



# Cloud NGFW for Azure Deployment guide

Version: 1.0 Authors: Ravisankar Pegada

### **Table of Contents**

Table of Contents2About This Guide3



Integrate Cloud NGFW into Azure Virtual Network(VNet) Infrastructure	5
Pre-deployment of Cloud NGFW - setting up the VNet environment Topology	<b>5</b> 5
Create Spoke VNets with a virtual machine on each of them Create Spoke App01 VNet with Ubuntu Server Create Spoke App02 VNet with Ubuntu Server (For EW-traffic)	6 6 10
Deployment of Cloud NGFW into VNet Infrastructure	11
	24
Post Deployment of Cloud NGFW Create/Update Rule stack	<b>24</b> 24
Source/Destination NAT rule on Cloud NGFW	32
Configure Logging	34
Update Network Security Group	38
Configure VNetpeering between Hub Vnet(that got created during Cloud N creation) and Spoke Vnets	IGFW 39
Add a Route Table to route traffic through Cloud NGFW	39
Testing traffic	41
Test Inbound Traffic	41
Accessing logs	43
Test Outbound Traffic	44
Test Outbound Block Rule	46
Test East-West Traffic flow	47
Integrate Cloud NGFW into Azure Virtual WAN(VWAN) Infrastructure	48
Pre-deployment of Cloud NGFW - setting up the environment	49
Тороlоду	49
Create Spoke VNets with a virtual machine on each of them	50
Create Spoke App01 VNet with Ubuntu Server	50
Create Spoke App02 VNet with Ubuntu Server (For EW-traffic) Create Azure Virtual WAN with Hub	54 55
Deployment of Cloud NGFW	59
Verify for SaaS Solution within Virtual WAN Hub	<b>55</b> 71
Post Deployment of Cloud NGFW	73
Create/Update Rule stack	73
Source/Destination NAT rule on Cloud NGFW	82



Configure Logging	86
Add Spoke(Application) VNets as Virtual Network Connections to Virtual WAN	89
Configure VWAN Hub Routing Intent and Routing Policies	90
Testing traffic	92
Test Inbound Traffic	92
Accessing logs	94
Test Outbound Traffic	97
Test Outbound Block Rule	99
Test East-West Traffic flow	100
Resources	103
Contact	103

# **About This Guide**

Cloud NGFW is the industry's only machine learning (ML)-powered NGFW delivered as a cloud-native service on Azure. With Cloud NGFW, you can run more apps securely at cloud speed and cloud-scale with an actual cloud-native experience. There is no trade-off between cloud agility and sophisticated, multi-layered security. You get to experience the best of both worlds with natively integrated network security delivered as a service on Azure.

This guide explains how to configure and integrate Cloud NGFW into Azure Virtual Network(VNet) and Azure Virtual WAN(VWAN) infrastructure, enabling the users to utilize the benefits of Palo Alto Networks next-generation firewall as a service. The sections in the document provide details about the architecture and various



components of this service. This document also provides guidance on how to set up and configure Cloud NGFW using a simplified configuration workflow and explains how to route your application/spoke traffic through Cloud NGFW.

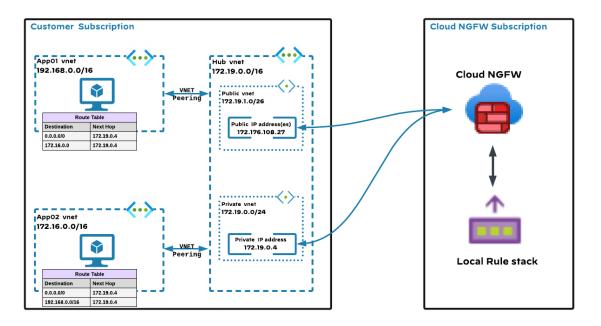


# Integrate Cloud NGFW into Azure Virtual Network(VNet) Infrastructure

# Pre-deployment of Cloud NGFW - setting up the VNet environment

## Topology

A hub-spoke topology is used as an example to route traffic through Cloud NGFW. Cloud NGFW supports all topologies.



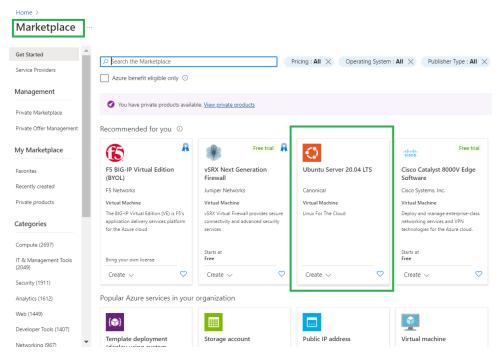
#### Integrate Cloud NGFW into Azure Virtual Network(VNet)

As per the above topology, in order to set up a lab environment, there should be a hub VNet, 2 spoke VNets and a virtual machine on one of those spoke VNets that's running a web server (apache2). Create this environment before creating and deploying the Cloud NGFW resources.

# Create Spoke VNets with a virtual machine on each of them

#### Create Spoke App01 VNet with Ubuntu Server

1. Go to <u>Azure Marketplace</u> and search for "<u>Ubuntu</u>" Server as shown below:



2. Choose this Ubuntu server and click 'Create' to start the creation of the Ubuntu server:



3. Fill in the details (Resource Group, VM Name, Region and the type of image while leaving other fields to default.) to complete the creation of the Ubuntu server. Make sure to choose the region appropriately based on Cloud NGFW service.

Home > Marketplace > Ubuntu Serve	r 20.04 LTS >					
Create a virtual machine						
Basics Disks Networking Ma	anagement Monitoring Advanced Tags Review + create					
Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more C <sup>3</sup>						
Project details						
Select the subscription to manage deploy your resources.	yed resources and costs. Use resource groups like folders to organize and manage a	all				
Subscription * ①	AzureTME	$\sim$				
Resource group * ①	(New) raviCngfwSpokeApp1RG					
	Create new					
Instance details						
Virtual machine name * 🛈	raviCngfwSpokeApp1	~				
Region * ①	(US) East US 2	$\sim$				
Availability options 🕕	No infrastructure redundancy required	$\sim$				
Security type 🕕	Standard	$\sim$				
Image * 🛈	Image * ① Ubuntu Server 20.04 LTS - Gen2					
	See all images   Configure VM generation					
VM architecture ①	Arm64					

4. In the networking section, select an existing VNet or create a new one in which this Ubuntu server will be installed:



Home > Marketplace > Ubuntu Server 20.04 LTS >					
Create a virtual machine					
Define network connectivity for your virtual	agement Monitoring Advanced Tags Review + create machine by configuring network interface card (NIC) settings. You can control ports, curity group rules, or place behind an existing load balancing solution.				
When creating a virtual machine, a network	interface will be created for you.				
Virtual network * ①	(new) raviCngfwSpokeApp1RG-vnet				
Subnet * 🕕	(new) raviCngfwSpokeApp1Subnet (192.168.0.0/24)				
Public IP ①	(new) raviCngfwSpokeApp1-ip				
NIC network security group ①					
Public inbound ports * ①	<ul> <li>Advanced</li> <li>None</li> <li>Allow selected ports</li> </ul>				

- 5. Review the configuration and create the server.
- 6. Once the Ubuntu server deployment is complete, install an apache server on it. To do this, go to the serial console of the created Ubuntu server and execute the commands below to install an apache server:

sudo apt update



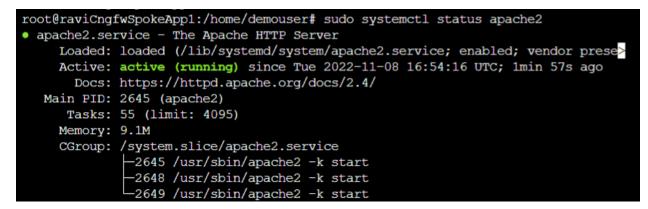
🔎 Search	« ? Feedback 🖸 🐯 🕛 🎟
Workbooks	The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the
Automation	individual files in /usr/share/doc/*/copyright.
🖧 Tasks (preview)	Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
Export template	applicable law.
Help	To run a command as administrator (user "root"), use "sudo <command/> ". See "man sudo_root" for details.
℅ Resource health	demouser@raviCngfwSpokeApp1:~\$
Boot diagnostics	demouser@raviCngfwSpokeApp1:~\$
Performance diagnostics	demouser@raviCngfwSpokeApp1:~\$ demouser@raviCngfwSpokeApp1:~\$ sudo su
💐 VM Inspector (Preview)	<pre>root@raviCngfwSpokeApp1:/home/demouser# root@raviCngfwSpokeApp1:/home/demouser#</pre>
🕈 Reset password	root@raviCngfwSpokeApp1:/home/demouser sudo apt update Hit:1 http://azure.archive.ubuntu.com/ubuncu focal inverse
Redeploy + reapply	Get:2 http://azure.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Ubuntu Advantage support alap	Get:3 http://azure.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB] Get:4 http://azure.archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]
plan	Get:5 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 Packages [862
🚺 Serial console	Get:6 http://azure.archive.ubuntu.com/ubuntu focal/universe Translation-en [512 Get:7 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadat
Connection troubleshoot	Get:8 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 C-n-1 Metadat Get:8 http://azure.archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [1

sudo apt install apache2

raviCngfwSpokeApp1   Serial console					
✓ Search «	? Feedback 🛛 🎼 🖽				
Logs     Connection monitor (classic)	<pre>root@raviCngfwSpokeApp1:/home/demouser# root@raviCngfwSpokeApp1:/home/demouser# sudo apt install apache2 Reading package lists Done Building dependency tree</pre>				
	Reading state information Done				

Confirm that the apache server installed successfully using the following command:

sudo systemctl status apache2





### Create Spoke App02 VNet with Ubuntu Server (For EW-traffic)

Repeat the above steps to create Spoke VNet2 with Ubuntu server.



## Deployment of Cloud NGFW into VNet Infrastructure

- 1. Now that the environment is set up, deploy the Cloud NGFW to protect the traffic coming from that hub VNet.
- 2. Login to <u>Azure portal</u><sup>1</sup> (*use this link only*) and search for "paloalto". This search displays the Cloud NGFW service by Palo Alto Networks:

≡	Microsoft Azure		
	Azu	All         Services (2)         Resources (1)         Resource Groups (1)         Marketplace (16)         Documentation (1)	
		Azure Active Directory (66)	
	C	Services	
re 🗞 Cloud NGFWs by Palo Alto Network		Cloud NGFWs by Palo Alto Networks 👼 Local Rulestacks for Cloud NGFW by Palo Alto Networks	

- **3.** Click "Cloud NGFWs" to start the creation of the Palo Alto Networks Cloud NGFW service for Azure.
- **4.** The following screen is the landing page for the Cloud NGFW resource. This screen populates all the available, pre-created Cloud NGFW instances (if not a first-time user). Click **Create** to start the creation of a Cloud NGFW resource:

$\leftrightarrow$ $\rightarrow$ C $\triangle$ $$ portal.azure.com/?Azure_Marketpla	ace_PaloAltoNetwork
$\equiv$ Microsoft Azure Restore default configuration $\checkmark$ Search resou	irces, services, and docs (G+,
Home >	
Cloud NGFWs & ··· Palo Alto Networks Inc. (paloaltonetworks.onmicrosoft.com)   PREVIEW	
$+$ Create 🐯 Manage view $\lor$ 🖒 Refresh $\downarrow$ Export to CSV $~\%$ Op	en query \mid 🧔 Assign ta
Filter for any field Subscription equals all Resource group	equals <b>all</b> X Location
Name ↑⊥	Resource arou

<sup>&</sup>lt;sup>1</sup> Deployment of Cloud NGFW can only be done through this private link. This portal has orange colored on the top unlike the typical blue color.



**5.** After clicking **Create**, the Create Palo Alto Networks Cloud NGFW screen appears. Use the information in the table below to populate basic information for your Cloud NGFW resource:

Subscription	Automatically selected based on the subscription used while logged in.
Resource Group	Use one of the existing resource groups or create a new resource group (by clicking the <b>Create New</b> option) in which the Cloud NGFW resource is created.
Firewall Name	Name of the Cloud NGFW Firewall resource.
Region	Region in which Cloud NGFW is provisioned. For this Private Preview, only US East-2 and US Central regions are supported.



≡ №	/licrosoft Azure	e Restore de	fault configuratic	n 🔎 Search re	esources, services, and do	cs (G+/)
	Cloud NGFWs		orks Clou	d NGFW		
Basics	Networking	Rulestack	DNS Proxy	Tags Terms	Review + create	
Some on	ne or two liner de	scription. Learn	more			
Project	details					
	ne subscription to all your resources		ed resources and	d costs. Use resou	rce groups like folders to	organize and
Subscrip	otion * 🛈		AzureTME			$\checkmark$
F	Resource group *	(i)	(New) raviDe Create new	moCngfwRG		$\sim$
Firewall	Details					
Firewall I	Name * 🗊		raviDemoCn	gfw		$\checkmark$
Region *	* (i)		East US 2			$\sim$
			_		1	
Review	w + create	< Previous	Next : Ne	tworking >		

6. Once the details are filled in, click Next: Networking > and provide information for your networking environment. Choose the Network Injection type from Virtual network and Virtual Wan Hub. (Virtual Wan Hub will be available from the end of November). Create a new virtual network or select an existing virtual network. You can also specify IP addresses. Specify the Source NAT option if Network Address Translation (NAT) is used on the traffic going out to the Internet:



Microsoft Azure Restore defa	ault configuration $P$ Search resources, services, and docs (G+/)					
Home > Cloud NGFWs >						
Create Palo Alto Netwo	Create Palo Alto Networks Cloud NGFW					
Basics Networking Rulestack	DNS Proxy Tags Terms Review + create					
Please configure your Firewall deployment	t with network requirements, i.e., Public IP CIDR and virtual network settings.					
Network Injection						
Type *	Virtual Network					
	🔘 Virtual Wan Hub					
Configure virtual networks						
Virtual Network * 🛈	(new) raviDemoCngfw-vnet					
	Create new					
Private Subnet * 🕠	(new) subnet1 (172.19.0.0/24)					
Public Subnet * 🕡	(new) subnet2 (172.19.1.0/26)					
Public IP Address Configuration						
Public IP Address(es) * 🔋	Create new					
	Use existing					
Public IP Address Name(s) * 🛈	raviDemoCngfw-public-ip					
Source NAT Settings	_					
Enable Source NAT (i)						
Use the above Public IP Address(es)						
Review + create < Previous	Next : Rulestack >					

7. Click Next: Rulestack > to create a Local Rule stack where rules can be defined. This is a placeholder for the local rule stack. After the creation of Cloud NGFW resource, this rulestack can be modified to add/edit rules, FQDN, and prefix list. If there is a Local Rule Stack that's already created, select it from the drop-down menu:



■ Microsoft Azure Restore d	efault configuration	$\mathcal{P}_{-}$ Search resources, services, and docs (G+/)
Home > Cloud NGFWs >		
Create Palo Alto Netw	orks Cloud NGF	W
Basics Networking Rulestack	DNS Proxy Tags Te	rms Review + create
Some description		
Choose a Local Rulestack * 🕕	Create new	
	<ul> <li>Use existing</li> </ul>	
Local Rulestack *	raviDemoCngfw-Irs	
	_	

Review + create <	IS Next : DNS Proxy >

8. Click Next: DNS Proxy > to configure Cloud NGFW as a DNS Proxy. It is disabled by default:



 ■ Microsoft Azure
 Restore default configuration
 P Search resources, services, and d

 Home > Cloud NGFWs >
 ■
 ■
 ■

 Create Palo Alto Networks Cloud NGFW
 …
 …

 Basics
 Networking
 Rulestack
 DNS Proxy
 Tags
 Terms
 Review + create

 DNS Proxy \* ①
 ①
 Disabled

Enabled

Review + create

< Previous

Next : Tags >



#### 9. Click Next: Tags > to specify tags as per your Azure requirements:

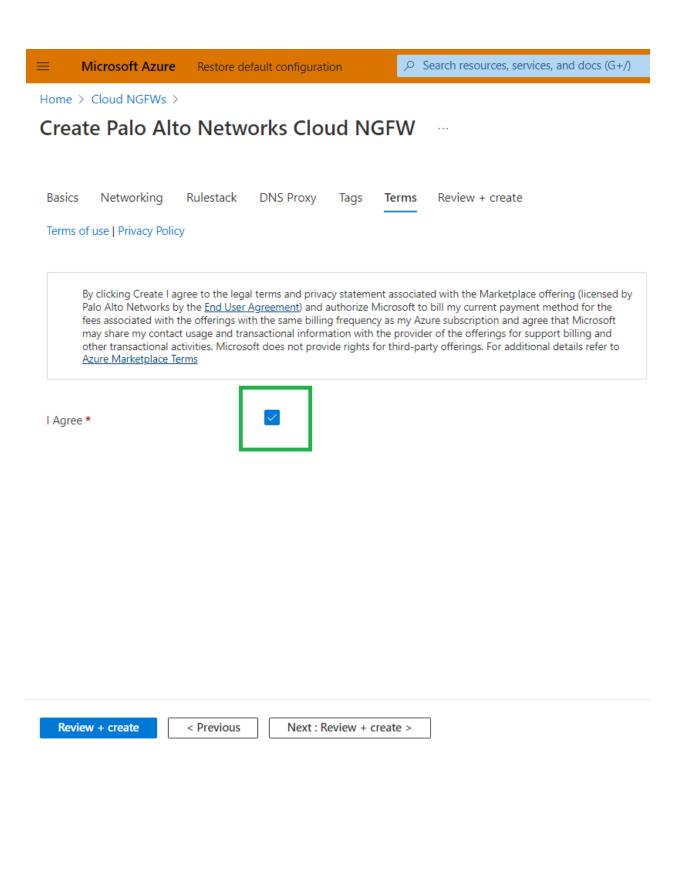
Microsoft Azure	Restore default configuration	$\wp$ Search resources, services, and docs (G+/)
ome > Cloud NGFWs >	Networks Cloud N	IGFW
Basics Networking	Rulestack DNS Proxy Tags	Terms Review + create
	nat enable you to categorize resourc d resource groups. Learn more abo	es and view consolidated billing by applying the same
		on other tabs, your tags will be automatically updated.
Name ①	Value ①	Resource
StoreStatusDND	: DND	7 selected V
		Select all
		Cloud NGFW
		Local Rulestack
		Microsoft.Network/virtualHub
		Network security group
		V Public IP address
		Virtual network
		Virtual WAN





10. Click Next: Terms > and accept the terms as shown below:





Strata by Palo Alto Networks | SW NGFW | Cloud NGFW for Azure - Private preview

🊧 paloalto<sup>®</sup>

 Click Next: Review + Create > and create a Cloud NGFW service. Like any other Azure native service, the resource is validated first and then created. Once the screen shows Validation Passed, click Create to deploy the Cloud NGFW service.



#### Home > Cloud NGFWs >

## Create Palo Alto Networks Cloud NGFW

🕑 Val	idation Passed								
Basics	Networking	Rulestack	DNS Proxy	Tags	Terms	Review + create			
Basics									
Subscrip	tion		AzureTME						
Resource	e group		raviDemoCng	fwRG					
Firewall	Name		raviDemoCng	ļfw					
Region			East US 2						
Networ	king								
Туре			Virtual Netwo	ork					
Virtual n	etwork		raviDemoCng	jfw-vnet					
Private S	Subnet		subnet1	subnet1					
Address	prefix (Private Su	bnet)	172.19.0.0/24						
Public Su	ubnet		subnet2						
Address	prefix (Public Sub	net)	172.19.1.0/26						
Public IP	Address(es)		Create new						
Public IP	Address Name(s)	)	raviDemoCng	gfw-public	c-ip				
Rulesta	ck								
Choose	a Local Rulestack		Create new						
Local Pu	lostack			fu lec					



< Previous



Strata by Palo Alto Networks | SW NGFW | Cloud NGFW for Azure - Private preview

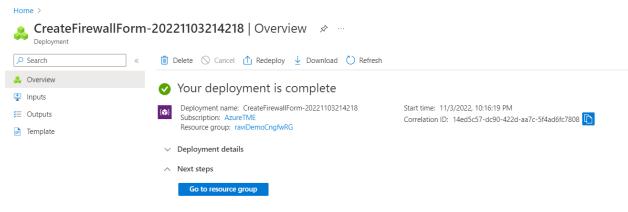
Next

After creating the Cloud NGFW service the deployment progress is displayed:

≡ м	Aicrosoft Azure	Restore default configuration	$\wp$ Search resources, services, and docs (G+/)		D. G
	reateFirewa	allForm-20221103214	218   Overview 🖈 …		
🔎 Search	:h	« 🔟 Delete 🚫 Can	cel 🖄 Redeploy 🞍 Download 💍 Refresh		
🙏 Overv	view	Deploym	ent is in progress		
😫 Inputs	ts	Depioyin	ent is in progress		
🃒 Outpu	uts	Deployment na     Subscription: /	ime: CreateFirewallForm-20221103214218 AzureTME	Start time: 11/3/2022, 10:16:19 PM Correlation ID: 14ed5c57-dc90-422d-aa7c-5f4	4ad6fc7808
📄 Templ	olate	Resource group	o: raviDemoCngfwRG		
		∧ Deployment deplo	atails		
		Resource	Туре	Status	Operation details
		📀 raviDemo(	Cngfw-vnet Microsoft.Network,	virtualNetworks OK	Operation details
		📀 raviDemo(	Ingfw-Irs PaloAltoNetworks.	Cloudngfw/localRulest OK	Operation details
		📀 raviDemo(	Engfw-vnet-nsg Microsoft.Network,	'networkSecurityGroups OK	Operation details
		📀 raviDemo(	Ingfw-public-ip Microsoft.Network	/publicIPAddresses OK	Operation details

#### The deployment of a Cloud NGFW takes approximately 30 minutes.

On a successful deployment, the screen below appears. Click Go to resource group to verify the resources created for this deployment:



**12.** There are five resources created, which include Cloud NGFW, Local Rule stack, Public IP address, Virtual Network, and security group:



Microsoft Azure Restore de	fault configuration ,P Search resources, services, and docs (G+/)		D 🕼 Q 🖗 🖓 🕂
Home > CreateFirewallForm-2022110			
raviDemoCngfwRG	i		
✓ Search «	+ Create 🐵 Manage view 🗸 📋 Delete resource group 🖒 Refresh 🞍 Export to CSV 📍	$\%$ Open query $\mid$ $\oslash$ Assign tags $ ightarrow$ Move $\checkmark$ $ ilde{\mathbb{II}}$ Delete	🛓 Export template 🔋 Open in
(•) Overview			
Activity log	Subscription (move) : AzureTME	Deployments : 1 Succeeded	
Access control (IAM)	Subscription ID : 0683d406-4d77-4bb7-b1a6-165c282b5d37	Location : East US 2	
🗳 Tags	Tags (edit) : Click here to add tags		
A Resource visualizer			
🗲 Events	Resources Recommendations		
Settings	Filter for any field Type equals all $\times$ Location equals all $\times$ $^{+}_{\nabla}$ Add filter		
1 Deployments	Showing 1 to 5 of 5 records. Show hidden types		No grouping
Security	Name ↑↓	Type ↑↓	Location ↑↓
Policies		Cloud NGFW	East US 2
Properties	invibencengi	Local Rulestack	East US 2
🔒 Locks	invibemoCngtw-jirs	Public IP address	East US 2
Cost Management	and ravibernocingiw-public-ip	Virtual network	East US 2
S Cost analysis	very ravibemocngiw-vnet	Network security group	East US 2
Cost alerts (preview)		Network security group	Edst US 2
Budgets			
Advisor recommendations			
Monitoring	< Previous Page 1 v of 1 Next >		

**13.** Once the Cloud NGFW resource is created, click on it to verify that the Provisioning state shows **Succeeded**. This screen also displays Public and Private IP addresses that are associated with the Cloud NGFW service. Use this information in further steps of this document to route traffic through the Cloud NGFW service:

Microsoft Azure Restore de	efault configuration	ch resources, services, and docs (G+/)		Σ 🗗 Ω
Home >				
raviDemoCngfw Cloud NGFW   PREVIEW	☆ ☆ …			
	🖒 Refresh 📋 Delete			
overview	→ Essentials			
<ul> <li>Activity log</li> </ul>	Resource group (move) : raviDem	oCngfwRG	Resource id : /subscr	riptions/0683d406-4d77-4bb7-b1a
Access control (IAM)	Location : East US 2	2	Type : paloalt	onetworks.cloudngfw/firewalls
🖉 Tags	Subscription (move) : <u>AzureTN</u>	E	Public IPs : 172.17	6.108.27
	Subscription ID : 0683d40	6-4d77-4bb7-b1a6-165c282b5d37	Private IPs : 172.19	.0.4
Settings			Source NAT Public IPs : 172.17	6.108.27
Networking & NAT	Tags (edit) : StoreSt	atusDND : DND		
Rulestack				
Log Settings	Get started Properties Re	ecommendations		
DNS Proxy				
🖶 Rules	PaloAltoNetworks.Clouding	gfw firewall	DNS settings	
Properties	Identity 🛈		Enable DNS proxy 🛈	DISABLED
A Locks	System data 🛈	View value as JSON	Enabled DNS type 🛈	CUSTOM
	Properties		DNS servers ①	
Vonitoring			Plan data	
II Alerts	ETag ()	36921c84-5b97-11ed-8db2-0a6ebcacd256	Usage type ①	PAYG
	Front end settings ① Provisioning state ①	Succeeded	Billing cycle ①	MONTHLY
Automation	Provisioning state ()	Succeeded	Plan id ①	cloud-ngfw-payg
			Flairiu	cloud-ligtw-payg
Tasks (preview)	🙊 Network profile		Effective date ①	1/1/1 5-53-28 AM
Automation Tasks (preview) Export template	Xetwork profile	View value as JSON	Effective date 🛈	1/1/1, 5:53:28 AM



## Post Deployment of Cloud NGFW

## **Create/Update Rule stack**

1. To update/edit the rulestack, click the **Rulestack** option available in the Cloud NGFW resource. As shown below, this displays the rulestack associated with the cloud NGFW service along with the resource group:

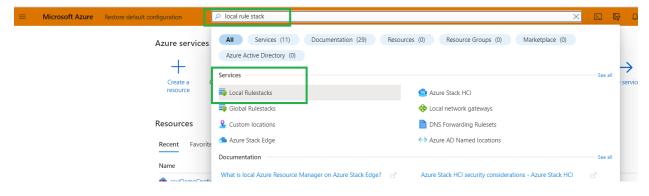
■ Microsoft Azure Restore defau	It configuration	∠ Search resources, services, and docs (G+/)
Home > raviDemoCngfw		
<b>raviDemoCngfw</b>   Ru	lestack …	
	🕐 Refresh	
💩 Overview		
Activity log	Rulestack	
Access control (IAM)	Local Rulestack *	raviDemoCngfw-Irs, raviDemoCngfwRG 🗸
🧳 Tags		Currently associated rulestack: raviDemoCngfw-lrs, region: eastus2
Settings		
↔ Networking & NAT		
👼 Rulestack		
Log Settings		
DNS Proxy		
💺 Rules		
III Pronerties		

The Local Rulestack is now associated with **raviDemoCngfw-Irs**.

Next, modify this rulestack to add firewall rules to allow some traffic and block specific traffic.

#### By default Cloud NGFW blocks all traffic.

2. Search for Local Rulestack service in the global search of the Azure portal:





Click the Local Rulestacks service to navigate to the list of local rulestacks associate with your Cloud NGFW subscription.

Within this page search for **raviDemoCngfw-Irs**, the local rulestack associated with the Cloud NGFW service created in the previous step:

=	Microsoft Azure	Restore default configuration		vices, and docs (G+/)				۶.	₽	Q	ø	?	8 . r	pegada@palo ALO ALTO NETWOS
Hor	ne >													
	Alto Networks Inc. (paloalto	5 & ∽ ···· onetworks.onmicrosoft.com)   PREVIEW												
+	Create 🔅 Manage vi	ew 🗸 🖒 Refresh 🞍 Export to CSV	🛚 😤 Open query 📔 ⊘	Assign tags 📋 Delete										
rav	viDemoCngfw-Irs	Subscription equals all Resou	arce group equals all $ imes$	Location equals all $ imes$	+ Add filter									
		-							1	No grou	ping		~	≡≡ List viev
	Name 🛧			Resource group $\uparrow\downarrow$		Location $\uparrow\downarrow$	Subscription	ID ↑↓				Sta	ite ↑↓	
	raviDemoCngfw-Irs			raviDemoCngfwRG		East US 2	0683d406-4c	177-4bb7-	b1a6-16	55c282b	5d37	Suc	cceeded	

Verify the state of this Local rulestack **Succeeded**.

**3.** Click your rulestack(raviDemoCngfw-Irs) to add rules as shown below. Modify the rules as per your use cases and functionality. Add a rule to allow traffic. Fill in the mandatory fields and use the default settings for the remaining fields:

Microsoft Azure Restore default conf	iguration 🦯 🖉 Search resources, servi	ices, and docs (G+/)		D 16 0 8
Home > Local Rulestacks > raviDemoCngfw-Irs Local Rulestacks « Palo Alto Networks Inc. (paloattonetworksonmicr			Add Rule Define Rule Parameters General	AllowAllTraffic
+ Create <sup>®</sup> Manage view ∨ ···· raviDemoCngfw-Irs Name ↑. ■ raviDemoCngfw-Irs ···	Search     «     Overview     Activity log     Access control (IAM)     Tags	C Refresh  LocalRule Header  LocalRule Description  + Add Delete	Name * Description Priority * Enabled Source Match Criteria	AllowAlltraffic           200           Image: Constraint of the second se
	Settings III Properties Characteristics	Priority Nam No data is available	Destination Match Criteria	Match
	Resources Prefix List FQDN List Rules	4	Granular Controls Application Match Criteria	Match  Any Select
	Profiles Deployment Monitoring Alerts		URL Category Match Criteria Protocol & Port	Any     Select
< Page 1 v of 1 >	Automation		Match Criteria Validate Cancel	Application Default     Any

Enable logging as part of the rule configuration, as shown below:



Microsoft Azure Restore default config	guration	℅ Search resources, set	vices, and docs (G+/)			Σ 🔂 🗅
Home > Local Rulestacks > raviDemoCngfw-Irs Local Rulestacks « Palo Alto Networks Inc. (paloaltonetworks.onmirc + Create ③ Manage view ~ ····		DemoCngfw-Irs	Refresh		Add Rule Define Rule Parameters Destination Match Criteria	Any
raviDemoCngfw-Irs Name ↑↓ ■ raviDemoCngfw-Irs ····	Overview     Activity log     Access cor     Tags		LocalRule Head LocalRule Description + Add I Delete	der	Granular Controls Application Match Criteria	Match  Any Select
	Settings Properties		Priority	Nam	URL Category Match Criteria	<ul> <li>Any</li> </ul>
	Locks Resources		No data is available	-	Protocol & Port Match Criteria	Select     Application Default
	Prefix List					Any     Select
	<ul> <li>Rules</li> <li>Profiles</li> <li>Deployment</li> </ul>	nt			Actions Actions	<ul> <li>Allow</li> </ul>
	Monitoring					<ul> <li>Deny</li> <li>Drop</li> <li>Reset both client and server</li> </ul>
	Automation	view)			Egress Decryption Logging	
< Page 1 v of 1 >	Export tem				Validate Cancel	

Click Validate and then Add to incorporate the rule.

**4.** Add an FQDN list that includes Facebook, and use this list to add a rule to block facebook.com:

Microsoft Azure Restore default conf	figuration 🖉 S	Search resources, servi	ices, and docs (G+/)			Σ 🔂 🗅	© ©	ন্দ	rpegada@paloalto PALO ALTO NETWORKS II
Home > Local Rulestacks > raviDemoCngfw-Irs	📻 raviDem	oCngfw-Irs	FQDN List	Add FQDN List Enter a fully-qualified domain name (FQDN)	to create an FQDN objec	t.			
Palo Alto Networks Inc. (paloaltonetworks.onmicr + Create 🛞 Manage view 🗸 …	Local Rulestack	«	🕐 Refresh	Name * Description	Facebook				
raviDemoCngfw-Irs Name ↑↓	<ul> <li>Overview</li> <li>Activity log</li> </ul>		FQDN List	FQDN *	www.facebook.cor	n			
raviDemoCngfw-Irs	Access control (IAN	M)	An Fully-Qualified Domain Names (FC enforcement. Because FQDNs can be translated to different IP addresses. + Add Delete		Enter one value pe	r line.		4	
	Settings	- 1	Name						
	Resources	- 1	No data is available						
[	FQDN List								
	<ul> <li>Profiles</li> <li>Deployment</li> </ul>	- 1							
	Monitoring	- 1							
	Automation	- 1							
< Page 1 v of 1 >	🚦 Tasks (preview) 🛃 Export template			Add Cancel					

Facebook now appears in the **FQDN List**:



Microsoft Azure Restore default conf	iguration R Search resources,	services, and docs (G+/)		N 🗣 Q 🛞 🕐 ;	rpegada@paloaltonetw
Home > Local Rulestacks > raviDemoCngfw-Irs	5				
Local Rulestacks « Palo Alto Networks Inc. (paloaltonetworks.onmicr	raviDemoCngfw-I	rs   FQDN List			×
🕂 Create 🔞 Manage view 🗸 \cdots	₽ Search	K C Refresh			
raviDemoCngfw-irs Name ↑↓  arraviDemoCngfw-irs	Overview     Activity log     Activity log     Access control (IAM)     Tags Settings		an be translated to many different IP addres	allows you to group specific source or destination FQDN that s, using an FQDN object is more efficient than specifying IP a	
	Properties	Name	FQDN	Description	
	A Locks	Facebook	www.facebook.com		

Return to the Rules setting page and add a rule that matches the FQDN list created. Set the action to **Drop** to block Facebook traffic:

■ Microsoft Azure Restore default conf	iguration 🖉 Search resources,	services, and docs (G+/)			D 🕼 🗅	© R	rpegada@pa PALO ALTO NETV
Home > Local Rulestacks > raviDemoCngfw-Irc Local Rulestacks « Palo Alto Networks Inc. (paloaltonetworks.onmicr + Create @ Manage view ~ ····		Irs   Rules ····	Add Rule Define Rule Parameters General Name *	BlockFacebook			
r Cleate ⊗ Manage New ♥ ravDemoCngfw-Irs Name ↑↓	Conview Convi		Description Priority * Enabled Source Match Criteria Destination	Incollection     Incollection     Incollection     Incollection     Any     Match     Any     Match			
	FQDN List  Kules  Profiles  Deployment  Monitoring		Countries Prefix List FQDN List Destination Exclude Granular Controls Application Match Criteria	Prefix List FQDN List Facebook Destination Exclude Granular Controls Application	~ ~ ~		
	Alerts Automation Cartainers Automation		URL Category Match Criteria	Select			



Add Rule Define Rule Parameters	
Prefix List	
FQDN List	Facebook
Destination Exclude Granular Controls	
Application	
Match Criteria	<ul> <li>Any</li> </ul>
	◯ Select
URL Category Match Criteria	
Match Criteria	Any
	Select
Protocol & Port	
Match Criteria	Application Default
	Any
	Select
Actions	
Actions	Allow
	Deny
	Drop
	Reset both client and server
Egress Decryption	
Logging	

5. Both the rules appear as shown below:



	« 💍 Refre	esh					
Overview	<b>A</b>						
Activity log	Loc	calRule H	eader				
Access control (IAM)		Rule Description					
🗳 Tags	+	Add 📋 Delete					
Settings	0	Priority	Name	Source	Destination	Constraints	Action
Properties		200	AllowAllTraffic	any	any	no/yes	Allow
🔒 Locks		200				,) ==	
Resources		100	BlockFacebook	any	match	no/yes	DenyReset
Prefix List	4						
FQDN List							
- Rules							

**6.** As part of this Cloud NGFW service, the security profiles are enabled with best practice configurations by default. This means that the traffic is secured with the best security profiles from day one, once the Cloud NGFW is deployed in the network:

h 🤍 🖁 Sar	ve 💍 Refresh	
iew IP	S and Spyware	Threats Protection
ty log		
control (IAM)	Vulnerability	is a network security and threat prevention technology that examines traffic flow to detect and pr
Enab		
Profi		Best Practice
An	ti-Spyware	
	-spyware protection zeroes in ou	tbound threats, especially command-and-control (C2) activity, where an infected client is being le
Enab	ble	
Profi	le	Best Practice V
М	alware and File	e-based Threat Protection
141		
	tivirus	prms, and trojans as well as spyware downloads.
Antiv		
	ble	Best Practice
Antiv Enab Profi	le	
) File	e Blocking	



7. Now that the rules have been modified, they should be deployed onto the Local rulestack associated with the Cloud NGFW service. Click the **Deployment** tab to see the page below. The deployment status displays as **Candidate**, which means the configuration was built but not deployed. Next, click **Deploy Configuration** to deploy the configuration onto the Cloud NGFW service. It is mandatory to do this step as without this the configuration will not be deployed onto the rulestack.

₽ Search	« 🕐 Refresh			
Overview	•			
Activity log	Deployn	nent		
Access control (IAM)				
Tags	Status		Action	
Settings	Candidate		PPP Dealer Confirmation	No. 1
Properties			Deploy Configuration	7 Revert
🖞 Locks				
Resources				
Prefix List				
FQDN List				
- Rules				
🔋 Profiles				
Deployment				
Monitoring				

After clicking **Deploy Configuration,** a pop-up displays the firewalls associated with this rulestack. Click **Deploy** to configure this rulestack on all the associated firewalls:



raviDemoCngfw-Irs	Deployment	
♀ Search «	🕐 Refresh	
Overview		
Activity log	Deployment	
Access control (IAM)		
🗳 Tags	Status	Action
Settings	Candidate	Revert
Properties		
🔒 Locks		Deploy ×
Resources		Push your configured rulestacks to your firewalls.
Prefix List		Associated Firewalls (1) to this rulestack
🧮 FQDN List		raviDemoCngfw(raviDemoCngfwRG)
🗲 Rules		
💼 Profiles		Deploy
📩 Deployment		
Monitoring		
III Alerts		
Automation		

After successfully deploying the configuration, the screen displays the deployment status as **Running** 

Search	« 🕐 Refresh			
Overview	<b>A</b>			
Activity log	Deployment			
Access control (IAM)				
Tags	Status	Actio	on	
tings	Running			0.0
Properties		<u>5</u> 2	Deploy Configuration	7 Revert
Locks		-		
sources				
Prefix List				
FQDN List				
Rules				
Profiles				
Deployment				

With this, the Cloud NGFW and Local rulestack are successfully deployed.



## Source/Destination NAT rule on Cloud NGFW

Configure a destination NAT rule with frontend configuration on Cloud NGFW to take care of Inbound traffic towards App1 or App2 present on spoke VNet1 or spoke VNet2.

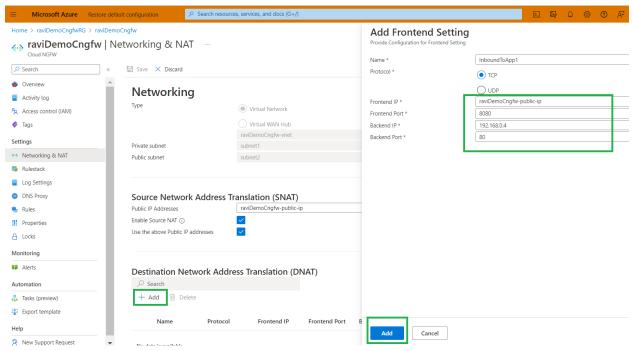
- Access the Networking & NAT settings screen for the loud NGFW resource. The first thing to observe is whether the Source NAT setting has been enabled or not. During the creation of the Cloud NGFW resource, (step 6) if Source NAT was enabled, that's how it will show up here.
- 2. Click **Edit** to add the Destination NAT rule.

	efault configuration	$\mathcal{P}$ Search resources, services, and docs (G+/)
Home > raviDemoCngfwRG > raviDe	moCngfw	
raviDemoCngfw   N Cloud NGFW	Networking & N	AT
✓ Search «	🖉 Edit 💍 Refresh	
<ul> <li>Overview</li> <li>Activity log</li> </ul>	Networkir	ıg
Access control (IAM)	Туре	Virtual Network
Tags		Virtual WAN Hub
Settings	Private subnet	raviDemoCngfw-vnet subnet1
<ul> <li>Networking &amp; NAT</li> </ul>	Public subnet	subnet2
📪 Rulestack		
Log Settings		
DNS Proxy	Source Netwo	rk Address Translation (SNAT)
💺 Rules	Public IP Addresses	172.176.108.27
Properties	Enable Source NAT 🕕	$\checkmark$
🔒 Locks	Use the above Public	P addresses
Monitoring		
II Alerts	Destination N	etwork Address Translation (DNAT)
Automation	✓ Search	
🔒 Tasks (preview)		

3. Add a **Destination NAT** rule with frontend configuration as shown below. Frontend IP is the Public IP address associated with Cloud NGFW (choose this from the drop-down menu). To access Appl (192.168.0.4), <u>deployed</u> on spoke VNet1, on port 80(HTTP), we are going to use Cloud NGFW frontend IP address



and port 8080. After adding the Destination NAT rule, save the configuration by clicking **Add** .



Once the destination NAT rule has been added, click **Save** to deploy this configuration on to the Cloud NGFW resource:



Microsoft Azure Restor	re default configuration	Search resources, s	ervices, and docs (G+/)			
Home > raviDemoCngfwRG > rav	viDemoCngfw					
raviDemoCngfw      Cloud NGFW	Networking & NAT					
	« 🛛 🗟 Save 🗡 Discard					
Overview	Networking					
Activity log	Туре		Virtual Network			
Access control (IAM)			Virtual WAN Hub aviDemoCngfw-vnet			
Settings	Private subnet		ubnet1			
Networking & NAT	Public subnet	S	ubnet2			
📮 Rulestack						
Log Settings					-	
DNS Proxy	Source Network		. ,			
Rules	Public IP Addresses	ra	aviDemoCngfw-public-ip	$\sim$		
Properties	Enable Source NAT  Use the above Public IP ac	Idresses				
ြ Locks	ose the above rubile in ac	•				
Monitoring						
Alerts	Destination Net	vork Address	Translation (DNAT)			
Automation	✓ Search					
Tasks (preview)	+ Add 🗎 Delete	2				
Export template	Name	Protocol	Frontend IP	Frontend Port	Backend IP	Backend Port
Help	Jahour JT- Arr-1	TCP	raviDomoCostiv public :-	8080	192 168 0.4	80
Rew Support Request	InboundToApp1	TCP	raviDemoCngfw-public-ip	8080	192.168.0.4	80

With this configuration in place, the address <u>http://frondendIP:8080</u> is redirected to App1 on port 80 through Cloud NGFW. This means that inbound traffic is now flowing through the Cloud NGFW.

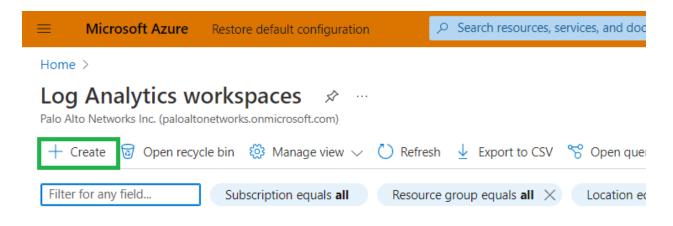
## **Configure Logging**

**///** paloalto<sup>®</sup>

 Before configuring Log settings on Cloud NGFW, create the Log Analytics workspace on Azure. Search for Azure Log Analytics workspace as shown below and click Log Analytics Workspaces service to add it to the workspace:

Azure services  All Services (22) Marketplace (1) Documentation (30) Resources (0)  Azure Active Directory (0)  Services  Documentation (30) Resources (0)  Azure Active Directory (0)  Services  All Services  All Cogic apps	≡	Microsoft Azure	Restore default configuration			
Create a resource Log Analytics workspaces			Azure services	All Services (22)	Marketplace (1)	Documentation (30) Resources (0)
Create a resource Log Analytics workspaces				Azure Active Directory (0)		
resource 😰 Log Analytics workspaces				Services		
🗐 Activity log 🗛 Logic apps				Log Analytics workspaces		Audit Logs
				Activity log		📥 Logic apps

2. Click on Create option to create a new Log Analytics Workspace.



3. Create the **Log analytics workspace** as shown below. Make sure that the region is either US-East-2 or US-central:



≡ Micr	osoft Azure	Restore defa	ult configuration	,	n resources, services, and docs	(G+/)
Home > Log	Analytics wor	kspaces >				
Create	Log Ana	ytics wo	orkspace …			
Basics Ta	igs Review	+ Create				
~ ~			management unit of Azure M .og Analytics workspace. <u>Lear</u>		There are specific considerations	×
	vironments for	-			m your monitored resources ir jical storage unit where your lo	
Project deta	ails					
	bscription to m our resources.	anage deploye	d resources and costs. Use	resource gro	oups like folders to organize ar	nd
Subscription	* (i)		AzureTME			$\sim$
Reso	urce group * 🤅	D	(New) raviCngfwLogWor	kspaceRG		$\sim$
			Create new			
Instance de	taila					
Name * (i)	tans	— Г	raviCngfwLogWorkspace			~
Region * 🛈			East US 2			~
Review +	Create	« Previous	Next : Tags >			

4. Now configure Cloud NGFW Log settings using the Log Analytics workspace created above. Go to the Cloud NGFW resource, select the **Log Settings** section, and click the **Edit** option to choose the Log analytics workspace that has just been created:



#### Home > raviDemoCngfwRG > raviDemoCngfw

raviDemoCngfw   Cloud NGFW	Log Settings	
	« 🖉 Edit 💍 Refresh	
💩 Overview	A	
Activity log	Log Settings	
Access control (IAM)	Log Settings	No log settings found
🧳 Tags		
Settings		
Networking & NAT		
💐 Rulestack		
Log Settings		
DNS Proxy		
🍨 Rules		

5. Enable **Log Settings** and choose the log analytics workspace created in the previous step from the drop-down, and save the configuration:

Home > raviDemoCngfwRG > raviDe	emoCngfw	
<b>raviDemoCngfw</b>	Log Settings	
🔎 Search 🛛 «	🔚 Save 🗙 Discard	
👩 Overview		
Activity log	Log Settings	
Access control (IAM)	Enable Log Settings	
🗳 Tags	Log Settings	raviCngfwLogWorkspace V
Settings		
Networking & NAT		
Rulestack		
Log Settings		
ONS Proxy		
L Rular		



#### **Update Network Security Group**

Next, update the network security group that was created as part of the Cloud NGFW deployment. This security group is associated with both the Private and Public subnet as part of Hub VNetin the Customer Subscription (refer to the topology).

 Allow traffic as per Frontend/Destination NAT rule configuration. Also, allow HTTP and HTTPS traffic so that the Internet can be accessed from Application VNets through Cloud NGFW:

Microsoft Azure Restore default	configuration	. ○ Search resources, services, ar	nd docs (G+/)					🔄 🕼 🗘 🍥 🕢 R 🔤 sit
Home > Network security groups > raviCk Network security g « Palo Alto Networks Inc. (paloaltonetworks.onmicr	udNGFW-vnet-nsg	<b>vnet-nsg</b>   Inbound	d security rules	<b>;</b> ☆ …				Add inbound security rule         ×           revicCoudt/GPW-vnet-rigg         •
$+$ Create $\ \otimes$ Manage view $\lor \ \cdots$		« 🕂 Add 🧠 Hide defa	ult rules 💍 Refresh 🛛	🗊 Delete 🛛 🛱 G	ve feedback			Destination ①
Filter for any field	💎 Overview	Network security group se						Any 🗸
Name 1.	Activity log	and direction as an existing	g rule. You can't delete del	ault security rules,	but you can override th	em with rules that hav	e a higher	Service ① Custom ✓
basicNsgbpTrustIntf	Access control (IAM)	P Filter by name		Port == all	Protocol == all	Source == all	Destin	
basicNsgbpUntrustIntf	🧳 Tags	Priority 1	Name ↑↓	Por	t Tu	Protocol 1		Destination port ranges * 8080.80.443
bpController-nsg	/ Diagnose and solve problems	65000	AllowVnetInBou	nd Any		Any		Protocol
BreakingPointVM-nsg	··· Settings	65001		BalancerinB Any		Any		Any
CloudNGFWDemo-vnet-nsg	Inbound security rules	65500	DenvAllInBound			Any		• TCP
CNGFWSpoke1-nsg	📩 Outbound security rules		benyrainboana					OUDP
CNGFWSpoke2-nsg	··· 🕼 Network interfaces							
DefaultNSG	··· Subnets							Action
💎 raviCloudNGFW-vnet-nsg	··· Properties							Deny
💎 Srv-Work-nsg	🔒 Locks							- ·
🜒 workserver2-nsg	Monitoring							Priority * ① 100
	Alerts							Name *
	Diagnostic settings							AllowAnyCustom8080-80-443Inbound
	P Logs							Description
	NSG flow logs							
	Automation							
	Tasks (preview)							
< Page 1 V of 1 >	Export template							Add Cancel

2. Click Add to incorporate this inbound security rule:

Search	🛛 🕂 Add 👒 Hide def	ault rules   Refresh 📋 Delete 🛛 🖓 Give feed	lback				
Overview Activity log		ecurity rules are evaluated by priority using the comb lete default security rules, but you can override them			protocol to allow or deny the	e traffic. A security rules can't l	have the same priority and dir
Access control (IAM)	Filter by name	Port == all Pr	otocol == all Sou	ce == all Destination == all	Action == all		
ags	Priority 1	Name ↑↓	Port ↑↓	Protocol 1	Source ↑↓	Destination ↑⊥	Action ↑⊥
		Hame To	Tott To	11010001 10	bounce r.p	bestination 14	raan iy
iagnose and solve problems	100	AllowAnyCustom8080-80-443Inbound	8080,80,443	TCP	Any	Any	Allow
	<b>100 65000</b>	AllowAnyCustom8080-80-443Inbound AllowVnetInBound	8080,80,443 Any	TCP Any	Any VirtualNetwork	Any VirtualNetwork	<ul> <li>Allow</li> <li>Allow</li> </ul>
iagnose and solve problems gs ibound security rules		· · · · · · · · · · · · · · · · · · ·					

These steps ensure that appl on spoke VNetl can access the Internet.



# Configure VNetpeering between Hub Vnet(that got created during Cloud NGFW creation) and Spoke Vnets

- Configure VNet peering between spoke VNet1 and Hub VNet. Search for the spoke-VNet1 and select the **Peerings** section. Click **Add** to create a new peering.
- 2. While adding a peer, give it a name and leave the rest to default settings. Choose the hub virtual network (as peering is from spoke-vnet1) that has to be peered.

raviDemoApp1_gro Virtual network	oup-vnet   Peerings 🛛 🛧 🗠			
	🕂 Add 💍 Refresh \mid 🖏 Sync			
🛖 Firewall				
Ø Microsoft Defender for Cloud	Filter by name	Peering status == all		
😚 Network manager	Name ↑↓	Peering status ↑↓	Peer ↑↓	Gateway transit ↑↓
DNS servers	CngfwDemoApp1ToHubVnet	Connected	raviDemoCngfw-vnet	Disabled
Peerings				
2 Service endpoints				
Private endpoints				
III Pronerties	1			

3. Configure VNetpeering between spoke-VNet2 and Hub VNet by repeating the steps above.

	~	🕂 Add 💍 Refresh 🛛 💭 Sync			
Microsoft Defender for Cloud					
Network manager		Filter by name	Peering status == all		
DNS servers		□ Name ↑↓	Peering status ↑↓	Peer ↑↓	Gateway transit ↑↓
Peerings		CngfwDemoApp2ToHubVnet	Connected	raviDemoCngfw-vnet	Disabled
Service endpoints					
> Private endpoints					
Properties					

#### Add a Route Table to route traffic through Cloud NGFW

- Create a route table by searching for the Route table in the Azure search bar. Then, click Create to establish a new route table. Fill in the necessary fields and click Review+create to create a route table.
- 2. After creating the route table, select the **Subnets** section and associate it with the Appl subnet from spoke-vnetl:



Home > Route tables > CNGFWSpoke1RT						
Route tables « Palo Alto Networks Inc. (paloaltonetworks.onmicr	CNGFWSpoke1RT   S Route table	Subnets 🛪 …				×
+ Create 🛞 Manage view 🗸 …		+ Associate				
Filter for any field	🖄 Overview	✓ Search subnets				
Name 1	Activity log	Name ↑↓	Address range $\uparrow_{\downarrow}$	Virtual network ↑↓	Security group ↑↓	
A BPClientToSvr ····	Access control (IAM)	Default	192.168.0.0/24	CNGFWSpoke1RG-vnet		
CNGFWSpoke1RT ····	🗳 Tags					
CNGFWSpoke2RT ····	Diagnose and solve problems					
🐁 Firewall-route	Settings					
🐁 raviRouteTB2 …	Configuration					
🐁 SvrToClient 🚥	🖄 Routes					
	<ul> <li>Subnets</li> </ul>					
	Properties					
	🔒 Locks					
	Monitoring					
	Alerts					
	Automation					
	🖧 Tasks (preview)					
	😫 Export template					
	Support + troubleshooting					
	Effective routes					
	Request					
< Page 1 > of 1 >						<u>A</u> 1 🔀

3. Configure the default route (for outbound traffic) and route towards the App2 subnet (for east-west traffic) with the next hop as the Cloud NGFW private IP address:

App1RouteTable 🖉	* 🛧 …				×
✓ Search «	$ ightarrow$ Move $\lor$ 📋 Delete 🕐 Refresh   $\sharp$	Give feedback			
🐴 Overview 🔶					JSON View
Activity log	Resource group (move) : raviDemoApp1_group		Associations : 1 subnet associations		
Access control (IAM)	Location : East US 2				
< Tags	Subscription (move) : AzureTME				
Diagnose and solve problems	Subscription ID : 0683d406-4d77-4bb7 Tags (edit) : StoreStatusDND : DN				
Settings					
Configuration	Routes				
🐁 Routes					
Subnets	Name	↑↓ Address prefix	↑↓ Next hop type	↑↓ Next hop IP address	↑↓
Properties	DefaultRoute	0.0.0/0	Virtual appliance	172.19.0.4	
A Locks	RouteToApp2	172.16.0.0/16	Virtual appliance	172.19.0.4	
Monitoring	Subnets		-		
4 Alerts	♀ Search subnets				
	Name	↑↓ Address range	↑↓ Virtual network	↑↓ Security group	¢↓
Automation	raviDemoApp1Subnet	192.168.0.0/24	raviDemoApp1_group-vnet	· ·	•••
Tasks (preview)					
Export template					

 Similarly, associate one more route table with the App2 subnet from spoke-VNet2. Configure a default route (for outbound traffic) and route towards the App1 subnet (for east-west traffic) with the next hop as the Cloud NGFW private IP address:



App2RouteTable	> ☆ ···			
₽ Search «	$ ightarrow$ Move $\lor$ 📋 Delete 🖒 Refresh	R Give feedback		
🐴 Overview 🔺	↑ Essentials			
Activity log	Resource group (move) : raviDempApp2_group	1	Associations : 1 subnet associations	
Access control (IAM)	Location : East US 2			
Tags	Subscription (move) : AzureTME			
Diagnose and solve problems	Subscription ID : 0683d406-4d77-4bb7			
Settings	Tags (edit) : Click here to add tags Routes			
Configuration	✓ Search routes			
🐁 Routes	Name	↑↓ Address prefix	↑↓ Next hop type	↑↓ Next hop IP address
<ul> <li>Subnets</li> </ul>	DefaultRoute	0.0.0/0	Virtual appliance	172.19.0.4
Properties	RouteToApp1	192.168.0.0/16	Virtual appliance	172.19.0.4
🔒 Locks	Subnets			
Monitoring	Subnets			
III Alerts	Name	↑↓ Address range	↑↓ Virtual network	↑↓ Security group
Automation	default	172.16.0.0/24	raviDempApp2_group-vnet	
🖧 Tasks (preview)				
Export template				

# **Testing traffic**

#### **Test Inbound Traffic**

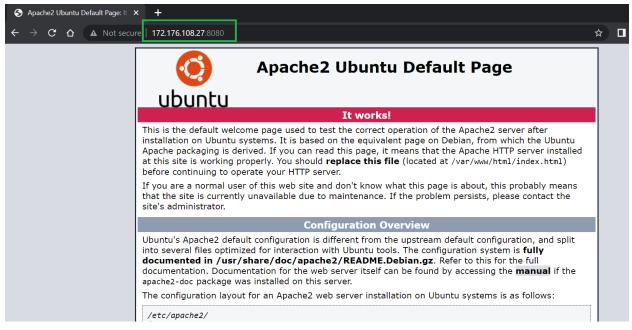
- 1. To validate the inbound connection towards App1, try to access <u>http://<Cloud</u> <u>NGFW Public IP>:8080.</u>
- 2. As per the Destination NAT configuration on Cloud NGFW, if <u>http://<Cloud</u> <u>NGFW Public IP>:8080</u> is accessed, the connection will be redirected to App1 after inspection by Cloud NGFW.

Make sure to allow HTTP traffic on the application server network interface. For this, go to Appl, select **Networking**, and add an inbound port rule that allows any HTTP inbound traffic. Configure the source as **IP Addresses**, port as 80, protocol as TCP, and set the **Action** to**Allow:** 



	🖉 Attach network int	terface 🧬 Detach network interface 🖗 Feedb	ack					
Overview	ravidemoapp1158							
Activity log	IP configuration ①							
Access control (IAM)	ipconfig1 (Primary)	$\sim$						
🖉 Tags	S Network Interfa	ce: ravidemoapp1158 Effective security rule	es Troubleshoot VM con	nection issues Topology (	)			
Diagnose and solve problems		et: raviDemoApp1_group-vnet/raviDemoApp1Subne				nabled		
ettings	Inhound port rules	Outhound post pilos     Application securit	to around to ad balancia	~				
ettings Networking Connect		s Outbound port rules Application securit y group raviDemoApp1-nsg (attached to networks, 1 network interfaces		~			Add inbou	nd port rule
Networking	Network securit	- y group raviDemoApp1-nsg (attached to networ		~	Source	Destination	Add inbou Action	nd port rule
Networking     Connect     Disks	Network security Impacts 0 subnet	<ul> <li>y group raviDemoApp1-nsg (attached to networ is, 1 network interfaces</li> </ul>	rk interface: ravidemoapp11!	58)	Source Any	Destination Any		nd port rule
t Networking Connect Disks Size	Network security Impacts 0 subnet Priority	- y group raviDemoApp1-nsg (attached to networ s, 1 network interfaces Name	rk interface: ravidemoapp11! Port	58) Protocol			Action	
Networking     Connect     Disks     Size     Microsoft Defender for Cloud	Network security Impacts 0 subnet Priority 310	y group raviDemoApp1-nsg (attached to networ s, 1 network interfaces Name AllowAnyHTTPInbound	rk interface: ravidemoapp11! Port 80	58) Protocol TCP	Any	Any	Action Allow	
Vetworking Vetworking Disks Size Vetworking Vetworking Size Vetworking Vetwo	Network securit Impacts 0 subnet Priority 310 65000	y group raviDemoApp1-nsg (attached to network s, 1 network interfaces Name AllowAnyHTTPInbound AllowVnetinBound	rk interface: ravidemoapp11! Port 80 Any	58) Protocol TCP Any	Any VirtualNetwork	Any VirtualNetwork	Action Allow Allow	

If <u>http:/<Cloud NGFW Public IP>:8080/</u> is accessed, the following screen appears if the apache server was running as the default web server. Here, once the public IP of the Cloud NGFW was accessed, it will redirect the traffic to App1 on spoke-vnet1 where apache server was running. Since Inbound HTTP is enabled on App1, it will run the apache server that was deployed on App1.

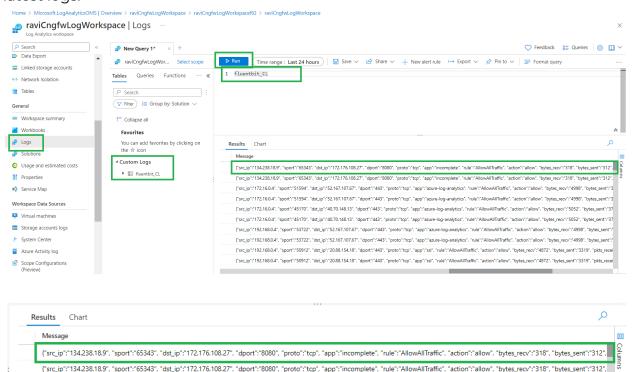




#### Accessing logs

To verify that this particular inbound traffic was processed correctly by Cloud NGFW, go to the **Log Analytics workspace** and verify the logs as shown below.

Within Log analytics workspace **raviCngfwLogWorkspace**, navigate to the **Logs** section, select **Custom Logs** and select **fluentbit\_CL** and run the query to get the latest logs:



("src.jp':'172.16.04", 'sport':'51594", 'dst.jp':'52.167.107.67", 'dport':'443", 'proto':'tcp', 'app':'azure-log-analytics', 'rule':'AllowAllTraffic', 'action':'allow', "bytes\_recv':'4998", "bytes\_sent':'3

From the log, it can be seen that the source IP address is the IP address of the machine from which the request originated, and the destination IP address is Cloud NGFW public IP address, and it's hitting the **AllowAllTraffic** rule that has been created in the rulestack. The screenshot below shows the IP address of the machine from which the request originated:



# What's my IP

# 134.238.18.9

Your public IP address

### **Test Outbound Traffic**

To validate the outbound connection, try to access twitter.com from App1 as shown below. Go to App1, select the Serial console section and type the following command:

Wget twitter.com



Home > raviDemoApp1 >	
raviDemoApp1   Se	erial console
✓ Search «	? Feedback 🛛 🎼 🌐
Metrics       Diagnostic settings       Logs       Connection monitor (classic)       Workbooks	<pre>root@raviDemoAppl:/home/demouser# wget twitter.com 2022-11-04 16:23:11 http://twitter.com/ Resolving twitter.com (twitter.com) 104.244.42.65, 104.244.42.193 Connecting to twitter.com (twitter.com) 104.244.42.65 :80 connected. HTTP request sent, awaiting response 301 Moved Permanently Location: https://twitter.com/ [following] 2022-11-04 16:23:11 https://twitter.com/ Connecting to twitter.com (twitter.com) 104.244.42.65 :443 connected. HTTP request sent, awaiting response 200 OK</pre>
Automation	Length: unspecified [text/html] Saving to: `index.html.1'
🖧 Tasks (preview)	index.html.1 [ <=> ] 135.64KKB/s in 0.05s
Export template	2022-11-04 16:23:12 (2.60 MB/s) - `index.html.1' saved [138892]
Help	root@raviDemoApp1:/home/demouser#
℅ Resource health	
Boot diagnostics	
Performance diagnostics	
Review VM Inspector (Preview)	
📍 Reset password	
Redeploy + reapply	
<ul> <li>Ubuntu Advantage support plan</li> </ul>	
Serial console	
Connection troubleshoot	

The connection has been established. Verify that this traffic is being processed by Cloud NGFW by going to the **Log Analytics workspace**. <u>Repeat</u> the steps to access logs.

Run the query again to get the latest logs.

Search	« P New Query 1* × +	💛 Feedback 📰 Queries   🛞 🛄
Data Export	raviCngfwLogWor Select scope	▶ Run (Time range : Last 24 hours) 🗟 Save 🗸 🖄 Share 🗸 🕂 New alert rule \mapsto Export 🗸 🔗 Pin to 🗸 😇 Format query
inked storage accounts Vetwork Isolation	Tables Queries Functions … «	1 fluentbit_CL
ables	♀ Search :	
ral	( Filter ) I≣ Group by: Solution ∨	
Workspace summary	T Collapse all	
Workbooks	Favorites	
logs	You can add favorites by clicking on	Results Chart 🔎
Solutions	the ☆ icon	Message
Jsage and estimated costs	<ul> <li>Custom Logs</li> </ul>	(src.ip:t1/21b.04, sport: 52/20, dst.ip:t2044.17.5, dport: 445, proto:tcp://app:tazure-log-analytics, rule: AllowAllitathc, action:tailow, bytes_recv: 4996, bytes_tent: 575/
Properties	▶ ⊞ fluentbit_CL	["src.jp":192.168.0.4", "sport"/55684", "dst.jp":104.244.42.193", "dport":143", "proto":1cp", "app":"twitter-base", "rule":"AllowAllTraffic", "action":"allow", "bytes_recv":156452", "bytes_sent":253
ervice Map		["src.jp":192.1680.4", "sport":55684", "dst.jp":104.244.42.193", "dport":1443", "proto":tcp", "app":twitter-base", "nule":AllowAllTraffic", "action":allow", "bytes_recv":156452", "bytes_sent":253



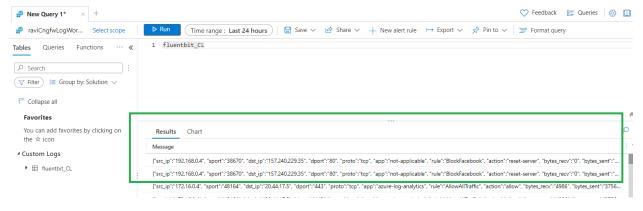
	Results Chart	Q
	Message (src_jp::1/2.16.0.4, sport: 52020, dst_jp::20.44.17.5, dport: 445, proto: tcp, app::azure-log-analytics, rule: AllowAllIratic, action: allow, bytes_recv: 4998, bytes_sent: 575	T 🛄 වේකාන
Г	{"src_ip":"192.168.0.4", "sport":"55684", "dst_ip":"104.244.42.193", "dport":"443", "proto":"tcp", "app":"twitter-base", "rule":"AllowAllTraffic", "action":"allow", "bytes_recv":"156452", "bytes_sent":"2	53
L	{"src_ip":"192.168.0.4", "sport":"55684", "dst_ip":"104.244.42.193", "dport":"443", "proto":"tcp", "app":"twitter-base", "rule":"AllowAllTraffic", "action":"allow", "bytes_recv":"156452", "bytes_sent":"2	53
	{"src_ip":"192.168.0.4", "sport":"51178", "dst_ip":"52.167.107.67", "dport":"443", "proto":"tcp", "app":"azure-log-analytics", "rule":"AllowAllTraffic", "action":"allow", "bytes_recv":"5190", "bytes_sent"	9°

#### **Test Outbound Block Rule**

Now try to access Facebook. The traffic to Facebook should get blocked as per the rule configured. Go to App1, select**Serial console** and type the following command: *wget www.facebook.com* 



Connection won't be established. Go to **Azure Log Analytics** to validate that Cloud NGFW has blocked this connection as per the rRulestack configuration.



Results	Chart
Message	
{"src_ip":"19	2.168.04", "sport": "38670", "dst_ip": "157.240.229.35", "dport": "80", "proto": "tcp", "app": "not-applicable", "rule": "BlockFacebook", "action": "reset-server", "bytes_recv": "0", "bytes_
{"src ip":"19	2.168.0.4", "sport": "38670", "dst_ip": "157.240.229.35", "dport": "80", "proto": "tcp", "app": "not-applicable", "rule": "BlockFacebook", "action": "reset-server", "bytes_recv": "0", "bytes_

From these logs, it is evident that the traffic to Facebook was blocked after hitting the **BlockFacebook** rule. This confirms that Cloud NGFW is able to block traffic as per configured rulestack.

#### **Test East-West Traffic flow**

Validate east-west traffic flow by trying to send traffic from App1 to App2.

On App1, execute the following command:

wget http:// <app2 ip<="" th=""><th>Paddress&gt;</th></app2>	Paddress>
Home > raviDemoApp1 >	
<b>raviDemoApp1</b>	Serial console
	« ? Feedback 🛛 🛱 🙂 🛲
📸 Metrics	<pre>root@raviDemoApp1:/home/demouser# root@raviDemoApp1:/home/demouser# wget http://172.16.0.4</pre>
Diagnostic settings	2022-11-04 17:19:21 http://172.16.0.4/
₽ Logs	Connecting to 172.16.0.4:80 connected. HTTP request sent, awaiting response 200 OK
🕵 Connection monitor (classic)	Length: 10918 (11K) [text/html] Saving to: 'index.html.5'
🧹 Workbooks	index.html.5 100%[====>] 10.66KKB/s in 0s
Automation	2022-11-04 17:19:21 (178 MB/s) - `index.html.5' saved [10918/10918]
🔒 Tasks (preview)	root@raviDemoApp1:/home/demouser#
😫 Export template	

The connection has been established. Validate by going to the to **Azure Log Analytics** workspace:



RaviCngfwLogWorks	space   Logs		×
	P New Query 1* × +	💎 Feedback 🐮 Queries   🍥	
Linked storage accounts	PraviCngfwLogWor Select scope	D Run (Time range : Last 24 hours)  Save ∨  Share ∨ + New alert rule → Export ∨  Pin to ∨  Format query	
<ul> <li>Network Isolation</li> </ul>	Tables Queries Functions ··· «	1 fluentbit_CL	
Tables	Search :		- 1
General	\[     \]     \[     \]     Filter     \[     \]     E Group by: Solution ∨		
<ul> <li>Workspace summary</li> </ul>	T Collapse all		- 1
🧹 Workbooks	Favorites		*
🧬 Logs	You can add favorites by clicking on	Results Chart	Q
P Solutions	the 🖈 icon	Message	Тур 🔟
<ul> <li>Usage and estimated costs</li> </ul>	<ul> <li>Custom Logs</li> </ul>		
Properties	fluentbit_CL	["src.ip"/172.16.0.4", "sport"/58090", "dst.ip"/52.167.106.94", "dport"/1443", "proto"/"tcp", "app"/"azure-log-analytics", "rule"/"AllowAllTraffic", "action"/"allow", "bytes recv"//4964", "bytes sent"/"4.	n mg
📫 Service Map		['src_jp':192.168.04', 'sport':'54844', 'dst_jp':'172.16.04', 'dport':'80', 'proto':'tcp', 'app':'web-browsing', 'rule':'AllowAllTraffic', 'action':'allow', 'bytes_reor':'12029', 'bytes_sent':'607', 'p	
Workspace Data Sources		("src_ip")"192.168.04", "sport": 54844", "dst_ip": "172.16.04", "dport": "80", "proto": "tcp", "app": "web-browsing", "rule": "AllowAllTraffic", "action": "allow", "bytes_recv": "12029", "bytes_sent": "607", "p	
Virtual machines		(srcjp::1/2.16.04, sport:sb226, dstjp::40./0.148.15, dport:443, proto:tcp; app:azure-log-analytics, rule:AllowAllirattic, action:allow, bytes_recv:bb2, bytes_sent:s/	-
Storage accounts logs		['srcjp':'172.160.4', 'sport':'36228', 'dst_jp':'40.70.148.13', 'dport':'443', 'proto':'tcp', 'app':'azure-log-analytics', 'rule':'AllowAllTraffic', 'action':'allow', 'bytes_recv':'5052', 'bytes_sent':'37	
		Exc io/1192168.04*, "port/149346", "dst io/152167.107.67", "doort/143", "proto/"top/"app/"asure-loo-analyticr, "rule "AllowAllTaffic", "action "fallow", "bytes rec/14999", "bytes sent")	
Results Chart			Q
Message			Тур
{"src_ip":"172.16.0.4", "spor	t":"58090", "dst_ip":"52.167.106.94", "o	dport":"443", "proto":"tcp", "app":"azure-log-analytics", "rule":"AllowAllTraffic", "action":"allow", "bytes_recv":"4964", "bytes_sent":"4	
{"src ip":"172.16.0.4", "spor	t":"58090", "dst ip":"52.167.106.94", "c	dport":"443", "proto":"tcp", "app":"azure-log-analytics", "rule":"AllowAllTraffic", "action":"allow", "bytes recv":"4964", "bytes sent":"4	
{"src_ip":"192.168.0.4", "spc	ort":"80", "proto":"tcp", "app":"web-browsing", "rule":"AllowAllTraffic", "action":"allow", "bytes_recv":"12029", "bytes_sent":"607", "p		
{"src_ip":"192.168.0.4", "spc	ort":"54844", "dst_ip":"172.16.0.4", "dp	ort":"80", "proto":"tcp", "app":"web-browsing", "rule":"AllowAllTraffic", "action":"allow", "bytes_recv":"12029", "bytes_sent":"607", "p	
{ src_ip : 1/2.16.0.4 , spor	t:36228, dst_ip:40.70.148.13, d	port : 443 , proto : tcp , app : azure-log-analytics , rule : AllowAllTraffic , action : allow , bytes_recv : 5052 , bytes_sent : 3/	-

From these logs, it is visible that the traffic sent between App1 (192.168.0.4) and App2 (172.16.0.4) is going through the Cloud NGFW service and hitting the **AllowAllTraffic** rule which is part of the local rulestack.

Thus the inbound, outbound, and east-west traffic has been tested and is flowing through the Cloud NGFW service.



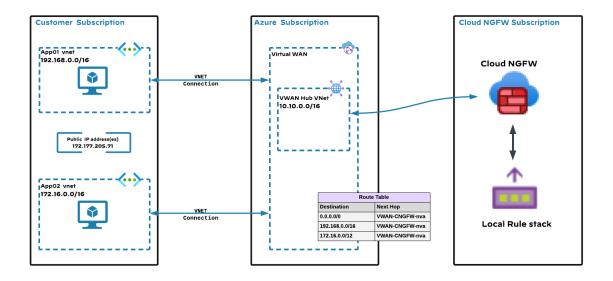
# Integrate Cloud NGFW into Azure Virtual WAN(VWAN) Infrastructure

# Pre-deployment of Cloud NGFW - setting up the environment

### Topology

A hub-spoke topology is used as an example to route traffic through Cloud NGFW. Cloud NGFW supports all topologies.

#### Integrate Cloud NGFW into Azure Virtual WAN(VWAN)



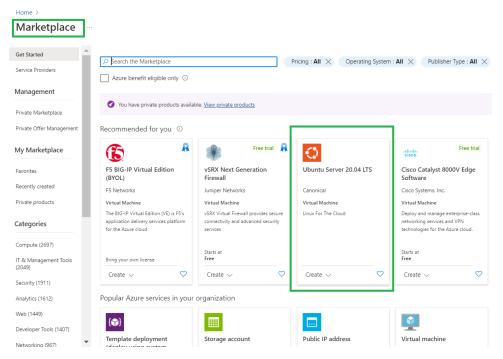
As per the above topology, in order to set up a lab environment, there should be a Azure Virtual WAN with VWAN Hub, 2 spoke VNets and a virtual machine on each of those spoke VNets that's running a web server (apache2). Create this environment before creating and deploying the Cloud NGFW resources.



# Create Spoke VNets with a virtual machine on each of them

#### Create Spoke App01 VNet with Ubuntu Server

1. Go to <u>Azure Marketplace</u> and search for "<u>Ubuntu</u>" Server as shown below:



2. Choose this Ubuntu server and click 'Create' to start the creation of the Ubuntu server:



3. Fill in the details (Resource Group, VM Name, Region and the type of image while leaving other fields to default.) to complete the creation of the Ubuntu server.

Basics Disks	Networking	Management	Monitoring	Advanced	Tags	Review	+ create	
Create a virtual mach image. Complete the for full customization	Basics tab then I		-			-		
Project details								
Select the subscriptio your resources.	on to manage de	ployed resources	and costs. Use re	source groups l	like folde	rs to organ	ize and man	age all
Subscription *		AzureTM	E					$\sim$
Resource gro	up * 🕕	raviCNGF Create new						$\sim$
Instance details								
Virtual machine name	e* (i)	raviCngfv	/Spoke App1					~
Region * 🛈		(US) East	US 2					$\sim$
Availability options (	D	No infras	tructure redunda	ncy required				$\checkmark$
Security type 🛈		Standard						$\sim$
Image \star 🕠			tu Server 20.04 L1					$\sim$
		See all ima	ges   Configure V	M generation				
VM architecture 🛈		Arm64	ł					
		💽 x64						

4. In the networking section, select an existing VNet or create a new one in which this Ubuntu server will be installed:



Home > Marketplace > Ubuntu Server 20.04 LTS >					
Create a virtual machine					
Define network connectivity for your virtual inbound and outbound connectivity with se Learn more of Network interface	agement Monitoring Advanced Tags Review + create machine by configuring network interface card (NIC) settings. You can control ports, curity group rules, or place behind an existing load balancing solution.				
When creating a virtual machine, a network	interface will be created for you.				
Virtual network * ①	(new) raviCngfwSpokeApp1RG-vnet				
Subnet * 🕕	(new) raviCngfwSpokeApp1Subnet (192.168.0.0/24)				
Public IP ①	(new) raviCngfwSpokeApp1-ip				
NIC network security group ①					
Public inbound ports * ①	None     Allow selected ports				

- 5. Review the configuration and create the server.
- 6. Once the Ubuntu server deployment is complete, install an apache server on it. To do this, go to the serial console of the created Ubuntu server and execute the commands below to install an apache server:

sudo apt update



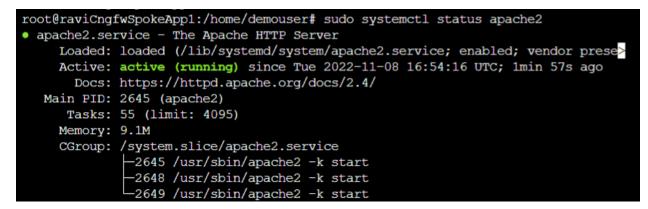
🔎 Search	« ? Feedback 🗹 🐯 🕛 🏧
Workbooks  Automation	▲ The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.
Tasks (preview)	Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
Export template	applicable law.
Help	To run a command as administrator (user "root"), use "sudo <command/> ". See "man sudo_root" for details.
➢ Resource health	demouser@raviCngfwSpokeApp1:~\$
Boot diagnostics	demouser@raviCngfwSpokeApp1:~\$
Performance diagnostics	demouser@raviCngfwSpokeApp1:~\$ demouser@raviCngfwSpokeApp1:~\$ sudo su
VM Inspector (Preview)	root@raviCngfwSpokeApp1:/home/demouser# root@raviCngfwSpokeApp1:/home/demouser#
Reset password	root@raviCngfwSpokeAppl:/home/demouser sudo apt update Hit:1 http://azure.archive.ubuntu.com/ubuncu rocal inversase
Redeploy + reapply	Get:2 http://azure.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Ubuntu Advantage support	Get:3 http://azure.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB] Get:4 http://azure.archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Serial console	Get:5 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 Packages [862 Get:6 http://azure.archive.ubuntu.com/ubuntu focal/universe Translation-en [512 Get:7 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadat
Connection troubleshoot	Get:8 http://azure.archive.ubuntu.com/ubuntu focal/ulliverse amd64 Packages [1

sudo apt install apache2

raviCngfwSpokeApp1   Serial console						
✓ Search «	? Feedback 🛛 🔯 🕛 🛲					
Logs     Connection monitor (classic)	<pre>root@raviCngfwSpokeApp1:/home/demouser# root@raviCngfwSpokeApp1:/home/demouser# sudo apt install apache2 Reading package lists Done Building dependency tree</pre>					
Reading state information Done						

Confirm that the apache server installed successfully using the following command:

sudo systemctl status apache2





#### Create Spoke App02 VNet with Ubuntu Server (For EW-traffic)

Repeat the above steps to create Spoke VNet2 with Ubuntu server.

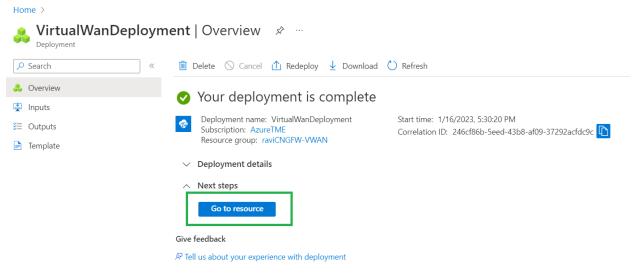


#### **Create Azure Virtual WAN with Hub**

1. Login to Azure portal and search for Virtual WAN and click on "Create" option to create Virtual WAN Service

Home >
Virtual WANs ☆ … Palo Alto Networks Inc. (paloaltonetworks.onmicrosoft.com)
+ Create 🐯 Manage view $\lor$ 🖒 Refresh 🞍 Export to CSV 😚 Open query 🛛 🗞 Assign tags
Filter for any field       Subscription equals all       Resource group equals all       Location equals all $+_{\nabla}$ Add filter

On successful creation of Virtual WAN service, you can go to the resource by clicking on "Go to resource" as per the screenshot below.



 Add Hub to the Virtual WAN created.
 After going to the Virtual WAN created in the above step, add a new hub by going to "Connectivity > Hubs" as shown below.



Home > VirtualWanDeployment   Overview	· > CNGFW-VW	AN	
CNGFW-VWAN   Hub	S ☆ …		
₽ Search «	+ New Hub	🕐 Refresh	
Overview	₽ Search for I	hubs by name Clear all filte	ars
<ul> <li>Activity log</li> </ul>			
Access control (IAM)	+ Add filter		
🔷 Tags	Hub	Hub status	Region
Settings	No results		
a Configuration			
Properties			
🔒 Locks			
Connectivity			
👾 Hubs			
VPN sites			

Configure Hub private address space as shown below and click on "Next : Site to Site >"



Home > Virtual WANs > CNGFW-VWAN | Hubs >

#### Create virtual hub

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). Learn more 🗗

#### Project details

The hub will be created under the same subscription and resource group as the vWAN. ☑

Subscription	AzureTME V			
Resource group	raviCNGFW-VWAN	$\sim$		
Virtual Hub Details				
Region *	East US 2	$\sim$		
Name *	raviVWANHub	~		
Hub private address space * ①	10.10.0/16	<u> </u>		
Virtual hub capacity * 🥡	2 Routing Infrastructure Units, 3 Gbps Router, Supports 2000 VMs	$\sim$		
Hub routing preference * ①	ExpressRoute	$\sim$		
Hub routing preference * ①	ExpressRoute	$\checkmark$		
Hub routing preference * ①	ExpressRoute	$\checkmark$		
Hub routing preference * ③ Creating a hub with a gateway will take		~		

After this you can directly go to the "Tags" section and configure Tag as shown below.



Home > Virtual WANs > CNGFW-VWAN | Hubs >

Create virtual hub		
to multiple resources and resource gro	you to categorize resources and view consolio ups. <u>Learn more</u> 더	dated billing by applying the same tag
Note that if you create tags and then d	hange resource settings on other tabs, your t Value ①	Resource
hubSaaSPreview	: true	9 selected 🗸 🕅
		9 selected V
<b>()</b> Creating a hub with a gateway will ta	ake 30 minutes.	
Review + create Pre	evious Next : Review + create >	

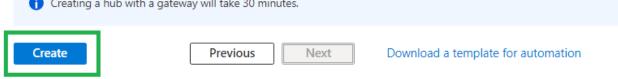
**NOTE**: Tag name "hubSaaSPreview" and Value "true" should be provided while creation of the hub and should not be provided after creation of hub.

On successful validation of the configuration, click on "Create" to create Virtual WAN Hub



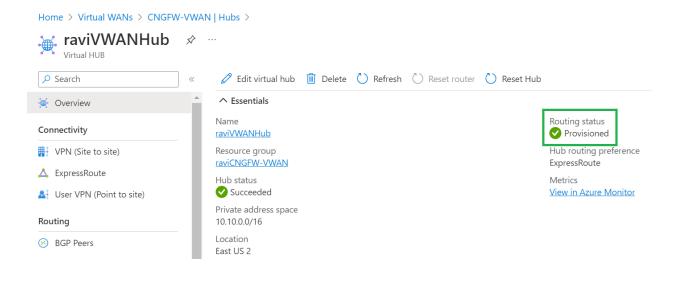
Home > VirtualWanDeployment | Overview > CNGFW-VWAN | Hubs >

#### Create virtual hub . . . Validation passed ExpressRoute Basics Site to site Point to site Tags Review + create The hub will be created under the same subscription and resource group as the vWAN. Basics Region East US 2 raviVWANHub Name Hub private address space 10.10.0.0/16 Virtual hub capacity 2 Routing Infrastructure Units, 3 Gbps Router, Supports 2000 VMs Hub routing preference ExpressRoute Site to site Site to site (VPN gateway) Disabled Point to site Point to site (VPN gateway) Disabled Creating a hub with a gateway will take 30 minutes.



After creation of Virtual WAN Hub, make sure that the Routing status is in "Provisioned" state





## **Deployment of Cloud NGFW**

- **1.** Now that the Virtual WAN environment is set up, deploy the Cloud NGFW to protect the traffic going through Virtual WAN Hub.
- **2.** Login to Azure portal and search for "paloalto". This search displays the Cloud NGFW service by Palo Alto Networks:

≡	Microsoft Azure		×	D 🖓	Q
	Azu	All         Services (2)         Resources (1)         Resource Groups (1)         Marketplace (16)           Azure Active Directory (66)         Azure Active Directory (20)         Azure Active Directory (20)         Azure Active Directory (20)	Documentation (1)		
	C	Services	GFW by Palo Alto Netwo	orks	

- **3.** Click "Cloud NGFWs" to start the creation of the Palo Alto Networks Cloud NGFW service for Azure.
- **4.** The following screen is the landing page for the Cloud NGFW resource. This screen populates all the available, pre-created Cloud NGFW instances (if not a first-time user). Click **Create** to start the creation of a Cloud NGFW resource:



Home >

# Cloud NGFWs 🛷 🖤

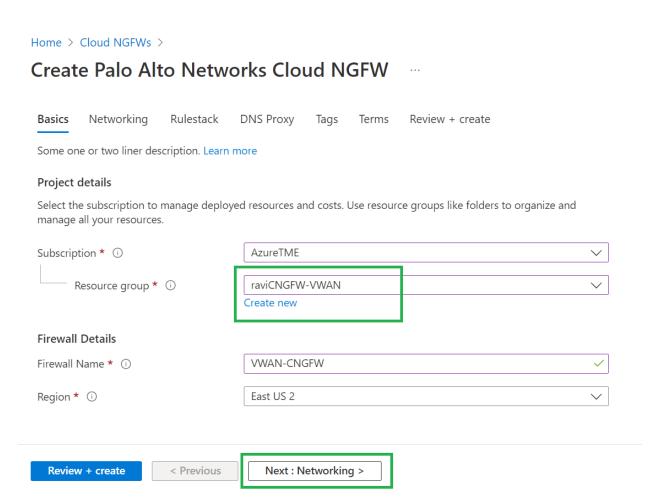
Palo Alto Networks Inc. (paloaltonetworks.onmicrosoft.com) | PREVIEW

🕂 Create 🐯 Manage view	w 🗸 🖒 Refresh	↓ Export to C	SV 😚 Open query	Ę
Filter for any field	Subscription equal	s <b>all</b> Reso	ource group equals <b>all</b>	X

**5.** After clicking **Create**, the Create Palo Alto Networks Cloud NGFW screen appears. Use the information in the table below to populate basic information for your Cloud NGFW resource:

Subscription	Automatically selected based on the subscription used while logged in.
Resource Group	Use one of the existing resource groups or create a new resource group (by clicking the <b>Create New</b> option) in which the Cloud NGFW resource is created.
Firewall Name	Name of the Cloud NGFW Firewall resource.
Region	Region in which Cloud NGFW is provisioned. For this Private Preview, only US East-2 and US Central regions are supported.





6. Once the details are filled in, click Next: Networking > and provide information for your networking environment. Choose the Network Injection type as Virtual Wan Hub. And select Virtual Hub Name from the dropdown(this is the Hub which got created in above step.). You can also specify IP addresses. Specify the Source NAT option if Network Address Translation (NAT) is used on the traffic going out to the Internet:





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	k Type							
Type *		0 •	Virtual Network Virtual Wan Hub	1				
Virtual \	Wan Hub Detail	s						
{") fa		"true"}. Note that this re	esource tag must b			e deployed with hub resource tag ition and cannot be applied after the		
vir coor fr		ra	viVWANHub			$\checkmark$		
	P Address Confi		VIVWANHUD			~		
Public IF		guration	Create new Use existing			~		
Public IF Public IP	P Address Confi	guration	Create new	blic-ip		~		
Public IF Public IP Public IP Source I	P Address Confi Address(es) * ④	guration	Create new Use existing	blic-ip				

7. Click Next: Security Policies > to create a Local Rule stack where rules can be defined. This is a placeholder for the local rule stack. After the creation of Cloud NGFW resource, this rulestack can be modified to add/edit rules, FQDN,



and prefix list. If there is a Local Rule Stack that's already created, select it from the drop-down menu after selecting Use existing option:

### Create Cloud NGFW by Palo Alto Networks

Basics Networking Sec	urity Policies DNS Proxy Tags Terms Review + create
Managed by * ①	<ul> <li>Azure Portal Rulestack</li> <li>Palo Alto Networks Panorama</li> </ul>
Choose a Local Rulestack * 🕕	• Create new
	Use existing
Local Rulestack *	VWAN-CNGFW-Irs
Firewall rules * (i)	<ul> <li>Allow all (Enables all security services using best-practices profile to inspect traffic)</li> </ul>
	O Deny all
	Advanced Cloud-Delivered Security Services (such as Advanced Threat Prevention, Advanced DNS Security), you must register your Azure Tenant at the Palo Alto Networks Customer wall creation.
Without registering your Az and URL Filtering) will be of	zure Tenant, only the standard Cloud-Delivered Security Services (such as Threat Prevention, ifered, if enabled.
Deview L greate	evious Next : DNS Proxy >
Review + create < Pre	evious Next : DNS Proxy >

8. Click Next: DNS Proxy > to configure Cloud NGFW as a DNS Proxy. It is disabled by default:



Home > Cloud NGFWs >

# Create Palo Alto Networks Cloud NGFW

Basics	Networking	Rulestack	DNS Proxy	Tags	Terms	Review + create
DNS Prox	ку <b>*</b> (і)		<ul> <li>Disabled</li> </ul>			
			◯ Enabled			





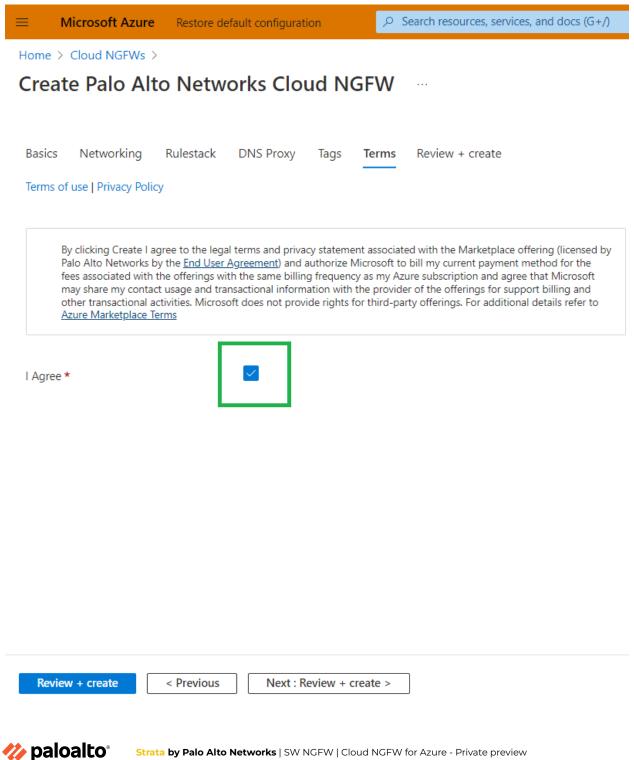
9. Click Next: Tags > to specify tags as per your Azure requirements:

Microsoft Azure	Restore default configuration	n 🔎 S	Search resources, services, and docs (G+/)
Iome > Cloud NGFWs >			
Create Palo Alto	Networks Clou	d NGFW	
Basics Networking I	Rulestack DNS Proxy	Tags Terms	Review + create
			consolidated billing by applying the same
	d resource groups. Learn mor		
Note that if you create tags a	and then change resource sett	ings on other tabs	, your tags will be automatically updated.
Name 🛈	Value (i)		Resource
StoreStatusDND	: DND		7 selected 🗸 📋
	:		Select all
			Cloud NGFW
			✓ Local Rulestack
			Microsoft.Network/virtualHub
			Network security group
			Public IP address
			Virtual network
			Virtual WAN

vious Next : Terr	ns >	Next : Terms >
-------------------	------	----------------



10. Click Next: Terms > and accept the terms as shown below:



 Click Next: Review + Create > and create a Cloud NGFW service. Like any other Azure native service, the resource is validated first and then created. Once the screen shows Validation Passed, click Create to deploy the Cloud NGFW service.



#### Home > Cloud NGFWs >

# Create Palo Alto Networks Cloud NGFW

🕑 Val	idation Passed					
Basics	Networking	Rulestack	DNS Proxy	Tags	Terms	Review + create
Basics						
Subscrip	tion		AzureTME			
Resource	e group		raviCNGFW-\	/WAN		
Firewall I	Name		VWAN-CNGF	W		
Region			East US 2			
Networ	king					
Туре			Virtual Wan H	Hub		
Virtual H	lub Name		raviVWANHu	b		
Public IP	Address(es)		Create new			
Public IP	Address Name(s)	)	VWAN-CNGF	W-public	:-ip	
Rulesta	ck					
Choose a	a Local Rulestack		Create new			
Local Ru	lestack		VWAN-CNGF	W-lrs		
	_					
Create	e 🛛 < Previ	ous	lext			

After creating the Cloud NGFW service the deployment progress is displayed:



CreateFirewallF	orm-20	230117160644   Overvie	W 🖈 …			
© Search	« [	] Delete 🚫 Cancel 📋 Redeploy 🚽	🕐 Download 💍 Refresh			
Vverview		Deuleument is in one				
Inputs		<ul> <li>Deployment is in prog</li> </ul>	ress			
Outputs	{ <b>\$</b>	Deployment name: CreateFirewallForm Subscription: AzureTME	n-20230117160644	Start time: 1/17/2023, 4:14:58 PM Correlation ID: e155ac21-cc3c-4f5b-a1c3-386c7a4ade09 🖺		
Template		Resource group: raviCNGFW-VWAN				
	,	∧ Deployment details				
		Resource	Туре	Status	Operation details	
		S VWAN-CNGFW-Irs	PaloAltoNetworks.Cloud	dngfw/localR Created	Operation details	
		S VWAN-CNGFW-nva	Microsoft.Network/netw	vorkVirtualAp Created	Operation details	
		VWAN-CNGFW-public-ip	Microsoft.Network/pub	C-IDA delegance OK	Operation details	

#### The deployment of a Cloud NGFW takes approximately 30 minutes.

On a successful deployment, the screen below appears. Click Go to resource group to verify the resources created for this deployment:

Search	🗌 « 📲 Delete 🚫 Cancel 🚹 Redeploy 🚽 Download 🖒 R	efresh
Overview	Your deployment is complete	
Inputs		
Outputs	Deployment name: CreateFirewallForm-20230117160644 Subscription: AzureTME	Start time: 1/17/2023, 4:14:58 PM Correlation ID: e155ac21-cc3c-4f5b-a1c3-386c7a4ade09 🌓
Template	Resource group: raviCNGFW-VWAN	
	✓ Deployment details	
	<ul> <li>Next steps</li> </ul>	

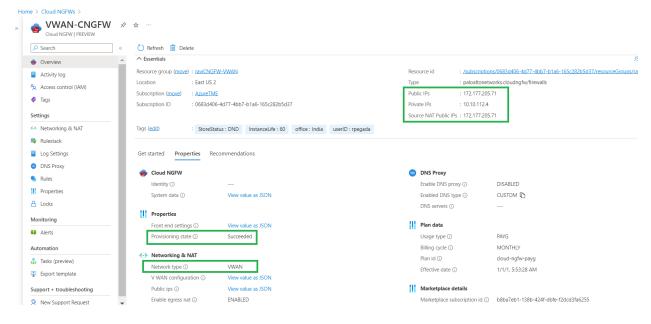
**12.** There are Four resources created, which include Cloud NGFW, Local Rule stack, Public IP address and Cloud NGFW-nva:



Home > CreateFirewallForm-202301171	60644   Overview >		
Resource group	\$ t		
	🕂 Create 🔞 Manage view 🗸 📋 Delete resource group 💍 Refresh 🞍 Export to CSV 😽	Open query $ $ $\oslash$ Assign tags $\rightarrow$ Move	∽ 🗊 Delete 🕁 Export tem
() Overview	↑ Essentials		
Activity log	Subscription (move) : AzureTME	Deployments : 3 Succeeded	
Access control (IAM)	Subscription ID : 0683d406-4d77-4bb7-b1a6-165c282b5d37	Location : East US 2	
🗳 Tags	Tags (edit)         :         StoreStatus : DND         UserID : rpegada         office : India		
🛧 Resource visualizer			
🗲 Events	Resources Recommendations		
Settings	Filter for any field		
1 Deployments			
Security	Showing 1 to 6 of 6 records. 🗹 Show hidden types 🛈		No grouping V
Policies	□ Name ↑↓	Туре ↑↓	Location $\uparrow_{\downarrow}$
Properties	CNGFW-VWAN	Virtual WAN	East US 2
🔒 Locks	□ 👾 raviVWANHub	Microsoft.Network/virtualHub	East US 2
Cost Management	🗌 🏚 VWAN-CNGFW	Cloud NGFW	East US 2
S Cost analysis	🗌 👼 VWAN-CNGFW-Irs	Local Rulestack	East US 2
Cost analysis	🗌 🎯 VWAN-CNGFW-nva	microsoft.network/networkvirtualappliance	East US 2
<ul> <li>Budgets</li> </ul>	🗌 🥅 VWAN-CNGFW-public-ip	Public IP address	East US 2

13. Once the Cloud NGFW resource is created, click on it to verify that the Provisioning state shows Succeeded. This screen also displays Public and Private IP addresses that are associated with the Cloud NGFW service. Use this information in further steps of this document to route traffic through the Cloud NGFW service

Also make sure that the Network type is **VWAN**:

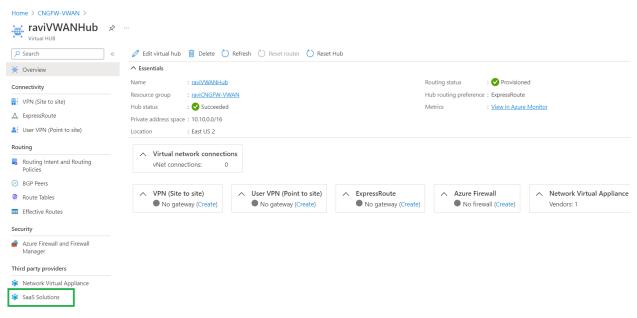




#### Verify for SaaS Solution within Virtual WAN Hub

After successful creation of the Cloud NGFW service with network type as Virtual WAN Hub. Verity for cloud NGFW to be added as a **SaaS Solution** for Virtual WAN Hub used.

Go to the Virtual Hub used while creating the cloud NGFW and click on "SaaS Solutions"



Cloud NGFW created will be added as a SaaS solution to this Hub as shown below.



	Create SaaS III Delete SaaS			
💓 Overview	SaaS Solutions			
Connectivity	Name	Provisioning State	Offering	Manage SaaS
VPN (Site to site)	😺 VWAN-CNGFW-nva	Succeeded	Palo Alto NGFWaaS	Click here
🛆 ExpressRoute				
🛂 User VPN (Point to site)				
Routing				
Routing Intent and Routing Policies				
BGP Peers				
Route Tables				
Effective Routes				
ecurity				
Azure Firewall and Firewall Manager				
Third party providers				
Network Virtual Appliance				
🔅 SaaS Solutions				

Within this screen, you can go to Cloud NGFW service created by clicking on "Click here" hyperlink, which is part of the Manage SaaS column.

Home 🗧 raviVWANHub   SaaS Solution	ons >		
	x 🛧 …		
Cloud NGFW   PREVIEW			
,Ω βearch ≪	C Refresh 🔟 Delete		
😝 Overview	Essentials		
Activity log	Resource group (move) : raviCNGFW-VWAN	Resource id	: /subscriptions/0683d406-4d77-4bb7-b1a6-165c282b5d
Access control (IAM)	Location : East US 2	Туре	: paloaltonetworks.cloudngfw/firewalls
Tags	Subscription (move) : AzureTME	Public IPs	: 172.177.205.71
<ul> <li>Tags</li> </ul>	Subscription ID : 0683d406-4d77-4bb7-b1a6-165c282b5d37	Private IPs	: 10.10.112.4
Settings		Source NAT Public IPs	; 172.177.205.71
Networking & NAT	Tags (edit) : StoreStatus : DND InstanceLife : 60 office : India UserID : rpegada		
💐 Rulestack			
Log Settings	Get started Properties Recommendations		
DNS Proxy			
💺 Rules	e Cloud NGFW	DNS Proxy	
Properties	Identity 🛈	Enable DNS prov	xy 🛈 DISABLED
	System data () View value as JSON	Enabled DNS typ	De (i) CUSTOM
🔒 Locks		DNS servers ①	
Monitoring	Properties		
Alerts	Front end settings ①	Plan data	
	Provisioning state ① Succeeded 🌓	Usage type 🛈	PAYG
Automation		Billing cycle 🛈	MONTHLY
Tasks (preview)	> Networking & NAT	Plan id 🛈	cloud-ngfw-payg
😫 Export template	Network type ①     VWAN	Effective date 🛈	1/1/1, 5:53:28 AM
	V WAN configuration View value as JSON		



## Post Deployment of Cloud NGFW

#### **Create/Update Rule stack**

1. To update/edit the rulestack, click the **Rulestack** option available in the Cloud NGFW resource. As shown below, this displays the rulestack associated with the cloud NGFW service along with the resource group:

Home > VWAN-CNGFW		
	ılestack …	
✓ Search «	💍 Refresh	
⅔     Access control (IAM)        Tags	Rulestack	
Settings	Local Rulestack *	VWAN-CNGFW-Irs, raviCNGFW-VWAN $\checkmark$ Currently associated rulestack: VWAN-CNGFW-Irs,
Networking & NAT		region: eastus2
💐 Rulestack		
Log Settings		
DNS Proxy		
🗣 Rules		

The Cloud NGFW is associated with **VWAN-CNGFW-Irs**.

Next, modify this rulestack to add firewall rules to allow some traffic and block specific traffic.

#### By default Cloud NGFW blocks all traffic.

2. Search for Local Rulestack in the global search of the Azure portal:



Microsoft Azure Res	tore defaul	t configuration	P VWAN-CNGFW-I13	) 🖟 🗘	<u>نې</u>	
Home > VWAN-CNGFW	'   Rule	estack …	All         Resources (1)         Documentation (29)         Services (0)         Resource Groups (0)         Marketplace (0)           Azure Active Directory (0)         Azure Active Directory (0)         Azure Active Directory (0)         Azure Active Directory (0)			
✓ Search	«	💍 Refresh	Resources			
Access control (IAM)	•		VWAN-CNGFW-Irs Local Rulestack			
🖗 Tags		Rulest	Documentation	See all		
iettings		Local Rulesta	Azure Virtual WAN Overview   Microsoft Learn 🛛 🖓 Monitoring Azure Virtual WAN - Data reference   Microsoft	t Learn (		
<ul> <li>Networking &amp; NAT</li> </ul>			Hub-spoke network topology with Azure Virtual WAN 🛛 🖉 🔋 Azure Virtual WAN FAQ   Microsoft Learn	C7		
Rulestack			Monitoring Virtual WAN - Azure Virtual WAN   Microsoft Learn 🛛 🖓 👘 What's new in Azure Virtual WAN?   Microsoft Learn	ď		
Log Settings			Install Azure Firewall in a Virtual WAN hub - Azure Virtual WAN  Disaster recovery design for Azure Virtual WAN   Microsoft	Learn (		
DNS Proxy			Tontinue searching in Azure Active Directory			
- Rules				_		
Properties			Searching all subscriptions. Change	R Give feedback		
- Locks						
Monitoring						

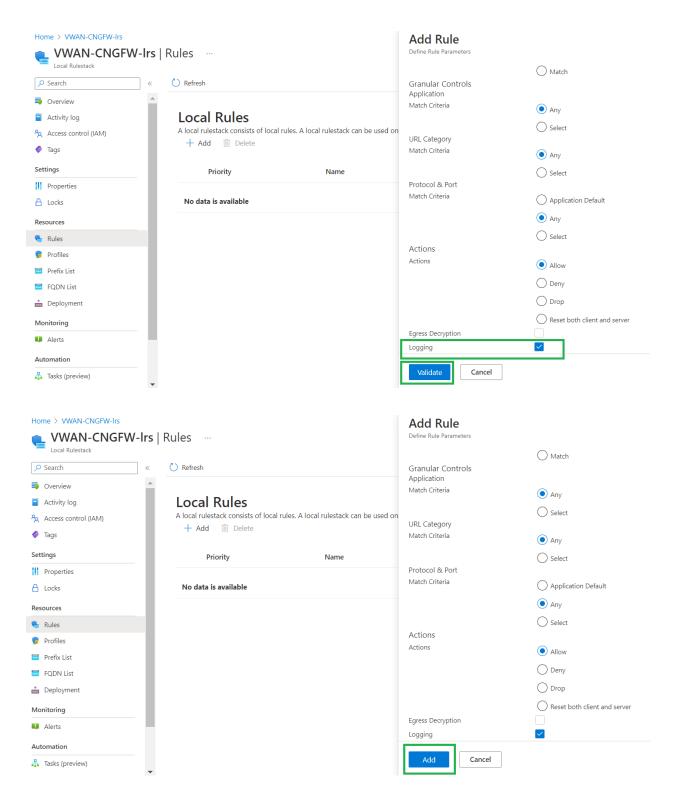
Click the Local Rulestacks to navigate to the rulestack associated with your Cloud NGFW service.

**3.** Click your rulestack(VWAN-CNGFW-Irs) to add rules as shown below. Modify the rules as per your use cases and functionality. Add a rule to allow traffic. Fill in the mandatory fields and use the default settings for the remaining fields:

Home > WAN-CNGFW-Irs WAN-CNGFW-Irs Local Rulestack Search	Add Rule Define Rule Parameters General Name * AllowAllTraffic
Coverview  Activity log  Access control (IAM)  Tags  Local Rules  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rules. A local rulestack can be used on  A local rulestack consists of local rule	Description Priority * ID0 Enabled Source Match Criteria O Any
Settings Priority Name	Match
Properties	Destination Match Criteria
A Locks No data is available	• Any
Resources           Rules           Profiles           Prefix List	Granular Controls Application Match Criteria
FIGN List	URL Category
Deployment	Match Criteria   Any
Monitoring	◯ Select
Alerts	Protocol & Port Match Criteria Application Default
Automation	Validate Cancel

Enable logging as part of the rule configuration, as shown below:





Click Validate and then Add to incorporate the rule.



**4.** Add an FQDN list that includes Facebook, and use this list to add a rule to block facebook.com:

Home > VWAN-CNGFW-Irs			Add FQDN List	
🥽 VWAN-CNGFW-Irs   F	QDN List		Enter a fully-qualified domain name (	FQDN) to create an FQDN object.
Local Rulestack	🖒 Refresh		Name * Description	Facebook
Overview			FQDN *	www.facebook.com
<ul> <li>Activity log</li> </ul>	FQDN List			
Access control (IAM)	An Fully-Qualified Domain Names	FQDN) List is security policy object t		
🗳 Tags	+ Add Delete	ress, using an FQDN object is more ¢		Enter one value per line.
Settings				
Properties	Name	FQDN		
🔒 Locks	No data is available			
Resources				
💺 Rules				
😡 Profiles				
🚾 Prefix List				
EQDN List				
📩 Deployment				
Monitoring				
💶 Alerts				
Automation				
🕌 Tasks (preview)			Add Cancel	

Facebook now appears in the **FQDN List**:

Home > VWAN-CNGFW-Irs	W-Irs   F	QDN List		
✓ Search	~	🕐 Refresh		
Overview	<u>_</u>			
Activity log		FQDN List		
Access control (IAM)				ows you to group specific source or destination FQDN that t than specifying IP addresses because FQDNs can be trans
🗳 Tags		+ Add 🗊 Delete	duress, dang un reprivebjeer is more emeter	e duri specifying in duaresses because repris can be duris.
Settings				
Properties		Name	FQDN	Description
🔒 Locks		Facebook	www.facebook.com	
Resources				
💺 Rules				
🔋 Profiles				
📅 Prefix List				
FQDN List				
Deployment				

Return to the Rules setting page and add a rule that matches the FQDN list created. Set the action to **Drop** to block Facebook traffic:



Home > VWAN-CNGFW-Irs			Add Rule		
🝋 VWAN-CNGFW-Irs	Rules		Define Rule Parameters		
Local Rulestack			General		
♀ Search «	🕐 Refresh		Name *	BlockFacebook	
Overview			Description		
Activity log	Local Rules		Priority *	50	
Access control (IAM)		I rules. A local rulestack can be used on	Enabled Source		
Tags	+ Add 🔟 Delete		Match Criteria	<ul> <li>Any</li> </ul>	
Settings	Priority	Name		◯ Match	
Properties	100	AllowAllTraffic	Destination		
🔒 Locks	100	AllowAll Ifattic	Match Criteria	Any	
Resources				<ul> <li>Match</li> </ul>	
🗣 Rules			IP Address (CIDR Format)		
💼 Profiles			Countries		
Prefix List			Prefix List		$\sim$
FQDN List			FQDN List Destination Exclude	Facebook	$\checkmark$
Deployment			Granular Controls Application		
Monitoring			Match Criteria	<ul> <li>Any</li> </ul>	
📮 Alerts				Select	
Automation					
Tasks (preview)			Validate Cancel		



## Add Rule **Define Rule Parameters** Destination Exclude Granular Controls Application Match Criteria Any Select URL Category Match Criteria Any Select Protocol & Port Match Criteria Application Default Any Select Actions Actions Allow Deny 🔵 Drop Reset both client and server Egress Decryption Logging $\checkmark$ Cancel Add

#### 5. Both the rules appear as shown below:

Home > VWAN-CNGFW-Irs								
	s   Rules …							
✓ Search «	💍 Refresh							
Overview     Activity log     Access control (IAM)     Tags	Local Rules	rules. A local rulestack can be used on mul	Itiple firewalls within the san	ne subscription.				
Settings	Priority	Name	Source	Destination	Constraints	Action	Logging	Egress Decry
Properties	100	AllowAllTraffic	any	any	no	Allow	yes	Disabled
Resources	50	BlockFacebook	any	match	no	DenyResetServer	yes	Disabled
🗲 Rules								
🧓 Profiles								
🔤 Prefix List								

**6.** As part of this Cloud NGFW service, the security profiles are enabled with best practice configurations by default. This means that the traffic is secured with the best security profiles from day one, once the Cloud NGFW is deployed in the network:



Home > VWAN-CNGFW-Irs			
<b>VWAN-CNGFW-</b> Local Rulestack	Irs   Profiles		
₽ Search	« 🛛 🛛 💭 Refresh		
Overview			
Activity log	IPS and Sp	yware Threats Protection	
Access control (IAM)	IPS Vulnerabili	ity	
🗳 Tags		n System (IPS) is a network security and threat prevention t	technology that examines traffic flow to dete
Settings	Enable		
Properties	Profile	Best Practice	$\checkmark$
🔒 Locks	Anti-Spyware		
Resources		on zeroes in outbound threats, especially command-and-co	ontrol (C2) activity, where an infected client is
🗲 Rules		Best Practice	~
🔋 Profiles	Profile	Dest Fractice	V
🖻 Prefix List			
FQDN List	Malware a	nd File-based Threat Prote	oction
nt Deployment			
Monitoring	Antivirus	nst viruses, worms, and trojans as well as spyware downloa	de
I Alerts	Enable	nst viruses, worms, and trojans as wen as spyware dowinioa	us.
Automation	Profile	Best Practice	$\sim$
Automation	File Bleeking		
Tasks (preview)	File Blocking	event the transmission of specific file types sent over your r	network.
😫 Export template	Enable		
Support + troubleshooting	Profile	Best Practice	~
R New Support Request			

7. Now that the rules have been modified, they should be deployed onto the Local rulestack associated with the Cloud NGFW service. Click the **Deployment** tab to see the page below. The deployment status displays as **Candidate**, which means the configuration was built but not deployed. Next, click **Deploy Configuration** to deploy the configuration onto the Cloud NGFW service. It is mandatory to do this step as without this the configuration will not be deployed onto the rulestack.



Home > VWAN-CNGFW-Irs			
◆ VWAN-CNGFW-Irs Local Rulestack	Deployment		
	💍 Refresh		
Overview			
<ul> <li>Activity log</li> </ul>	Deployment		
Access control (IAM)			
🗳 Tags	Status	Action	
Settings	Candidate	Beploy Configuration	7 Revert
Properties			
🔒 Locks			
Resources			
💺 Rules			
🕵 Profiles			
Prefix List			
FQDN List			
💼 Deployment			
Monitoring			

After clicking **Deploy Configuration,** a pop-up displays the firewalls associated with this rulestack. Click **Deploy** to configure this rulestack on all the associated firewalls:

₽ Search	« 🕐 Refresh	
Overview	*	
Activity log	Deploym	ent
Access control (IAM)		
Tags	Status	
ttings	Candidate	— Deploy ×
Properties		Push your configured rulestacks to your firewalls.
Locks		The following firewall(s) will be deployed with the changes made to the rulestack.
sources		VWAN-CNGFW(raviCNGFW-VWAN)
Rules		
Profiles		Deploy Cancel
Prefix List		
FQDN List		
Deployment		

After successfully deploying the configuration, the screen displays the deployment status as **Running** 



Home > VWAN-CNGFW-Irs			
VWAN-CNGFW-Irs	Deployment		
₽ Search «	🕐 Refresh		
Overview			
Activity log	Deployment		
Access control (IAM)			
🇳 Tags	Status	Action	
Settings	Running	····	5
Properties		Deploy Configuration	7 Revert
🔒 Locks			
Resources			
💺 Rules			
🔋 Profiles			
🧮 Prefix List			
FQDN List			
📩 Deployment			
Monitoring			

With this, the Cloud NGFW and Local rulestack are successfully deployed.

#### Source/Destination NAT rule on Cloud NGFW

Configure a destination NAT rule with frontend configuration on Cloud NGFW to take care of Inbound traffic towards App1 or App2 present on spoke VNet1 or spoke VNet2.

- Access the Networking & NAT settings screen for the cloud NGFW resource. The first thing to observe is whether the network type is selected as "Virtual WAN Hub" and Source NAT setting has been enabled or not. During the creation of the Cloud NGFW resource,(step 6) if Source NAT was enabled, that's how it will show up here.
- 2. Click **Edit** to add the Destination NAT rule.



Home > VWAN-CNGFW

VWAN-CNGFW   Netv     Cloud NGFW	vorking & NAT	
₽ Search «	🖉 Edit 💍 Refresh	
😑 Overview		
Activity log	Networking	
Access control (IAM)	Туре	Virtual Network
🗳 Tags		Virtual WAN Hub
Settings	Virtual Hub	raviVWANHub
Networking & NAT	NVA Id	VWAN-CNGFW-nva
<table-of-contents> Rulestack</table-of-contents>		
Log Settings		
ONS Proxy	Source Network Address	
🖕 Rules	Public IP Addresses	172.177.205.71
Properties	Enable Source NAT () Use the above Public IP addresses	
🔒 Locks		_
Monitoring		
Alerts	Destination Network Add	ress Translation (DNAT)

3. Add a **Destination NAT** rule with frontend configuration as shown below. Frontend IP is the Public IP address associated with Cloud NGFW (choose this from the drop-down menu). To access Appl (192.168.0.4), <u>deployed</u> on spoke VNet1, on port 80(HTTP), we are going to use Cloud NGFW frontend IP address and port 8080. After adding the Destination NAT rule, save the configuration by clicking **Add**.



Home > VWAN-CNGFW

✓ Search	« 🗄 :	Save 🗙 Discard		
Overview	<u>^</u> N	letworking		
Activity log	Ту	5	Virtual Network	
Access control (IAM)				
			Virtual WAN Hub	
🇳 Tags		rtual Hub	raviVWANHub	
Settings	N\	VA Id	VWAN-CNGFW-nva	
🕪 Networking & NAT				
Rulestack				
Log Settings			ress Translation (SNAT)	
DNS Proxy		ıblic IP Addresses	VWAN-CNGFW-public-ip	$\checkmark$
		able Source NAT 🛈		
Rules	Us	se the above Public IP addresse	is 🖌	
Properties				
Locks				
-		estination Network	Address Translation (DNAT)	
Monitoring Alerts Automation			Address Translation (DNAT)	
Alerts Automation ome > VWAN-CNGFW	ĺ	Search Add Delete	d Setting	
Alerts Automation and States States Automation Automati	ĺ	Search Add Delete  Provide Configuration for I Name *	d Setting Frontend Setting	
Alerts Automation  Methods  Alerts  Automation  Methods  Automation  Methods  Automation	letworking & NAT	Search Add Delete	d Setting Frontend Setting InboundApp1 © TCP	
Alerts Automation  Mere > VWAN-CNGFW  VWAN-CNGFW  VWAN-CNGFW  Cloud NGFW  Cloud NGFW  Cloud NGFW  Coverview  ()	letworking & NAT	Search Add Delete  Provide Configuration for I Name *	d Setting Frontend Setting	
Alerts Automation  Mere > VWAN-CNGFW  VWAN-CNGFW  VWAN-CNGFW NGFW  Search  Verview  Activity log Access control (IAM)	letworking & NAT Save × Discard Networking Type	Search  Add  Delete  Add Frontent Provide Configuration for I Name * Protocol *  Frontend IP * Frontend IP * Frontend Port *	d Setting Frontend Setting InboundApp1 TCP UDP VWAN-CNGFW-public-ip 8080	
Alerts Automation  Automation  Automation  Automation  Automation  Automation  Automation  Autivity log  Access control (IAM)  Tags	letworking & NAT	Search  Add  Delete  Add Fronten  Provide Configuration for I  Name *  Protocol *  Frontend IP *	d Setting Frontend Setting InboundApp1 TCP UDP VWAN-CNGFW-public-ip	
Alerts Automation	letworking & NAT Save X Discard Networking Type Virtual Hub	Search  Add  Delete  Add Frontent Provide Configuration for I Name* Protocol*  Frontend IP* Frontend IP* Backend IP*	d Setting Frontend Setting InboundApp1 TCP UDP VWAN-CNGFW-public-ip 8080 192.168.0.4	
Alerts Al	letworking & NAT Save × Discard Networking Type Virtual Hub NVA Id	Search  Add  Delete  Add Fronten Provide Configuration for I Name * Protocol *  Frontend IP * Backend IP * Backend Port *	d Setting Frontend Setting InboundApp1 TCP UDP VWAN-CNGFW-public-ip 8080 192.168.0.4	
Alerts Alerts Alerts WAN-CNGFW VWAN-CNGFW Cloud NGFW Cloud NGFW Cloud NGFW Coverview Activity log Access control (IAM) Tags ttings Networking & NAT Rulestack	letworking & NAT Save X Discard Networking Type Virtual Hub NVA Id Source Network A	Search  Add  Delete  Add Fronten Provide Configuration for I Name * Protocol *  Frontend IP * Backend IP * Backend Port *	d Setting Frontend Setting InboundApp1 TCP UDP VWAN-CNGFW-public-ip 8080 192.168.0.4	
Alerts Al	letworking & NAT Save × Discard Networking Type Virtual Hub NVA Id	Search  Add  Delete  Add Fronten Provide Configuration for I Name * Protocol *  Frontend IP * Backend IP * Backend Port *	d Setting Frontend Setting InboundApp1 TCP UDP VWAN-CNGFW-public-ip 8080 192.168.0.4	
Alerts Automation	letworking & NAT Save X Discard Networking Type Virtual Hub NVA Id Source Network A Public IP Addresses	Search Add Delete  Add Frontend Provide Configuration for I Name * Protocol *  Frontend IP * Frontend IP * Backend Port * Backend Port *	d Setting Frontend Setting InboundApp1 TCP UDP VWAN-CNGFW-public-ip 8080 192.168.0.4	
Alerts Automation	Letworking & NAT Save Discard Networking Type Virtual Hub NVA Id Source Network A Public IP Addresses Enable Source NAT ()	Search Add Delete  Add Frontend Provide Configuration for Name * Protocol *  Frontend IP * Frontend IP * Backend IP * Backend Port *	d Setting Frontend Setting InboundApp1 TCP UDP VWAN-CNGFW-public-ip 8080 192.168.0.4	
Alerts Automation	Letworking & NAT Save × Discard Networking Type Virtual Hub NVA Id Source Network A Public IP Addresses Enable Source NAT () Use the above Public IP addr	Search  Add  Delete  Add Frontend Provide Configuration for Name * Protocol *  Frontend IP * Backend IP * Backend Port *  Address Trar resses	d Setting Frontend Setting InboundApp1 TCP UDP VWAN-CNGFW-public-ip 8080 192.168.0.4	
Alerts Automation ame > VWAN-CNGFW Automation Automatio	Letworking & NAT Save Discard Networking Type Virtual Hub NVA Id Source Network A Public IP Addresses Enable Source NAT ()	Search  Add  Delete  Add Frontend Provide Configuration for Name * Protocol *  Frontend IP * Backend IP * Backend Port *  Address Trar resses	d Setting Frontend Setting InboundApp1 TCP UDP VWAN-CNGFW-public-ip 8080 192.168.0.4	

Once the destination NAT rule has been added, click **Save** to deploy this configuration on to the Cloud NGFW resource:



Home > VWAN-CNGFW

	working & NAT					
	🔚 Save 🗙 Discard					
😑 Overview	Virtual Hub	ravi	VWANHub			
Activity log	NVA Id	VW	AN-CNGFW-nva			
Access control (IAM)						
🗳 Tags						
	Source Network A				7	
Settings	Public IP Addresses	VW	AN-CNGFW-public-ip	$\sim$		
Networking & NAT	Enable Source NAT 🕠	<b>~</b>				
획 Rulestack	Use the above Public IP addr	esses 🗸				
Log Settings						
ONS Proxy						
💺 Rules	Destination Netwo	ork Address T	ranslation (DNAT)			
Properties	Search					
🔒 Locks	🕂 Add 🗎 Delete					
Monitoring	Name	Protocol	Frontend IP	Frontend Port	Backend IP	Backend Port
III Alerts	InboundApp1	ТСР	VWAN-CNGFW-public-ip	8080	192.168.0.4	80
Automation						

#### After saving the configuration, the screen would look as shown below

Home > VWAN-CNGFW

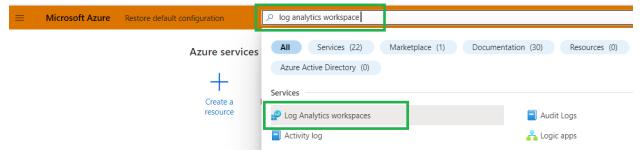
Search	« 🖉 Edit 🕐 Refre	esh				
Overview	A		Virtual WAN Hub			
Activity log	Virtual Hub		raviVWANHub			
Access control (IAM)	NVA Id		VWAN-CNGFW-nva			
Tags						
tings						
Networking & NAT			s Translation (SNAT)			
Rulestack	Public IP Addresse Enable Source NA		172.177.205.71			
.og Settings	Use the above Pu	0	<ul> <li>✓</li> </ul>			
DNS Proxy	ose the above ra	blie il dudiesses				
,						
Rules	Doctination	Notwork Ad	dress Translation (DI			
Properties	Search	I Network Au		NAI)		
	- Search					
Locks						
ocks toring	Name	Protocol	Frontend IP	Frontend Port	Backend IP	Backend Port



With this configuration in place, the address <u>http://frondendIP:8080</u> is redirected to App1 on port 80 through Cloud NGFW. This means that inbound traffic is now flowing through the Cloud NGFW.

### **Configure Logging**

 Before configuring Log settings on Cloud NGFW, create the Log Analytics workspace on Azure. Search for Azure Log Analytics workspace as shown below and click Log Analytics Workspaces service to add it to the workspace:



2. Click on Create option to create a new Log Analytics Workspace.

≡	Microsoft Azure	Restore default configuration	$\wp$ Search resources, services, and doc						
Home	>								
	Log Analytics workspaces 🖉 … Palo Alto Networks Inc. (paloaltonetworks.onmicrosoft.com)								
+ c	reate 🐻 Open recyc	cle bin   ଊ Manage view 🗸 🕐 Re	efresh 🞍 Export to CSV 😚 Open que						
Filter	for any field	Subscription equals <b>all</b> Res	source group equals all $ imes$ Location equals						

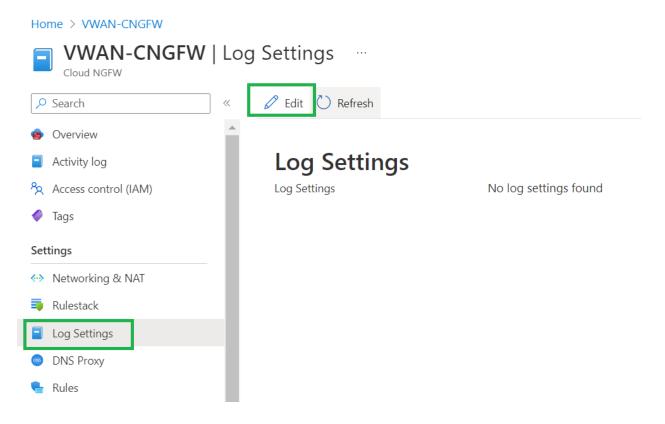
3. Create the **Log analytics workspace** as shown below. Make sure that the region is either US-East-2 or US-central:



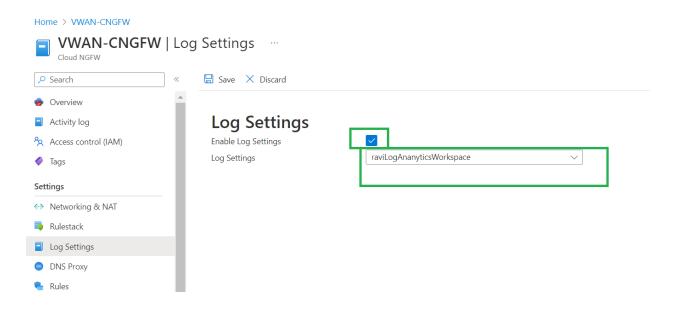
≡	Microsoft Azure	Restore defa	ult configuration	,⊃ Search	resources, services, and docs	(G+/)
Home >	> Log Analytics work	kspaces >				
Crea	te Log Anal	ytics wo	orkspace			
	-	-	-			
Basics	Tags Review	+ Create				
· · · ·			management unit of Azure M og Analytics workspace. <u>Learr</u>		There are specific considerations	×
and oth					m your monitored resources in jical storage unit where your lo	
Project	t details					
	the subscription to ma e all your resources.	anage deploye	d resources and costs. Use	resource gro	oups like folders to organize an	ıd
Subscri	iption * 🛈		AzureTME			$\sim$
	Resource group * 🤅	)	(New) raviCngfwLogWorl	kspaceRG		$\sim$
			Create new			
Name '	ce details * (i)	_ Г	raviCngfwLogWorkspace			~
Region	* ①		East US 2			
Region	0		Last ob L			
Revie	ew + Create	« Previous	Next : Tags >			

4. Now configure Cloud NGFW Log settings using the Log Analytics workspace created above. Go to the Cloud NGFW resource, select the **Log Settings** section, and click the **Edit** option to choose the Log analytics workspace that has just been created:





5. Enable **Log Settings** and choose the log analytics workspace created in the previous step from the drop-down, and save the configuration:





### Add Spoke(Application) VNets as Virtual Network Connections to Virtual WAN

1. Add spoke vnets as **Virtual Network Connections** to Virtual WAN Hub by clicking on **"+ Add Connection**" as shown below.

Home > CNGFW-VWAN						
	l   Vir	tual network	connections	Å		
	~	+ Add connection	🕐 Refresh			
Connectivity	•	Hub	Hub region	Virtual network	Connection Name	Connection Provisio
👾 Hubs			5			
VPN sites		raviVWANHub ∢	East US 2	Virtual networks (	0)	
& User VPN configurations						
🛕 ExpressRoute circuits						
${\mathbb Q}_{\mathbb P}$ Virtual network connections	٠.					

2. Select Spokel VNet as Virtual Network while adding the connection as shown below.

Home > CNGFW-VWAN			Add connection		×
CNGFW-VWAN   Vi	rtual network	connections	Connection name *		
₽ Search «	+ Add connection	n 🖒 Refresh	CngfwSpokeApp1		~
Connectivity	Hub	Hub region	Hubs * ①		
👾 Hubs	raviVWANHub	East US 2	raviVWANHub		$\sim$
VPN sites	raviVWANHub	East US 2	Subscription *		
🔠 User VPN configurations			AzureTME		$\sim$
🙏 ExpressRoute circuits			Resource group *		
Virtual network connections			raviCNGFW-VWAN		$\checkmark$
Monitor			Virtual network * raviCngfwApokeApp1-vnet		$\sim$
🔝 Connection monitor			Routing configuration ①	1	
Insights			Propagate to none ①		
Automation			Yes No		
🖧 Tasks (preview)			Associate Route Table		
😫 Export template					$\sim$
Support + troubleshooting			Propagate to Route Tables 0 selected		$\sim$
📀 Getting started					
R New Support Request			Create		

3. Similarly select Spoke2 VNet as Virtual Network while adding the connection as shown below.



Home > CNGFW-VWAN				Add connection	>
CNGFW-VWAN	Virtua	network	connections		
Virtual WAN				Connection name *	
₽ Search	« +	Add connection	🕐 Refresh	CngfwSpokeApp2	~
Connectivity	^ H	ub	Hub region	Hubs * O	
👾 Hubs				raviVWANHub	$\sim$
VPN sites	ra	wiVWANHub	East US 2	Subscription *	
User VPN configurations	4			AzureTME	$\sim$
▲ ExpressRoute circuits				Resource group *	
Virtual network connections				raviCNGFW-VWAN	$\sim$
				Virtual network *	
Monitor				raviCngfwSpokeApp2-vnet	$\sim$
🕵 Connection monitor				Routing configuration ①	
💡 Insights				Propagate to none ①	
Automation				Yes No	
Tasks (preview)				Associate Route Table	
					$\sim$
🔄 Export template					
Support + troubleshooting				Propagate to Route Tables	_
				0 selected	$\sim$
📀 Getting started				Create	
🙊 New Support Request					

4. After successful addition of the connections, it would look something as shown below. Make sure that the status is in **Connected** state.

Home > CNGFW-VWAN								
CNGFW-VWAN	Virt	ual netwo	ork conne	ections 🛧 …				×
₽ Search	] «	+ Add conne	ection 💍 Refr	resh				
Connectivity	*	Hub	Hub region	Virtual network	Connection Name	Connection Provisioning Status	Connectivity Status	Associated to Route Table
👾 Hubs		nup	Hub region	VIFTUAI NETWORK	Connection Name	Connection Provisioning status	connectivity status	Associated to Route Table
VPN sites		raviVWANHub	East US 2	✓ Virtual networks (2)		Succeeded (2)	Connected (2)	
User VPN configurations				raviCngfwApokeApp1-vnet	CngfwSpokeApp1	Succeeded	Connected	raviVWANHub/defaultRouteTable
▲ ExpressRoute circuits				raviCngfwSpokeApp2-vnet	CngfwSpokeApp2	Succeeded	Connected	raviVWANHub/defaultRouteTable
		4						•
Virtual network connections	1							
Monitor								
Connection monitor								
Insights								

#### **Configure VWAN Hub Routing Intent and Routing Policies**

- 1. Routing Policies within Virtual WAN Hub will be used to route traffic through Cloud NGFW service.
- 2. To route Internet bound traffic and Private Traffic(Spoke to Spoke), configure the next hop as VWAN Cloud NGFW as shown below



Home > raviVWANHub									
Rou virtual HUB	iting Intent and R	outing Policies							
✓ Search «	🔚 Save 🗙 Cancel 📋	Delete							
🔆 Overview	Configure routing policies fo	or raviVWANHub Virtual Hub							
Connectivity	Routing Policies for Internet Traffic apply to all connections connected to the Virtual Hub								
VPN (Site to site)	Pouting Policies for Drivato 1	Routing Policies for Private Traffic apply to all private traffic destined for addresses in the Private Traffic Prefixes below (regardless of the source) that enters the virtual hub							
🙏 ExpressRoute	Routing Policies for Private I		ne Frivate franc Frenkes below (	regardiess of the source) that enters the virtual hub					
Luser VPN (Point to site)	Internet traffic		Next Hop Resource						
	SaaS solution	~	VWAN-CNGFW-nva	~					
Routing	Private traffic		Next Hop Resource						
Routing Intent and Routing	SaaS solution	~	VWAN-CNGFW-nva	×					
Policies	Private Traffic:	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16,							
⊗ BGP Peers	invate name.	10,0,0,0,0, 112,10,0,0,12, 102,100,0,0,10,							
🔅 Route Tables									
Effective Routes									

3. After configuring Routing Policies, check for the routing table to be updated to route traffic through Cloud NGFW

Click on Route Tables and select Default routing table

Home	>	CNGFW-VWAN	Hubs >	raviVWANHub
nome	/	CIVOLVV VV/IIV	Thubs /	

raviVWANHub   Virtual HUB	Rou	te Tables 🛷 …					
	«	+ Create route table 💧 R	lefresh				
👾 Overview		Route Tables					
Connectivity		Name	$\uparrow_{\downarrow}$	Provisioning State	$\uparrow_{\downarrow}$	Labels	
VPN (Site to site)		Default		Succeeded		default	
👗 ExpressRoute		None		Succeeded		none	
🛃 User VPN (Point to site)							
Routing							
Routing Intent and Routing Policies							
BGP Peers							
📚 Route Tables							
Effective Routes							

This will provide the details related to the routes associated with the Default Routing table. Over here we can see that any traffic going out to internet or to other spoke VNets will be routed through Cloud NGFW



Home CNGFW-VWAN	Hubs > raviVV	VANHub	Route Tables >				
Edit route table	<b>.</b>						
Basics Labels Asso	ciations Pro	pagation	IS				
Project details							
Subscription		AzureT	ME				$\sim$
Resource group		raviCNO	GFW-VWAN				
Resource group		TaviCive	JEVV-VVVAIN				~
Instance details							
Name		default	RouteTable				
View effective routes for the	nis table						
Branch routes apply to aggregated address of			xpressRoute circuits a	ind Use	r VPN connections. Destina	ation prefix can be	
Route name	Destination typ	pe	Destination prefi	x	Next hop	Next Hop IP	
_policy_Internet	CIDR		0.0.0/0		VWAN-CNGFW-nva		
_policy_PrivateTraffic	CIDR		10.0.0.0/8,172.16.	0	VWAN-CNGFW-nva		
	CIDR	$\sim$			~	]	
•							•

# Review + create Previous Next : Labels >

## **Testing traffic**

#### **Test Inbound Traffic**

- 1. To validate the inbound connection towards App1, try to access <u>http://<Cloud</u> <u>NGFW Public IP>:8080.</u>
- 2. As per the Destination NAT configuration on Cloud NGFW, if <u>http://<Cloud</u> <u>NGFW Public IP>:8080</u> is accessed, the connection will be redirected to Appl after inspection by Cloud NGFW.

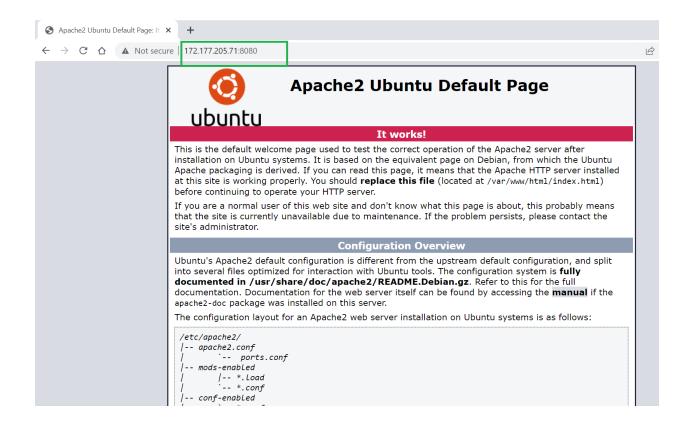


Make sure to allow HTTP traffic on the application server network interface. For this, go to Appl, select **Networking**, and add an inbound port rule that allows any HTTP inbound traffic. Configure the source as **IP Addresses**, port as 80, protocol as TCP, and set the **Action** to**Allow:** 

Virtual machine	etworking 🖈							×
	🖉 Attach network i	nterface 🖉 Detach network interface 🛛 🔗 Feedba	ck					
📮 Overview 🔺	ravidemoapp1158							
Activity log	IP configuration ①							
Access control (IAM)	ipconfig1 (Primary	) ~						
🗳 Tags	S Network Interf	face: ravidemoapp1158 Effective security rule:	s Troubleshoot VM con	nection issues Topology ()				
Diagnose and solve problems		net: raviDemoApp1_group-vnet/raviDemoApp1Subnet		1 55	Accelerated networking: E	nabled		
Settings								
2 Networking	Inbound port rul			- -				
Ø Connect		ity group raviDemoApp1-nsg (attached to network	c interface: ravidemoapp11	58)			Add inbour	nd port rule
	impacts o subm	ets, 1 network interfaces						
Bisks	Priority	Name	Port	Protocol	Source	Destination	Action	
<ul> <li>Disks</li> <li>Size</li> </ul>			Port 80	Protocol TCP	Source	Destination	Action Allow	
-	Priority	Name						
Size	Priority 310	Name AllowAnyHTTPInbound	80	TCP	Any	Any	Allow	
<ul> <li>Size</li> <li>Microsoft Defender for Cloud</li> </ul>	Priority 310 65000	Name AllowAnyHTTPInbound AllowVnetinBound	80 Any	TCP Any	Any VirtualNetwork	Any VirtualNetwork	<ul><li>Allow</li><li>Allow</li></ul>	
<ul> <li>Size</li> <li>Microsoft Defender for Cloud</li> <li>Advisor recommendations</li> </ul>	Priority 310 65000 65001	Name AllowAnyHTTPinbound AllowVinetinBound AllowAzureLoadBalancerinBound	80 Any Any	TCP Any Any	Any VirtualNetwork AzureLoadBalancer	Any VirtualNetwork Any	<ul><li>Allow</li><li>Allow</li><li>Allow</li><li>Allow</li></ul>	
Size Microsoft Defender for Cloud Advisor recommendations Extensions + applications	Priority 310 65000 65001	Name AllowAnyHTTPinbound AllowVinetinBound AllowAzureLoadBalancerinBound	80 Any Any	TCP Any Any	Any VirtualNetwork AzureLoadBalancer	Any VirtualNetwork Any	<ul><li>Allow</li><li>Allow</li><li>Allow</li><li>Allow</li></ul>	

If <u>http:/<Cloud NGFW Public IP>:8080/</u> is accessed, the following screen appears if the apache server was running as the default web server. Here, once the public IP of the Cloud NGFW was accessed, it will redirect the traffic to App1 on spoke-vnet1 where apache server was running. Since Inbound HTTP is enabled on App1, it will run the apache server that was deployed on App1.





#### Accessing logs

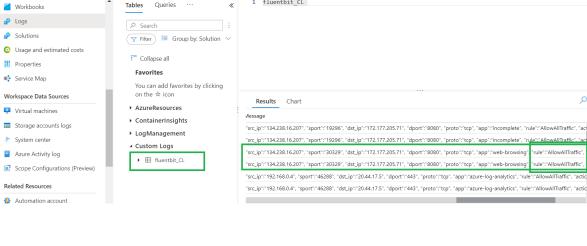
To verify that this particular inbound traffic was processed correctly by Cloud NGFW, go to the **Log Analytics workspace** and verify the logs as shown below.

Within Log analytics workspace **raviCngfwLogWorkspace**, navigate to the **Logs** section, select **Custom Logs** and select **fluentbit\_CL** and **run** the query to get the latest logs:



#### Home > Log Analytics workspaces > raviLogAnanyticsWorkspace

	护 New Query 1* 🛛 🛛 🕂	
🞽 Workbooks	PraviLogAnanyticsW Select scope	▶ Run Time range : Last 30 minu
₽ Logs	Tables Queries Functions ···· «	1 fluentbit_CL
P Solutions		
Usage and estimated costs	Search :	
Properties	Group by: Solution ∨	
🞼 Service Map	t <sup>™</sup> Collapse all	
Workspace Data Sources	Favorites	
Virtual machines	You can add favorites by clicking on the $lpha$ icon	Queries History
Storage accounts logs	<ul> <li>AzureResources</li> </ul>	:
System center	ContainerInsights	
Azure Activity log	▶ LogManagement	
Scope Configurations (Preview)	Custom Logs	
Related Resources	▶	
Automation account		
Log Analytics workspaces > raviLogAnanyticsWorkspace		
raviLogAnanyticsWorkspace   Lo	gs	
Log Analytics workspace		



Strata by Palo Alto Networks | SW NGFW | Cloud NGFW for Azure - Private preview

~

Q

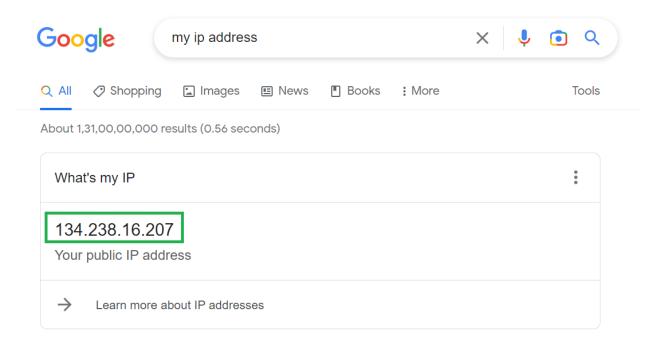
Results Chart	Q
Иessage	I
"src_ip":"134.238.16.207", "sport":"19296", "dst_ip":"172.177.205.71", "dport":"8080", "proto":"tcp", "app":"incomplete", "rule":"Allow	vAllTraffic", "action":"allow", '
"src_ip":"134.238.16.207", "sport":"19296", "dst_ip":"172.177.205.71", "dport":"8080", "proto":"tcp", "app":"incomplete", "rule":"Allow	vAllTraffic", "action":"allow", '
"src_ip":"134.238.16.207", "sport":"30329", "dst_ip":"172.177.205.71", "dport":"8080", "proto":"tcp", "app":"web-browsing", "rule":"A	llowAllTraffic", "action":' allov
"src_ip":"134.238.16.207", "sport":"30329", "dst_ip":"172.177.205.71", "dport":"8080", "proto":"tcp", "app":"web-browsing", "rule":"A	llowAllTraffic", "action":"allov

From the log, it can be seen that the source IP address is the IP address of the machine from which the request originated, and the destination IP address is Cloud NGFW public IP address, and it's hitting the **AllowAllTraffic** rule that has been created in the rulestack.

Home > VWAN-CNGFW-Irs									
Local Rulestack	-lrs   Ru	iles							×
₽ Search	] « Č	Refresh							
Overview	<b>A</b>								
Activity log		Local Rules	S						
Access control (IAM)			ists of local rules. A local rulesta	ick can be used on multiple fire	walls within the sam	e subscription.			
🗳 Tags		🕂 Add 🗎 Del	lete						
Settings		Priority	Name	Source	Destination	Constraints	Action	Logging	Egre
Properties		100	AllowAllTraffic	any	any	no	Allow	yes	Disa
🔒 Locks		100	AllowAlmanic	any	any	110	Allow	yes	Disa
Resources		50	BlockFacebook	any	match	no	DenyResetServer	yes	Disa
	- H.	•							۱.
💺 Rules									
ᠶ Profiles									

The screenshot below shows the IP address of the machine from which the request originated:





And the screenshot below shows the Public IP address of Cloud NGFW

Cloud NGFW   PREVIEW	Ŵ	☆ …								
➢ Search	«	🖒 Refresh 📋 Dele	ete							
Overview		∧ Essentials								JSON Viev
Activity log		Resource group (move)	): raviCNGFW-VWAN				Resource id	: /subscriptions/0683	d406-4d77-4bb7-b1a6-16	5c282b5d37/r
Access control (IAM)		Location	: East US 2				Туре	: paloaltonetworks.cl	oudngfw/firewalls	
Tags		Subscription (move)	: AzureTME				Public IPs	: 172.177.205.71		
r lags		Subscription ID	: 0683d406-4d77-4bb7	7-b1a6-165c282b5d3	37		Private IPs	: 10.10.112.4		
ettings							Source NAT Pub	lic IPs : 172.177.205.71		
Networking & NAT		Tags ( <u>edit</u> )	StoreStatus : DND	InstanceLife : 60	office : India	userID : rp	pegada			
Rulestack										

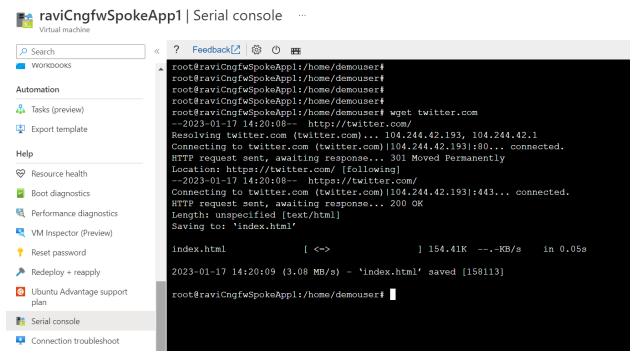
#### **Test Outbound Traffic**

To validate the outbound connection, try to access twitter.com from App1 as shown below. Go to App1, select the **Serial console** section and type the following command:

Wget twitter.com

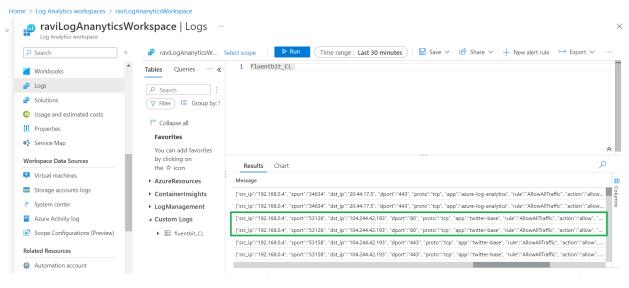


Home > raviCngfwSpokeApp1 >



The connection has been established. Verify that this traffic is being processed by Cloud NGFW by going to the **Log Analytics workspace**. <u>Repeat</u> the steps to access logs.

Run the query again to get the latest logs.





₽ Search «	🧬 raviLogAnanyticsW	$ \begin{array}{ c c c c c } \hline \hline & Run \\ \hline & Time range : Last 30 minutes \\ \hline & \Box \\ \hline & Save \lor & \raimes \\ \hline & Share \lor & + \\ \hline & New alert rule \\ \hline & \vdash \\ \hline & Export \lor \\ \hline & \\ \hline \\ \hline$	
Workbooks	Tables Queries ··· «	1 fluentbit_CL	
🖗 Logs	₽ Search :		
Solutions	Filter 🔚 Group by: !		
Usage and estimated costs			
Properties	T Collapse all		
🔄 Service Map	Favorites		
	You can add favorites by clicking on		
Workspace Data Sources	the 🖈 icon	Results Chart	Q
Virtual machines	AzureResources	Message	
Storage accounts logs	ContainerInsights		w
System center	LogManagement	("src_jp":"192.168.0.4", "sport":"34634", "dst_jp":"20.44.17.5", "dport":"443", "proto":"tcp", "app":"azure-log-analytics", "rule":"AllowAllTraffic", "action":"allo	w
<ul> <li>Azure Activity log</li> </ul>	Custom Logs	{"src_ip":"192.168.0.4", "sport":"53126", "dst_ip":"104.244.42.193", "dport":"80", "proto":"tcp", "app":"twitter-base", "rule":"AllowAllTraffic", "action":"allow",	
Scope Configurations (Preview)	▶ 目 fluentbit_CL	("src_ip":"192.168.0.4", "sport":"53126", "dst_ip":"104.244.42.193", "dport":"80", "proto":"tcp", "app":"twitter-base", "rule":"AllowAllTraffic", "action":"allow",	
		{"src_ip";"192.168.0.4", "sport";"53158", "dst_ip";"104.244.42.193", "dport";"443", "proto";"tcp", "app";"twitter-base", "rule";"AllowAllTraffic", "action";"allow"	,

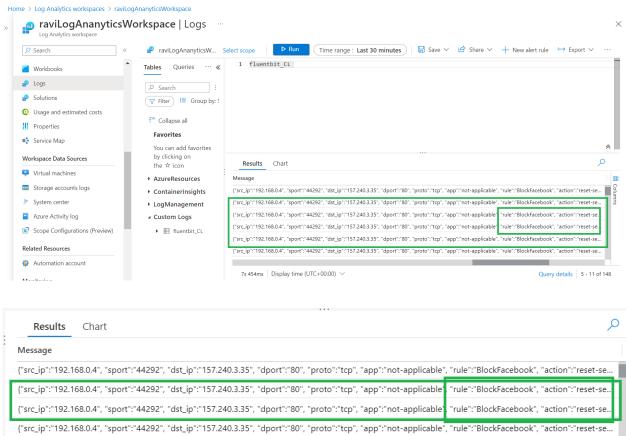
#### **Test Outbound Block Rule**

Now try to access Facebook. The traffic to Facebook should get blocked as per the rule configured. Go to App1, select**Serial console** and type the following command: *wget www.facebook.com* 

```
Home > raviCngfwSpokeApp1 >
raviCngfwSpokeApp1 | Serial console
       Virtual machine
                                            ? Feedback 🛛 🐯 🕛 🎟
"
                                             root@raviCngfwSpokeApp1:/home/demouser#
root@raviCngfwSpokeApp1:/home/demouser#
Workbooks
                                             root@raviCngfwSpokeApp1:/home/demouser#
Automation
                                             root@raviCngfwSpokeApp1:/home/demouser#
🔒 Tasks (preview)
                                             root@raviCngfwSpokeApp1:/home/demouser#
                                            root@ravichgiwspokeAppl:/home/demouser#
root@raviCngfwSpokeAppl:/home/demouser# wget www.facebook.com
--2023-01-17 14:23:52-- http://www.facebook.com/
Resolving www.facebook.com (www.facebook.com)... 157.240.3.35, 2a03:2880:f101:83:face:b00c:0:25de
Connecting to www.facebook.com (www.facebook.com) |157.240.3.35|:80...
😫 Export template
Help
\ensuremath{\mathfrak{S}} Resource health
Boot diagnostics
Performance diagnostics
VM Inspector (Preview)
📍 Reset password
≯ Redeploy + reapply
Ubuntu Advantage support
     plan
脂 Serial console
Connection troubleshoot
```



Connection won't be established. Go to **Azure Log Analytics** to validate that Cloud NGFW has blocked this connection as per the rRulestack configuration.



From these logs, it is evident that the traffic to Facebook was blocked after hitting the **BlockFacebook** rule. This confirms that Cloud NGFW is able to block traffic as per configured rulestack.

#### **Test East-West Traffic flow**

Validate east-west traffic flow by trying to send traffic from App1 to App2.

App2 IP address can be checked as shown below



Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20230117195801 | Overview > raviCngfwSpokeApp2 >

RaviCngfwSpo	keApp2   Serial console
₽ Search	≪ ? Feedback[∕] 🐯 () ⊞
Workbooks	<pre>root@raviCngfwSpokeApp2:/home/demouser# ifconfig eth0 eth0: flags=4163<up,broadcast,running,multicast> mtu 1500</up,broadcast,running,multicast></pre>
Automation	inet 172.16.0.4 netmask 255.255.255.0 broadcast 172.16.0.255
🖧 Tasks (preview)	<pre>inet6 fe80::6245:bdff:feb7:5ec8 prefixlen 64 scopeid 0x20<link/> ether 60:45:bd:b7:5e:c8 txqueuelen 1000 (Ethernet)</pre>
😫 Export template	RX packets 3174 bytes 30356380 (30.3 MB) RX errors 0 dropped 0 overruns 0 frame 0
Help	TX packets 3218 bytes 829259 (829.2 KB)
ныр	TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
$\bigotimes$ Resource health	root@raviCngfwSpokeApp2:/home/demouser#
Boot diagnostics	
<b>•••</b> • •	

#### On App1, execute the following command:

wget http://<App2 IP address>

Home > raviCngfwSpokeApp1 >

<b>raviCngfwSpoke</b>	App1   Serial console
✓ Search	≪ ? Feedback[ℤ   袋 ① ⊞
Overview	<pre>root@raviCngfwSpokeApp1:/home/demouse # wget http://172.16.0.42023-01-17 14:50:31 http://172.16.0.4/</pre>
Activity log	Connecting to 172.16.0.4:80 connected. HTTP request sent, awaiting response 200 OK
Access control (IAM)	Length: 10918 (11K) [text/html]
🗳 Tags	Saving to: 'index.html.1'
Diagnose and solve problems	index.html.1 100%[====>] 10.66KKB/s in 0s
Settings	2023-01-17 14:50:31 (52.6 MB/s) - `index.html.1' saved [10918/10918]
🧟 Networking	<pre>root@raviCngfwSpokeApp1:/home/demouser# root@raviCngfwSpokeApp1:/home/demouser#</pre>
~ -	nost (now Configuration of the contract of the

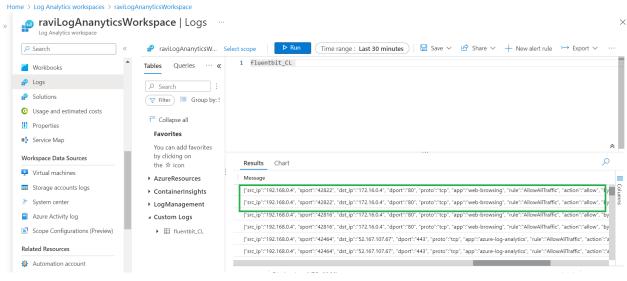
The connection has been established. Validate by going to the to **Azure Log Analytics** workspace:

After running the query, make sure you have sorted the logs based on TimeGenerated to see the latest logs on the top of the list.



#### Home > Log Analytics workspaces > raviLogAnanyticsWorkspace

🔎 Search	« 🔐 raviLogAnanyticsW S	Select scope Prun (Time range : Last 30 minu
<b>Workbooks</b>	Tables Queries ···· «	1 fluentbit_CL
₽ Logs	Search :	
P Solutions	( ↓ Filter ) ↓ Group by: !	
<ol> <li>Usage and estimated costs</li> </ol>		
Properties	↑ Collapse all	
🔹 Service Map	Favorites	
Workspace Data Sources	You can add favorites by clicking on the な icon	Results Chart
Virtual machines	AzureResources	TimeGenerated [UTC] ↑↓ ···· FirewallName s
Storage accounts logs	<ul> <li>ContainerInsights</li> </ul>	> 1/17/2023, 2:51:23.534 PM VWAN-CNGFW
System center	LogManagement	> 1/17/2023, 2:51:23.534 PM VWAN-CNGFW
Azure Activity log	Custom Logs	> 1/17/2023, 2:51:04.686 PM VWAN-CNGFW
Scope Configurations (Preview)	► 目 fluentbit_CL	> 1/17/2023, 2:51:04.686 PM VWAN-CNGFW
		> 1/17/2023, 2:50:53.219 PM VWAN-CNGFW





Results	Chart										Q
Message											
{"src_ip":"	192.168.0.4"	"sport":"42822	", "dst_ip":"172	.16.0.4", '	"dport":"80",	"proto":"tcp",	"app":"web-brows	ing", "rule":"/	AllowAllTraffic",	"action":"allow",	, "by
{"src_ip":"	192.168.0.4"	, "sport":"42822	", "dst_ip":"172	.16.0.4", '	"dport":"80",	"proto":"tcp",	"app":"web-brows	ing", "rule":"/	AllowAllTraffic",	"action":"allow",	, by
{"src_ip":"	192.168.0.4"	, "sport":"42816	", "dst_ip":"172	.16.0.4", '	"dport":"80",	"proto":"tcp",	"app":"web-brows	ing", "rule":"/	AllowAllTraffic",	"action":"allow",	, "by
{"src_ip":"	192.168.0.4"	, "sport":"42816	", "dst_ip":"172	.16.0.4", '	"dport":"80",	"proto":"tcp",	"app":"web-brows	ing", "rule":"/	AllowAllTraffic",	"action":"allow",	, "by

From these logs, it is visible that the traffic sent between App1 (192.168.0.4) and App2 (172.16.0.4) is going through the Cloud NGFW service and hitting the **AllowAllTraffic** rule which is part of the local rulestack.

Thus the inbound, outbound, and east-west traffic has been tested and is flowing through the Cloud NGFW service.

### Resources

# Contact

For any support, please email <u>cloud-ngfw-azure@paloaltonetworks.com</u> or reach out to your SE/CE.

