 🗸
Additional Prefixes To Private Traffic	c Range
Additional Prefixes ①	
Source NAT Settings	
Enable Source NAT 🛈	
Use the above Public IP Address(es)	
Previous Next Rev	ew + 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 Poli	cies	DNS Proxy	Tags	Terms	Review + create
Managed	by * i		•	Azure Rulestac Palo Alto Netw	k orks Pano	rama	
Choose a	Local Rulestack *	i	•	Create new Use existing			
Local Rule	estack *		Clo	oudNGFW-Azur	e-VWAN-	Demo-Irs	
Firewall ru	ules * 🛈			Allow all (Enabl inspect traffic)	les all secu	urity service	es using best-practices profile to
			0	Deny all			
<b>Π</b> Το	use Palo Alto Netv	orks Advanced	Cloud-	Delivered Securit	v Services	(such as Adv	vanced Threat Prevention, Advanced

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 NGEWS by Palo Alto Netwo	orks	>
---------------------------------------	------	---

## Create Cloud NGFW by Palo Alto Networks

Basics	Networking	Security Policies	DNS Proxy	Tags	Terms	Review + create
DNS Prox	y * 🛈		Disabled			
		0	Enabled			



• 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**" Home > Cloud NGFWs by Palo Alto Networks >

#### 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	
	:	5 selected V	

Previous	Next	Review + create

#### • Accept the terms

Click on check-box to agree for the terms and conditions as shown below 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

 Terms of use | Privacy Policy

By clicking Create | agree to the legal terms and privacy statement associated with the Marketplace offering (licensed by Palo Alto Networks by the <u>End User Agreement</u>) 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 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 \*

Γ	Previous	Next	Review + create
_			

• Review the configuration and Create Cloud NGFW

rionic / cloud rion by raid / allo	Home	>	Cloud	NGFWs	by	Palo	Alto	Networks	>
---	------	---	-------	-------	----	------	------	----------	---

#### Create Cloud NGFW by Palo Alto Networks Basics Networking Security Policies DNS Proxy Terms Review + create Tags 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 Туре Virtual Wan Hub CNGFW-Demo-VWAN-Hub01 Virtual Hub Name Public IP Address(es) Use existing Public IP Address Name(s) frontendip **Security Policies** Managed by Azure Rulestack ~ . .... Next Previous 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	1-202312	14145212   Overview 🛷 …			
	📋 Delete	🚫 Cancel 🚏 Redeploy 🛓 Download 💍 Refresh			
🙏 Overview	Der	lovment is in progress			
😫 Inputs	Dep	soyment is in progress			
š≡ Outputs	(ক) Deplo Subso	oyment name:CreateFirewallForm-20231214145212 rription  :AzureTME	Start time : 12/14 Correlation ID : 4574	/2023, 2:55:45 ccb7-abf1-4c03	PM 3-a42d-add38f7be866
📄 Template	Resou	rce group : CloudNGFW-Azure-Demo-Lab			
	✓ Deployment details				
		Resource	Туре	Status	Operation details
	Θ	CloudNGFW-Azure-VWAN-Demo-Irs	🜏 Local Rulestack for Cloud NGFW	Created	Operation details
	•	CloudNGFW-Azure-VWAN-Demo-nva	🤿 Microsoft.Network network virtu	Created	Operation details

### 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



- 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-202312141	45212 Overview 7		
CloudNGFW-Azure	-Demo-Lab ☆ ☆ …		
₽ Search «	🕂 Create 🚳 Manage view 🗸 📋 Delete resource group 💍 Refresh 🞍 Export to CSV 😤	Open query $\mid \ \oslash$ Assign tags $\rightarrow$ Move $\checkmark$	🛍 Delete 🚽 Export template
💓 Overview	✓ Essentials		
<ul> <li>Activity log</li> </ul>			
Access control (IAM)	Resources Recommendations		
🗳 Tags	Filter for any field		
🛧 Resource visualizer			
🗲 Events	Showing 1 to 16 of 16 records.		No grouping V
Settings	□ Name ↑↓	Туре ↑↓	Location $\uparrow\downarrow$
Deployments	CloudNGFW-Azure-VWAN-Demo	Cloud NGFW by Palo Alto Networks	East US
Security	CloudNGFW-Azure-VWAN-Demo-Irs	Local Rulestack for Cloud NGFW by Palo Alto	Net East US
Deployment stacks	CloudNGFW-Logs	Log Analytics workspace	East US
Policies	CNGFW-Demo-VWAN	Virtual WAN	East US
Properties	🗌 📮 database-vm	Virtual machine	East US
	🔲 🍘 database-vm-nic0	Network Interface	East US
	🗌 🛢 database-vm_OSDisk	Disk	East US
Cost Management	🗌 🧰 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".

₽ Search	« 💍 Refresh 📋 Delete		
👌 Overview	Resource group (move) : <u>CloudNGFW-Azure-Demo-Lab</u>	Resource id : /subscriptions/0	683d406-4d77-4bb7-b1a6-165o
Activity log	Location : East US	Health Status : 🔴 Healthy	
Access control (IAM)	Subscription (move) : AzureTME	Type : paloaltonetwork	s.cloudngfw/firewalls
Tags	Subscription ID : 0683d406-4d77-4bb7-b1a6-165c282b5d37	Public IPs : 4.156.189.70	
attin ac		Private IPs : 10.210.0.228	
ettings	Tags (edit) : StoreStatus : DND InstanceLife : 60 office : India userID : rpegada		
Networking & NAT	See more		
Security Policies			
Log Settings	Get started Properties Recommendations		
DNS Provv			
DIADTIONY			
Rules	Sloud NGFW	ONS Proxy	
Rules Properties	Cloud NGFW Identity ①	DNS Proxy Enable DNS proxy ①	DISABLED
Properties	Cloud NGFW Identity O System data O View value as JSON	DNS Proxy Enable DNS proxy ① Enabled DNS type ①	DISABLED CUSTOM
Rules Properties Locks	Cloud NGFW Identity O System data O View value as JSON	<b>DNS Proxy</b> Enable DNS proxy ① Enabled DNS type ① DNS servers ①	DISABLED CUSTOM
r Rules Properties Locks upport + troubleshooting	Cloud NGFW Identity O System data O View value as JSON  Properties	DNS Proxy Enable DNS proxy ① Enabled DNS type ③ DNS servers ③	DISABLED CUSTOM 
Rules Properties Locks pport + troubleshooting New Support Request	Cloud NGFW  Identity   Identity   Tropperties  Front end settings   Front end	DNS Proxy Enable DNS proxy ① Enabled DNS type ① DNS servers ③	DISABLED CUSTOM 
Rules     Properties     Locks     proort + troubleshooting     New Support Request     onitoring	Cloud NGFW  Identity   Identity   System data   View value as JSON  Properties  Front end settings   Front end settings   Succeeded	<ul> <li>DNS Proxy</li> <li>Enable DNS proxy ()</li> <li>Enabled DNS type ()</li> <li>DNS servers ()</li> <li>Plan data</li> <li>Usage type ()</li> </ul>	DISABLED CUSTOM  PAYG
Rules     Properties     Locks     prost + troubleshooting     New Support Request     onitoring     Alerts	Cloud NGFW  Identity   Identity   Trons and   Trons and settings   Front end settings   Front end settings   Front end settings   Succeeded   Tronsioning state  Networking & NAT	<ul> <li>DNS Proxy</li> <li>Enable DNS proxy ①</li> <li>Enabled DNS type ②</li> <li>DNS servers ③</li> <li>Plan data</li> <li>Usage type ③</li> <li>Billing cycle ③</li> </ul>	DISABLED CUSTOM  PAYG MONTHLY

## **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

Cloud NGEW by Pala Alta Natworks	e-VWAN-Demo   Log	g Settings 👒 …
Search	K Z Edit 🖒 Refresh	
Overview		
Activity log	Log Settings	
Access control (IAM)	Log Settings	No log settings found
Tags	5 5	5 5
tings		
Networking & NAT		
Security Policies		
Log Settings		
DNS Proxy		
Rules		
Properties		
Locks		

• 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

Home > CloudNGFW-Azure-Demo	-Lab > CloudNGFW-Azure-VWAN-Den	10	
Cloud NGFW by Palo Alto Network	serverse in the serverse servers and the serverse servers and the serverse servers and the serverse servers and the serverse se	Settings 🛪 …	
₽ Search	« 🔚 Save 🗙 Discard		
👶 Overview	*		
Activity log	Log Settings		
Access control (IAM)	Enable Log Settings		
🇳 Tags	Log Settings	CloudNGFW-Logs	~
Settings			
Networking & NAT			
Security Policies			
Log Settings			
DNS Proxy			
👇 Rules			
Properties			
A Locks			

#### 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

Cloud NGFW by Palo Alto Network	ure-VWAN-Demo   Network	sing & NAT 👒 …
♀ Search	« 🖉 Edit 💍 Refresh	
👴 Overview	A	
Activity log	Networking	
Access control (IAM)	Туре	Virtual Network
Settings		Virtual WAN Hub
↔ Networking & NAT	Virtual Hub	CNGFW-Demo-VWAN-Hub01
👵 Security Policies	NVA Id	CloudNGFW-Azure-VWAN-Demo-nva
Log Settings		
DNS Proxy		
🗲 Rules		
Properties	Source Network Address	Translation (SNAT)
Locks	Public IP Addresses	20.241.255.169
Support + troubleshooting		_
💺 New Support Request	Enable Source NAT (i)	
Monitoring	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

Home > CloudNGFW-Azure-Demo-Lab	b > CloudNGFW-Azure-VWAN	i-Demo				
CloudNGFW-Azure	e-VWAN-Demo   N	letworking	& NAT ☆			
Cloud NGFW by Palo Alto Networks						
✓ Search «	🗟 Save 🗙 Discard					
left overview						
Activity log	Source Network	Address Trar	slation (SNAT)	)		
Access control (IAM)		_	, , , , , , , , , , , , , , , , , , ,			
🗳 Tags	Public IP Addresses	f	rontendip		$\sim$	
Settings	Enable Source NAT 🛈	~	1			
🐡 Networking & NAT	Use the above Public IP a	ddresses 🗸				
or Security Policies			•			
Log Settings						
DNS Proxy	Destination Net	work Address	Translation (D	NAT)		
ᠲ Rules			x	·		
Properties	🔎 Search					
Locks	+ Add 🛍 Delete	è				
Support + troubleshooting						
🔚 New Support Request	Name	Protocol	Frontend IP	Frontend Port	Backend IP	Backend Port
Monitoring						
Alerts	No data is availab					

- 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

Nama *	AccessTo Web	
Name	Accessiowed	
Protocol *	💿 тср	
Frontend IP *	frontendip	V
Frontend Port *	80	
Backend IP *	10.5.0.5	
Backend Port *	80	



- 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
  - 0

## Add Frontend Setting Provide Configuration for Frontend Setting

Name *	SSHAccessToWeb	
Protocol *	• тср	
Frontend IP *	frontendip	~ ·
Frontend Port *	221	
Backend IP *	10.5.0.5	
Backend Port *	22	

Add	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

O Search	« 🔛 Sav	e 🗙 Discard					
Overview	▲ Sou	rce Network Addre	ss Translatio	n (SNIAT)			
Activity log	500		55 1141151410				
Access control (IAM)	Public	IP Addresses	frontendi	0		$\sim$	
Tags	Enable	e Source NAT 🛈	<b>~</b>				
ttings			_				
Networking & NAT	Use th	ne above Public IP addresses	<b>~</b>				
Security Policies							
Log Settings	Du	ting ting Network A		lation (DNAT)			
Log Settings DNS Proxy	Des	tination Network A	ddress Trans	slation (DNAT)			
Log Settings DNS Proxy Rules	Des ,2	tination Network A	ddress Trans	slation (DNAT)			
Log Settings DNS Proxy Rules Properties	Des >	tination Network A	ddress Trans	slation (DNAT)			
Log Settings DNS Proxy Rules Properties Locks	Des P	tination Network A Search Add i Delete	ddress Trans	slation (DNAT)			
Log Settings DNS Proxy Rules Properties Locks pport + troubleshooting	Des P	tination Network A Search Add I Delete	ddress Trans	Slation (DNAT)	Frontend Port	Backend IP	Backend Port
Log Settings DNS Proxy Rules Properties Locks port + troubleshooting New Support Request	Des ~ +	tination Network A Search Add i Delete Name	ddress Trans	Slation (DNAT)	Frontend Port	Backend IP	Backend Port
Log Settings DNS Proxy Rules Properties Locks port + troubleshooting New Support Request nitoring	Des P +	tination Network A Search Add  Delete Name AccessToWeb	ddress Trans	Frontend IP frontendip	Frontend Port	Backend IP	Backend Port

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

O Coarch		
Activity log	Networking	
Access control (IAM)		$\bigcirc$
Tags		Saving
ttings		
Networking & NAT		
Security Policies		
Log Settings		

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

#### Destination Network Address Translation (DNAT)

🔎 Search

Name	Protocol	Frontend IP	Frontend Port	Backend IP	Backend Port
AccessToWeb	ТСР	frontendip	80	10.5.0.5	80
SSHAccessToWeb	ТСР	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 Demo   Rules	* …						
	🕐 Refresh								
left overview	🔎 Search								
<ul> <li>Activity log</li> </ul>									
Access control (IAM)	<ul> <li>✓ Priorit</li> </ul>	ty	Name	Source	Destination	Constraints	Action	Logging	Egress Decry
Tags									
Settings	∨ Local	Rules (1)							1
🐡 Networking & NAT	10000	00	cloud-ngfw-default-rule	any	any	Default	Allow	yes	Disabled
👵 Security Policies				,	,			,	
Log Settings									1
DNS Proxy									
🗣 Rules									
Properties									
□ Locke									

#### 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

Home >			
CloudNGFW-Azure-I	Demo-Lab 🖉 🛧 …		
	🕂 Create 🛞 Manage view 🗸 📋 Delete resource group 🖒 Refresh 🞍 Export to CSV 😽 Op	hen query $ $ $@$ Assign tags $\rightarrow$ Move $\checkmark$ $1$	Delete 🛓 Export
() Overview	✓ Essentials		
<ul> <li>Activity log</li> </ul>	Describer of the Ch		
Access control (IAM)	Resources Recommendations (6)		
🗳 Tags	Filter for any field Type equals all X Location equals all X + Add filter		
🛧 Resource visualizer			
🗲 Events	Showing 1 to 16 of 16 records.	No	grouping
Settings	Name ↑↓	Type ↑↓	Location $\uparrow\downarrow$
↑ Deployments	CloudNGFW-Azure-VWAN-Demo	Cloud NGFW by Palo Alto Networks	East US
<ul> <li>Security</li> </ul>	CloudNGFW-Azure-VWAN-Demo-Irs	Local Rulestack for Cloud NGFW by Palo Alto Net.	East US
Deployment stacks	CloudNGFW-Logs	Log Analytics workspace	East US
Policies	CNGFW-Demo-VWAN	Virtual WAN	East US
Properties	🗌 📮 database-vm	Virtual machine	East US
in reperies	🗌 🧶 detekara yan aint	Network Interface	Eact LIS

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

Home > CloudNGFW-Azure-Demo-La	b > CloudNGFW-Azure-VWAN-Demo-Irs							
CloudNGFW-Azure	e- <b>VWAN-Demo-Irs</b>   Rule	2S ☆ …						
₽ Search «	🕐 Refresh							
🗟 Overview 🔺								
<ul> <li>Activity log</li> </ul>	Local Rules	A local a local de la sector de la sector de la constituida d'actor de	and the state of the					
Access control (IAM)	+ Add / Edit Delet	8. A local fulestack can be used on multiple frewails 8	s within the same subscription	JIL.				
🗳 Tags								
Settings	Priority	Name	Source	Destination	Constraints	Action	Logging	Egress Dec
Properties	1000000	cloud-ngfw-default-rule	any	any	Default	Allow	yes	Disabled
🔒 Locks								
Resources								
🗣 Rules								
🔋 Security Services								
Prefix List								

• 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	O Any
	Match
IP Address (CIDR Format)	10.5.0.0/24
Countries	
Prefix List	V
Exclude	
Destination	
Match Criteria	O Any
	Match
IP Address (CIDR Format)	10.6.0.0/24

Countries	
Prefix List	
FQDN List	
Destination Exclude	
Granular Controls	
Application Match Criteria	
Match Citteria	Any
	<ul> <li>Select</li> </ul>
Applications	mysql v
URL Category	
Match Criteria	Any
	○ Select
Protocol & Port	
Match Criteria	O Application Default
	Any
	O Select
Actions	
Actions	<ul> <li>Allow</li> </ul>
	O Drop
	O Reset Server
	O Reset Both
Egress Decryption (i)	
Logging	
Save	

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
	O Match
Destination	
Match Criteria	<ul> <li>Any</li> </ul>
	O Match
Granular Controls Application	
Match Criteria	<ul> <li>Any</li> </ul>
	○ Select

URL Category	
Match Criteria	O Any
	Select
Categories *	social-networking
Match Criteria	Application Default
	Any
	O Select
Actions	
Actions	O Allow
	Drop
	O Reset Server
	O Reset Both
Egress Decryption	
Logging	

#### Newly added policies would look as shown below

	« ک	Refresh							
Overview     Activity log     Access control (IAM)	Î A	Local Rules A local rulestack consists of I + Add	local rules. A local rulestack can be used on	multiple firewalls with	in the same subscript	ion.			
🗳 Tags									
Settings		Priority	Name	Source	Destination	Constraints	Action	Logging	Egress D
Properties		400	BlockSocialNetworking	any	any	Custom	Drop	yes	Disabled
Locks		500	AllowMySQLFromWebtoDB	match	match	Custom	Allow	yes	Disabled
Resources		1000000	cloud-ngfw-default-rule	any	any	Default	Allow	yes	Disabled
Security Services	1.1	4							E F
Prefix List									

#### **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

CloudNGFW-Azure-V	/WAN-Demo-Irs   Dep Ito Networks	oloyment 🛧 …		
✓ Search «	🕐 Refresh			
net state of the s				
Activity log	Deployment			
Access control (IAM)				
🗳 Tags	Config	Status	Action	
Settings	Candidate Configuration	Pending Deployment: LocalRule, Rulestack	Benloy Configuration	S Revert
Properties			<ul> <li>Deploy configuration</li> </ul>	
🔒 Locks				
Resources				
🗣 Rules				
🕵 Security Services				
Prefix List				
🧮 FQDN List				
📮 Certificates				
📩 Deployment				
Anaged Identity				

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.



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

Home > CloudNGFW-Azure-Dem	no-Lab > CloudNGFW-Azure-VWAN	N-Demo-Irs			
CloudNGFW-Azt	Cure-VWAN-Demo-Ir	s∣Deployment ☆			
♀ Search	🛛 « 💍 Refresh				
👵 Overview	A				
Activity log	Deploymen	it			
Access control (IAM)					
🗳 Tags	Config	Status	Ac	tion	
Settings	Candidate Configuratio	on Deployed	8	Deploy Configuration	19 Revert
Properties				Deploy configuration	
🔒 Locks					
Resources					
🗣 Rules					
🜻 Security Services					
Prefix List					
💳 FQDN List					
Certificates					
Deployment					
🌆 Managed Identity					

## 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

	e-Demo-Lab			×
🔎 Search 🤍	🕂 Create 🍥 Manage view 🗸 🔋 Delete resource group 💍 Refresh 🞍 Export to CSV 😚 Open que	ry $ $ $\oslash$ Assign tags $\rightarrow$ Move $\checkmark$ $\square$ Delete $\downarrow$	Export template	
() Overview	← Essentials			JSON View
Activity log	Subscription (move) : AzureTME	Deployments : 2 Succeeded		
Access control (IAM)	Subscription ID : 0683d406-4d77-4bb7-b1a6-165c282b5d37	Location : East US		
🗳 Tags	Tags (edit) : Add_tags			
A Resource visualizer				
🗲 Events	Resources Recommendations (6)			
Settings	Filter for any field Type equals all X Location equals all X * Add filter			
1 Deployments	Showing 1 to 16 of 16 records.		No grouping V	≡ List view ∨
Security	Name ↑↓	Type ↑↓	Location 1	
Deployment stacks	CourdNGEW Attice VMANI Domo	Cloud NGEW by Palo Alto Naturatio	East LIS	
Policies			East 05	
Properties	CloudNGFW-Azure-VWAN-Demo-Irs	Local Rulestack for Cloud NGFW by Palo Alto Networks	s East US	
Locks	CloudNGFW-Logs	Log Analytics workspace	East US	
	CNGFW-Demo-VWAN	Virtual WAN	East US	
Cost Management	🗌 🖳 database-vm	Virtual machine	East US	
🔍 Cost analysis	🔲 🧟 datahase-vm-nici)	Network Interface	East US	•
Cost alerts (preview)				•

Go to Hubs within the virtual wan selected.

Home > CloudNGFW-Azure-Den	no-Lab > ∙VWAI	CNGFW-Demo-VWAN N   Hubs ☆ …						
₽ Search	] «	+ New Hub 💍 Refresh						
🤝 Overview	-	Search for hubs by name	Clear all filters					
Activity log		ja Scaren for habs by hume	Clear an inters					
Access control (IAM)		⁺ <sub>7</sub> Add filter						
🗳 Tags		Hub	Hub status	Region	VPN sites	Address Space	Point-to-site	ExpressRo
Settings		* CNGFW-Demo-VWAN-Hub01	Succeeded	East US	-	10.210.0.0/24	-	-
Configuration								
Properties								
🔒 Locks								
Connectivity								
🔆 Hubs								
VPN sites								
User VPN configurations								

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

Home > CloudNGFW-Azure-Demo-Lab	> CNGFW-Demo-VWAN   Hubs > CNGFW-Demo-VWAN-Hub01						
CNGFW-Demo-VWAN-Hub01   Routing Intent and Routing Policies							
	🔜 Save 🗙 Cancel 📋 Delete						
🐳 Overview	Configure routing policies for CNGFW-Demo-VWAN-Hub01 Virtual Hub						
Connectivity	Routing Policies for Internet Traffic apply to all connections connected to the Virtual Hub						
VPN (Site to site)							
▲ ExpressRoute	Kouting Policies for Private Iraffic apply to all private traffic destined for addresses in the Private Traffic Prefixes below (regardless of the source) that enters the virtual hub						
Al User VPN (Point to site)	Internet traffic	Next Hop Resource					
	SaaS solution V	CloudNGFW-Azure-VWAN-Demo-nva					
Routing	Private traffic	Next Hop Resource					
Route Maps (Preview)	SaaS solution V	CloudNGFW-Azure-VWAN-Demo-nva 🗸					
Routing Intent and Routing Policies	Private Traffic:         10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16,						
BGP Peers							
🥺 Route Tables							
Effective Routes							

## 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

₽ Search		« ک	Refresh 🚫 Cancel 🚏 Redeploy <u>前</u> Delete	e 🞍 View template	
🧭 Overview		▲ Filte	er by deployment name or resources in the deployn	nent	
Activity log	1				
Access cont	trol (IAM)		Deployment name	Status	
🧳 Tags			CreateFirewallForm-20231214145212	Succeeded	
🛧 Resource vi	isualizer		Microsoft.Template-20231214135509	Succeeded	
🗲 Events					
Settings	_				
拾 Deploymen	nts				
Security					
Deploymen	nt stacks				
	it stacks				
Policies					
ome > CloudNGFW-Azure-D /licrosoft.Templat	te-20231214135509   Out	ate-20231214135509			
eployment	~ «				
Overview	web-server-url				
Inputs	http://4.156.189.70				<u> </u>
Outputs	web-server-url-wordpress				
j iempiate	http://4.156.189.70/wordpres	S			4
	web-server-url-sql-attack				
	http://4.156.189.70/sql-attac	k.html			<u> </u>
	ssh-web-vm				
	ssh paloalto@4.156.189.70 -p	221			(
	username				
	paloalto				Į.
	password				
	Pal0Alt0@123				Ū.
	frontend-IP				
	4.156.189.70				Î

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

web-server-unt	
http://4.156.189.70	
Let a set	
web-server-url-wordpress	
http://4.156.189.70/wordpress	Ð
web-server-url-sql-attack	
http://4.156.189.70/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 >			
CloudNGFW-Azure-	Demo-Lab 🖈 ★ …		
	🕂 Create 🚳 Manage view 🗸 📋 Delete resource group 🖒 Refresh 🞍 Export to CSV 😵 Open query	$  \hspace{0.1in} \textcircled{0} \hspace{0.1in} \operatorname{Assign} \operatorname{tags} \hspace{0.1in} \rightarrow \hspace{0.1in} \operatorname{Move} \hspace{0.1in} \smile \hspace{0.1in} \rule{0.1in}{1.5in} \rule$	Export template
() Overview	↑ Essentials		
Activity log	Subscription (move) : <u>AzureTME</u>	Deployments : 2 Succeeded	
Access control (IAM)	Subscription ID : 0683d406-4d77-4bb7-b1a6-165c282b5d37	Location : East US	
🗳 Tags	Tags (edit) : Add tags		
A Resource visualizer			
🗲 Events	Resources Recommendations (6)		
Settings	Filter for any field Type equals all $\times$ Location equals all $\times$ $+_{\nabla}$ Add filter		
Deployments	Showing 1 to 16 of 16 records. $\Box$ Show hidden types $\odot$	(	No grouping
Security	Name 1	Type 1	Location 1
Deployment stacks		Claud NCDA by Data Alta Nationalia	Estation
Policies		Cloud NGPW by Palo Alto Networks	East US
Properties	CloudNGFW-Azure-VWAN-Demo-Irs	Local Rulestack for Cloud NGFW by Palo Alto Networks	East US
Locks	CloudNGFW-Logs	Log Analytics workspace	East US
	CNGFW-Demo-VWAN	Virtual WAN	East US
Cost Management	🔲 📮 database-vm	Virtual machine	East US
S. Cost analysis	🔄 🚮 database-vm-nic0	Network Interface	East US
Cost alerts (preview)			

Close "Welcome to Log Analytics" pop-up window

© Search «	
Overview Activity log Access control (IAM) Tags Diagnose and solve problems	Welcome to Log Analytics Azure Monitor Log Analytics is a tool used to produce insights from Azure Monitor logs.
Logs ttings Tables Agents Usage and estimated costs	Azure Menitor Log A Polytics
Data export     Network isolation     Linked storage accounts	. Get instant insights from your logs

_ «		
		×
	Welcome to Log Analytics	
_	Azure Monitor Log Analytics is a tool used to produce insights from Azure Monitor logs.	
	Azure Menitor Log A Palytics	
	Get instant möglich from your logs	

• Close the Queries page as shown below

gs   Logs	x tz				
« 🥔 Nev	v Query 1 × +			♡	Feedback SE Querie
P Clo	Queries		(	Always show Queries 💿   Community Git repo	යී   Documentation යී 🗙 .
Tables	Query packs: Select query packs				- 4
P Sei	Category V	P Search (⁺♥ Add filter)			
E cd	* Favorites	APPLICATIONS			1
Favo	All Queries	CCF application errors	Response time trend	Request count trend	×
You o	Applications	Framework application errors.	Chart request duration over the last 12 hours.	Chart Request count over the last day.	
une s	Audie				

- After going to Log Analytics workspace(ClougNGFW-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

	P New Query 1* × +	
<ul> <li>Overview</li> </ul>	CloudNGFW-Logs Select scope	> Run Time range Last 30 minutes 🗟 Sav
<ul> <li>Activity log</li> </ul>	Tables Queries ···· «	1 fluentbit_CL
Access control (IAM)		
Tags	Search :	
Diagnose and solve problems	Filter ) = Group by: Solution V	
🖗 Logs	T Collapse all	
Settings	Favorites	
Tables	You can add favorites by clicking on the ☆ icon	Queries History
Agents	<ul> <li>Custom Logs</li> </ul>	
Usage and estimated costs	►	
Data export		

• After running the query, you will be seeing the logs as shown below.

CloudNGFW-Logs   Logs     Log Analytics workspace	☆ …											
» P New Query 1* × +	+											
P CloudNGFW-Logs Select scope	▶ Run Time range : Last 3	30 minutes 🛛 🗟 Sa	ve 🗸 🖻 Share 🗸	+ New alert rule → Export	🗸 🖈 Pin to	o 🗸 🛛 😇 Format que	ery					
Tables     Queries     Functions     ··· ≪	1 fluentbit_CL 2 3											
You can add favorites by clicking on	Results Chart											
the # icon	TimeGenerated [UTC] ↑↓	_timestamp_d pr	i_s time_s	host_s	ident_s	Year_s Month_s	Day_s Hou	r_s Min_s	Sec_s	Mess		
<ul> <li>Logivanagement</li> <li>Custom Logic</li> </ul>	> 12/14/2023, 11:18:38.399 AM	1702523915 14	Dec 14 03:18:35	cloudngfw-azure-vwan-demo	TRAFFIC	2023 12	14 03	18	35	{"src_		
, custom Logs	> 12/14/2023, 11:18:37.260 AM	1702523915 14	Dec 14 03:18:35	cloudngfw-azure-vwan-demo	TRAFFIC	2023 12	14 03	18	35	("src_		
	> 12/14/2023, 11:18:37.260 AM	1702523915 14	Dec 14 03:18:35	cloudngfw-azure-vwan-demo	TRAFFIC	2023 12	14 03	18	35	{"src_		
	> 12/14/2023, 11:18:32.567 AM	1702523910 14	Dec 14 03:18:30	cloudngfw-azure-vwan-demo	TRAFFIC	2023 12	14 03	18	30	{"src_		
	> 12/14/2023. 11:18:32.567 AM	1702523910 14	Dec 14 03:18:30	cloudngfw-azure-vwan-demo	TRAFFIC	2023 12	14 03	18	30	{"src_		
	> 12/14/2023, 11:18:32.524 AM	1702523910 14	Dec 14 03:18:30	cloudngfw-azure-vwan-demo	TRAFFIC	2023 12	14 03	18	30	{"src_		
	> 12/14/2023. 11:18:29.351 AM	1702523907 14	Dec 14 03:18:27	cloudngfw-azure-vwan-demo	TRAFFIC	2023 12	14 03	18	27	{"src_		
	> 12/14/2023. 11:18:28.382 AM	1702523905 14	Dec 14 03:18:25	cloudngfw-azure-vwan-demo	TRAFFIC	2023 12	14 03	18	25	{"src_		
	> 12/14/2023. 11:18:28.382 AM	1702523905 14	Dec 14 03:18:25	cloudngfw-azure-vwan-demo	TRAFFIC	2023 12	14 03	18	25	("src_		

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

Winew Query 1" × T					
P CloudNGFW-Logs Select scope	▶ Run Time range : Last	30 minutes	Save ∨	🖻 Share 🗸 🚽	– New alert rule → Exp
Tables Queries Functions … «	1 fluentbit_CL				
	3				
(					
T Collapse all					
Favorites					
You can add favorites by clicking on the 🖈 icon	Results Chart				
▶ LogManagement	TimeGenerated [Local Time] ↑↓	_timestamp_d	pri_s	time_s	host_s
Custom Logs	> 12/14/2023, 4:48:38.399 PM	1702523915	14	Dec 14 03:18:35	cloudngfw-azure-vwan-de
- custom bogs	> 12/14/2023, 4:48:37.260 PM	1702523915	14	Dec 14 03:18:35	cloudngfw-azure-vwan-de
	> 12/14/2023, 4:48:37.260 PM	1702523915	14	Dec 14 03:18:35	cloudngfw-azure-vwan-de
	> 12/14/2023, 4:48:32.567 PM	1702523910	14	Dec 14 03:18:30	cloudngfw-azure-vwan-de
	> 12/14/2023, 4:48:32.567 PM	1702523910	14	Dec 14 03:18:30	cloudngfw-azure-vwan-de
	> 12/14/2023, 4:48:32.524 PM	1702523910	14	Dec 14 03:18:30	cloudngfw-azure-vwan-de
	> 12/14/ UTC		14	Dec 14 03:18:27	cloudngfw-azure-vwan-de
			14	Dec 14 03:18:25	cloudngfw-azure-vwan-de
	> 12/14/				

• Sort the logs to view latest on top

₽	CloudNGFW-Logs   Logs	☆ …												
>>	🍄 New Query 1* 🛛 × 🕂										💙 Fe	edback B	Queries	Ø
	P CloudNGFW-Logs Select scope	▶ Run Time range : Last 3	0 minutes	🛾 Save 🗸	🖻 Share 🗸 🚽	New alert rule → Export	∨ 🖈 Pin	to 🗸   🗉	Format query					
	Tables     Queries     Functions     ···     《       P     Search     :     :     :       V     Filter     Illii Group by: Solution     ··       I <sup>®</sup> Collapse all     Favorites     :       You can add favorites by clicking on	1 fluentbit_CL Results Chart												
	the ☆ icon	TimeGenerated [Local Time ↑↓	_timestamp_d	pri_s	time_s	host_s	ident_s	Year_s	Month_s	Day_s	Hour_s	Min_s	Sec_s	N
	Custom Logs	> 11/21/2023, 11:21:01.632 AM	1700517059	14	Nov 20 21:50:59	cloudngfw-azure-vwan-demo	TRAFFIC	2023	11	20	21	50	59	ſ
	Image: International Internatinational International International International International	> 11/21/2023, 11:20:37.255 AM	1700517034	14	Nov 20 21:50:34	cloudngfw-azure-vwan-demo	THREAT	2023	11	20	21	50	34	("
		> 11/21/2023. 11:20:06.365 AM	1700516999	14	Nov 20 21:49:59	cloudngfw-azure-vwan-demo	TRAFFIC	2023	11	20	21	49	59	{"
		> 11/21/2023, 11:19:47.136 AM	1700516985	14	Nov 20 21:49:45	cloudngfw-azure-vwan-demo	TRAFFIC	2023	11	20	21	49	45	ſ
		> 11/21/2023. 11:19:02.120 AM	1700516940	14	Nov 20 21:49:00	cloudngfw-azure-vwan-demo	THREAT	2023	11	20	21	49	00	{"

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



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

CloudNGFW-Logs   Logs Log Analytics workspace	☆ …		>
» P New Query 1* × +		♡ Feedback 🔠 Queries   🛞 🗓	1
P CloudNGFW-Logs Select scope	▶ Run Time range : Last	30 minutes) 🔚 Save ∨ 😰 Share ∨ + New alert rule → Export ∨ 🖈 Pin to ∨   😇 Format query	
Tables     Queries     Functions     ···     ≪	1 fluentbit_CL 2 3		
Favorites			^
You can add favorites by clicking on the \$\phi\$ icon	Results Chart	م	١.
LogManagement	TimeGenerated [Local Time] $\uparrow \downarrow$	Message	
Custom Logs	> 12/14/2023, 4:44:44.204 PM	("src_jp":"134238.236.250", "sport":"40383", "dst_jp":"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.jp?:65.154226.167", "sport": 30740", "dst.jp?"4.156.189.70", "dport": 80", "proto"; "tcp", "app": Web-browsing", "rule", "doud-ngfw-default-rule", "action"; "allow", "bytes_recv"; "11141", "bytes_sent".	
	> 12/14/2023, 4:44:33.803 PM	("src_jp":10.5.0.5", "sport"/53786", "dst_jp":20.42.73.216", "dport":443", "proto":tcp", "app":"azure-log-analytics", "rule": doud-ngfw-default-rule", "action":"allow", "bytes_recv":"5110", "bytes_sent":"3	
	> 12/14/2023, 4:44:33.075 PM	(src.jp):10.6.05% sport/139676% dst.jp):140.71.12.254% dport/1443% proto/14cp% app/i/azure-log-analytics% rule/1/cloud-ngfw-default-rule% action/1/allow% bytes_recv/1/5110% bytes_recv/1/5110%	
	> 12/14/2023, 4:44:29.083 PM	("src.jp?134.238.236.250", "sport":403031, "dst"):4156.189.70", "dport":%0", "proto":"tcp", "app":"web-browsing", "rule":"doud-ngfw-default-rule", "arcion":"alert", "url_jdx":"3", "url_category_list":"me	
	> 12/14/2023, 4:44:28.401 PM	[src.jp?r65.154.226.1677, "sport"/307407, "dst"/4.156.189.707, "dport"/807, "proto"/tcp", "app"/web-browsing", "rule"/cloud-ngfw-default-rule", "action"/alert", "urt.jdx?"11", "urt.jdx?"11", "urt.jdx?"1", "ur	Ł
	> 12/14/2023, 4:44:24.959 PM	("src.jp":1134238236250", "sport":40383", "dst":4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"doud-ingfw-default-rule", "action":"alert", "url_idx:"1", "url_category_list":"me	Ł
	> 12/14/2023, 4:39:24.534 PM	["src.jp?"185.224.128.184", "sport": 555", "dst.jp?"4.156.189.70", "dport":80", "proto":tcp", "app"; "web-browsing", "rule": 'cloud-ngfw-default-rule", "action"; "allow", "bytes_recv":0", "bytes_rent":103",	1
	> 12/14/2023, 4:39:19.207 PM	("src_jp":185.224.128.184", "sport": 535", "dst":4.156.189.70", "dport": 80", "proto": "tcp", "app": "web-browsing", "rule": "cloud-ngfw-default-rule", "action": block-url", "url_jdx:"1", "url_category_list": "a.	
12/14/2023 4/4/33.075 PM ("err in")	10.6.0.5" "sport":"39676" "det ir	***/07/11225/1***/dourt**///3****reads***reads************************************	 "3
( <u>sic_i</u> ).	10.0.0.5 , sport , 55070 , dst_k	. 40/1/12/22/4 , dport 443 , proto tup , app . azore-log-analytics , fue : cloddengiw-denauterore , action . allow , bytes_tecv . 5110 , bytes_sent .	J.,
12/14/2023, 4:44:29.083 PM {"src_ip":"	'134.238.236.250", sport": "40383	, "dst":"4.156.189.70", "dport":"80", proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"alert", "url_idx":"3", "url_category_list":"m	e
12/14/2023, 4:44:28.401 PM {"src_ip":	'65.154.226.167", "sport": "30740"	"dst":"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	di.
12/14/2023, 4:44:24.959 PM {"src_ip":	134.238.236.250", "sport":"40383	", "dst":"4.156.189.70", "dport":"80", "proto":"tcp", "app":"web-browsing", "rule":"cloud-ngfw-default-rule", "action":"alert", "url_idx":"1", "url_category_list":""m	ie

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

Home > CloudNGFW-Azure-Dem	no-Lab >	CloudNGFW-Azure-VWAN-Demo-	-Irs
CloudNGFW-Az	ure-V / by Palo Al	<b>/WAN-Demo-Irs</b>   Se Ito Networks	ecurity Services 🛣 ···
🔎 Search		🖫 Save 💍 Refresh	
👵 Overview			
Activity log		(i) To use Palo Alto Networks Ad	vanced Cloud-Delivered Security Services (such as Advanced Threat Prevention, Advanced URL Filtering, Wildfire, and
Access control (IAM)		Without registering your Azur	re Tenant, only the standard Cloud-Delivered Security Services (such as Threat Prevention, and URL Filtering) will be o
🗳 Tags		Learn more about various Sec	rurity Services Best Practice profiles.
Settings			
Properties		Advanced Threa	at Prevention
🔒 Locks		Advanced Threat Prevention prote	ects your network by providing multiple layers of prevention during each phase of an attack while leveraging
Resources		nore nere	
💺 Rules		Vulnerability Protection	on Profiles
😡 Security Services		An Intrusion Prevention System (IF	PS) is a network security and threat prevention technology that examines traffic flow to detect and prevent $\boldsymbol{\nu}$
🔤 Prefix List		Enable	
🔤 FQDN List		Profile	Best Practice V
戸 Certificates		Anti-Spyware Profiles	
Deployment		Anti-spyware protection zeroes in	outbound threats, especially command-and-control (C2) activity, where an infected client is being leverage
Managed Identity		Enable 🛈	$\checkmark$
Managed identity		Profile	Best Practice 🗸
Support + troubleshooting		Antivirus Profiles	
🧲 New Support Request		Antivirus protects against viruses,	worms, and trojans as well as spyware downloads.
Monitoring		Enable	
💶 Alerts		Profile	Best Practice $\checkmark$
Automation		File Blocking Profiles	
	-	Use file blocking to prevent the tra	ansmission 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.

ome > CloudNGFW-Azure-Demo-Lab   Deployments > Microsoft.Template-20231214135509								
Microsoft.Template	-2023	1214135509   Outputs	×					
₽ Search	~							
👶 Overview		web-several						
😫 Inputs		nttp://4.1>6.184//0	J W					
€ Outputs		web-server-url-wordpress						
🖹 Template		http://4.156.189.70/wordpress	Ð					
	- I	web-server-url-sol-attack						
		http://14.156.189.70/vql-attack.html	]					

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



← → C A Not secure 4.156.189.70/cgi-bin/guess-sql-root-password.cgi?

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"

Hom	e > CloudNGFW-Logs	
•	CloudNGFW-Logs   Logs	<i>文</i> ☆ …
2	New Query 1* × +     CloudNGFW-Logs Select scope	D Run Time range : Last 30 minutes 🛛 🗟 Save 🗸 🖻 Share 🗸 🕂 Net
	Tables Queries ··· «	1 fluentbit_CL 2   where Message <u>contains</u> "threat" 3   where Message <u>contains</u> "mysql"
	Ø Search :	

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

🧬 New Query 1* 🛛 🖂 🕂							💙 Fee	dback 👫 Queries	© []
P CloudNGFW-Logs Sel	lect scope	▶ Run Time range	: Last 30	0 minutes 🛛 🔚 Save 🗸	✓ 🖻 Share ∨ 🕂 New ale	rt rule → Export 〜	🗸 📌 Pin to 🗸	📰 Format query	
Tables     Queries       P     Search       ▼ Filter     I≡ Group by: Soluti       F     Collapse all       Eavorites	… ≪ : :ion ∽	1 fluentbit_CL 2   where Message cont. 3   where Message cont. 5	ains "my ains "tŀ	ysql" hreat"					
You can add favorites by click	king	Results Chart							\$
on the ☆ icon		TimeGenerated [U ↑↓ ic	dent_s	Message		_		FirewallName_s	
<ul> <li>LogManagement</li> </ul>		> 12/14/2023, 5:12:26 Tr	HREAT	{"src_ip":"10.5.0.5", "spor	t":"37914", "dst":"10.6.0.5", "dport":"3	306", "proto":"tcp" "app'	":"mysql", "rule":	CloudNGFW-Azure-VW	VAN-Dem
<ul> <li>Custom Logs</li> </ul>		> 12/14/2023, 5:12:25 TH	HREAT	{"src_ip":"10.5.0.5", "spor	:":"38154", "dst":"10.6.0.5", "dport":"3	306", "proto":"tcp" "app	":"mysql", <mark>"</mark> rule":	CloudNGFW-Azure-VW	VAN-Demo
Results Chart									Ç
TimeGenerated [U ↑↓	ident_s	Message					Firewa	llName_s	
	TUDEAT	("crc in":"10 5 0 5" "c	sport":"3	37914", "dst":"10.6.0.5",	"dport":"3306", "proto":"tcp"	"app":"mysql", 'rul	e": CloudN	GFW-Azure-VWAN	I-Demo
> 12/14/2023, 5:12:26	INKEAI	( sic_ip : 10.5.0.5 , :	-F						

# 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	
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	
Pal0Alt0@123	

- 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.



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

	R	esults Chart			)
	Tim	eGenerated [Local Time] $\uparrow \downarrow$	ident_s	Message	
	>	5/31/2023, 2:57:16.399 PM	TRAFFIC	("src.jp":10.5.0.5", "sport":42300", "dst.jp":104.244.42.1", "dport":80", "proto":1cp", "app":twitter-base", "rule":BlockSocialNetworking", action":res	et-server", "bytes_i
	>	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":"res	et-server", "bytes_i
	>	5/31/2023, 2:55:51.964 PM	TRAFFIC	("src_ip":"10.5.0.5", "sport":"56758", "dst_in":"185.125.190.18", "dnort":"443", "norto":"tro", "ann":"ssl", "rule", "doud-nofw-default-rule", "action":"allow".	bytes_recv":"1199
:	>	5/31/2023, 2:55:51.964 PM	TRAFFIC	["src_jp":"10.5.0.5", "sport":"56756 ["src_jp":"10.5.0.5", "sport":"56756 ["app":"twitter-base", "rule":"BlockSocialNetworking, "action":"reset-server"	pytes_recv":"1199
	>	5/31/2023, 2:55:51.947 PM	DECRYPTION	("src_ip":"10.5.0.5", "sport":"56758 "bytes_recv":"548", "bytes_sent":"344", "pkts_received":"3", "pkts_sent":"3",	version":"TLS1.3",
	>	5/31/2023, 2:55:51.947 PM	DECRYPTION	("src_ip":"10.5.0.5", "sport":"56758 "start_time":"2023/05/31 02:27:13", "elapsed_time":"0", "repeat_count":"1",	version":"TLS1.3",
	>	5/31/2023, 2:48:51.880 PM	TRAFFIC	["src_ip":"66.240.205.34", "sport"] country":"United States", "session_end_reason":"policy-deny", "xff_ip":""}	tion":"allow", "byt
	>	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":"dpud-nofw-default-rule", "	

END of LAB