
Cloud NGFW for Azure in 7 steps

Quick Start Guide

v 1.2 (October 2023)

Get started with Cloud NGFW for Azure

Summary

Cloud NGFW for Azure is a Firewall as a service jointly offered by Palo Alto Networks and Microsoft Azure. The below list includes the required steps to get started with the Cloud NGFW. The more detailed instructions are described in the [Cloud NGFW for Azure Deployment Guide](#).

Supported Regions

- North America: **East US, East US 2, Central US, West US, West US 2, West US 3, Canada Central**
- Europe: **West Europe, North Europe, UK South, UK West**
- Asia Pacific: **Australia East, Australia Southeast, East Asia**

Deployment Models

- Virtual Network - hub-and-spoke using VNet peering and User Defined Routing (UDR)
- Virtual WAN - virtual hub using Routing Intent and Policies.

Security Policy Management

- Azure Portal - security policies are configured using Local Rulestack
- Panorama - security policies are configured and managed using Palo Alto Networks Panorama instance

Traffic Flows

- Outbound - secure traffic from VNet, on-prem, branch, and VPN to the Internet
- Inbound - secure traffic from the Internet toward the workloads in Azure
- Lateral - secure East-West traffic between VNets, on-prem, branch and VPN

Security Capabilities - Azure Portal managed

- Security Services: Threat Prevention, URL Filtering
- Best Practice Security Profiles: IPS Vulnerability, Anti-Spyware, Antivirus, File Blocking
- Security Rules: App-ID, URL Category, FQDN list, and Prefix List
- Web based Threat Protection: URL Categories and Filtering
- Encrypted Threat Protection: SSL Forward Proxy with the Azure Key vaults integration

Security Capabilities - Panorama managed

- Security Services: Advanced Threat Prevention, Advanced URL Filtering, WildFire, DNS Security
- Security Rules: App-ID, Custom App-ID, User-ID, Content-ID, URL Category, Custom URL Category, FQDN list, Prefix List, External Dynamic List, Dynamic Address Group
- Web based Threat Protection: URL Categories and Filtering
- Encrypted Threat Protection: SSL Forward Proxy

Networking Capabilities

- Destination NAT for Inbound connections
- Source NAT for Outbound connections
- DNS Proxy

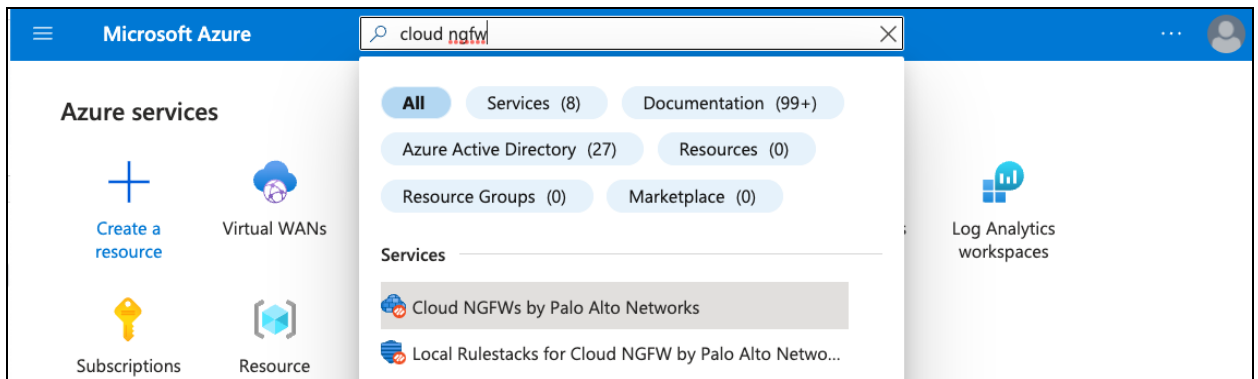
Logging

- Azure Log Analytics Workspace - Azure-managed
- Panorama Log Collector - Panorama-managed

Steps

1. Create Cloud NGFW

Search for Cloud NGFW service by using the terms “Cloud NGFW” and follow the creation wizard to provision the resource.



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

Home > Cloud NGFWs by Palo Alto Networks >

Create Cloud NGFW by Palo Alto Networks

Basics Networking Rulestack DNS Proxy Tags Terms Review + create

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

Project details

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

Subscription * ⓘ AzureTME

Resource group * ⓘ [Create new](#)

Firewall Details

Firewall Name * ⓘ

Region * ⓘ East US

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

For hub-and-spoke deployment model select or create a Hub VNet with Public and Private subnets

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

Home > Cloud NGFWs by Palo Alto Networks >

Create Cloud NGFW by Palo Alto Networks

Basics **Networking** Rulestack DNS Proxy Tags Terms Review + create

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

Network Type

Type *

Virtual Network
 Virtual Wan Hub

Configure virtual networks

Virtual Network * ⓘ (new) test-vnet

[Create new](#)

Private Subnet * ⓘ (new) subnet1 (10.8.0.0/26)

Public Subnet * ⓘ (new) subnet2 (10.8.1.0/26)

Public IP Address Configuration

Public IP Address(es) * ⓘ Create new
 Use existing

Public IP Address Name(s) * ⓘ test-public-ip

Source NAT Settings

Enable Source NAT ⓘ

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

If you are using an existing Hub VNet (minimum size of /25), make sure to have the required Public and Private subnets (minimum size of /26) and delegate them to “PaloAltoNetworks.Cloudngfw/firewalls” service

The screenshot shows the Microsoft Azure portal interface for a virtual network named 'cloudngfw-vnet-vnet'. The 'Subnets' page is displayed, showing a table of subnets. Two subnets, 'subnet2' and 'subnet1', are highlighted with a red box. Both subnets have an IPv4 address space of 10.1.1.0/26 and are delegated to the service 'PaloAltoNetworks.Cloudngfw/firewalls'. The 'Availability' column shows 56 for 'subnet2' and 55 for 'subnet1'. The 'IPv6' column shows a dash '-' for both.

Name	IPv4	IPv6	Availabl...	Delegated to
subnet2	10.1.1.0/26	-	56	PaloAltoNetworks.Cloudngfw/firewalls
subnet1	10.1.0.0/26	-	55	PaloAltoNetworks.Cloudngfw/firewalls

For the VWAN deployment model, select a pre-existing virtual hub.

The screenshot shows the Microsoft Azure portal interface for creating a Cloud NGFW by Palo Alto Networks. The breadcrumb navigation is 'Home > Cloud NGFWs by Palo Alto Networks >'. The main heading is 'Create Cloud NGFW by Palo Alto Networks'. Below the heading, there are tabs for 'Basics', 'Networking' (which is underlined), 'Rulestack', 'DNS Proxy', 'Tags', 'Terms', and 'Review + create'. A message states: 'Please configure your Firewall deployment with network requirements, i.e., Public IP CIDR and virtual network settings.'

Network Type

Type * Virtual Network Virtual Wan Hub

Virtual Wan Hub Details

Virtual Hub Name * ⓘ

Public IP Address Configuration

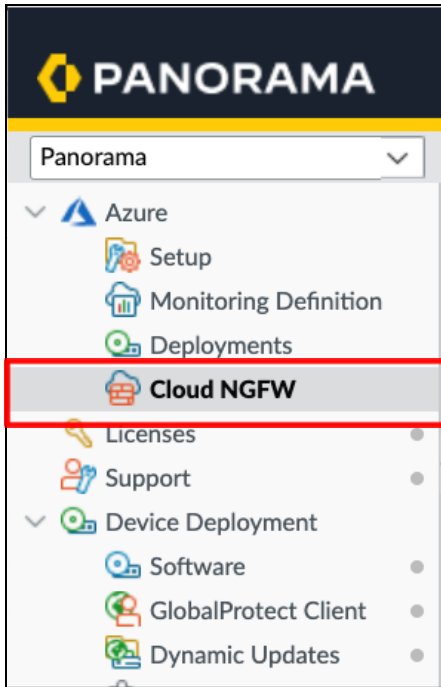
Public IP Address(es) * ⓘ

Public IP Address Name(s) * ⓘ

The dropdown menu for 'Virtual Hub Name' is open, showing two items:

- wan-hub-1
resource group: wwan-demo
- wan-hub-2
resource group: wwan-demo

For Panorama management, under the Azure Plugin add a Cloud Device Group and associate the Device Group, create a Template Stack, and specify the Device Certificate PIN.



The screenshot shows the 'Cloud Device Group' configuration dialog box. The 'Name' field is set to 'cngfw-az-'. The 'Description' field is empty. The 'Parent Device Group' is set to 'Shared'. The 'Template Stack' dropdown is open, showing a list of available template stacks: 'cngfw-az-anton-template-stack', 'cngfw-az-ravi-template-stack' (highlighted), 'cngfw-az-suhas', and 'cngfw-az-test-template-stack'. The 'Panorama IP' is 'cngfw-az-anton-template-stack', the 'Panorama HA Peer IP' is 'cngfw-az-ravi-template-stack', the 'Collector Group' is 'cngfw-az-suhas', and the 'Pin ID' is 'cngfw-az-test-template-stack'. The 'Confirm Pin ID' is 'New Template Stack'. The 'Pin Value' and 'Confirm Pin Value' fields are empty. The 'Zone mapping' section is collapsed. The 'OK' and 'Cancel' buttons are at the bottom right.

New Template Stack ?

Name cngfw-az-

OK Cancel

Generate the Registration string and copy it to the clipboard.

DASHBOARD ACC MONITOR Device Groups POLICIES OBJECTS NETWORK Templates DEVICE PANORAMA Commit

5 items

<input type="checkbox"/>	CLOUD DEVICE GROUP NAME	DESCRIPTION	TEMPLATE STACK	COLLECTOR GROUP	ASSOCIATED CLOUD NGFW RESOURCES	REGISTRATION STR
<input type="checkbox"/>	cngfw-az-DG1-GSS-PUBLIC-IP-TEST		cngfw-az-TS1-GSS-PUBLIC-IP-TEST		gs-netsec-fw1-tme-0419-with-ther	<input type="button" value="Generate"/>
<input type="checkbox"/>	cngfw-az-anton-rg		cngfw-az-anton-template-stack			<input type="button" value="Generate"/>
<input type="checkbox"/>	cngfw-az-Ravi-DG		cngfw-az-ravi-template-stack		cngfwwithpanorama	<input type="button" value="Generate"/>
<input type="checkbox"/>	cngfw-az-DG2-GSS-NO-THERMITE		cngfw-az-TS2-GSS-WITHOUT-THERMITE			<input type="button" value="Generate"/>

Registration String ?

Registration String

Expiration Date (yyyy/mm/dd)

Paste the string in the Cloud NGFW Panorama Registration String field.

The screenshot shows the 'Create Cloud NGFW by Palo Alto Networks' wizard in the Microsoft Azure portal. The current step is 'Rulestack'. The 'Managed by' section has 'Palo Alto Networks Panorama' selected. The 'Panorama Registration String' field contains 'base64 encoded Panorama Config String' and is highlighted with a red box. The 'Review + create' button is visible at the bottom left, and the 'Next : DNS Proxy >' button is visible at the bottom right.

The Cloud NGFW creation process takes approximately 20 minutes.

2. Connect to Cloud NGFW

VNet Deployment:

- Peer the spoke VNets with the Hub VNet where the Cloud NGFW was deployed to
- Create a Route Table with a default 0.0.0.0/0 route pointing to the Cloud NGFW Private IP address
- Associate the Route table to the spoke subnets

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

Home > Cloud NGFWs by Palo Alto Networks >

cloudngfw-vnet Cloud NGFW by Palo Alto Networks | PREVIEW

Search Refresh Delete

Overview

- Activity log
- Access control (IAM)
- Tags

Settings

- Networking & NAT
- Rulestack
- Log Settings
- DNS Proxy
- Rules

Essentials [JSON View](#)

- Resource group (move) : [vnet-demo](#)
- Location : Central US
- Subscription (move) : [AzureTME](#)
- Subscription ID : [REDACTED]
- Resource id : [REDACTED]
- Type : paloaltonetworks.cloudngf...
- Public IPs : [REDACTED]
- Private IPs : **10.1.0.4**
- Source NAT Public IPs : [REDACTED]
- Tags (edit) : [Click here to add tags](#)

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

Home > Cloud NGFWs by Palo Alto Networks > cloudngfw-vnet > vnet-demo > default-fwaas

default-fwaas | Routes Route table

Search + Add Refresh Give feedback

Search routes

Name ↑↓	Address prefix ↑↓	Next hop type ↑↓	Next hop IP addr... ↑↓
default	0.0.0.0/0	VirtualAppliance	10.1.0.4

Overview

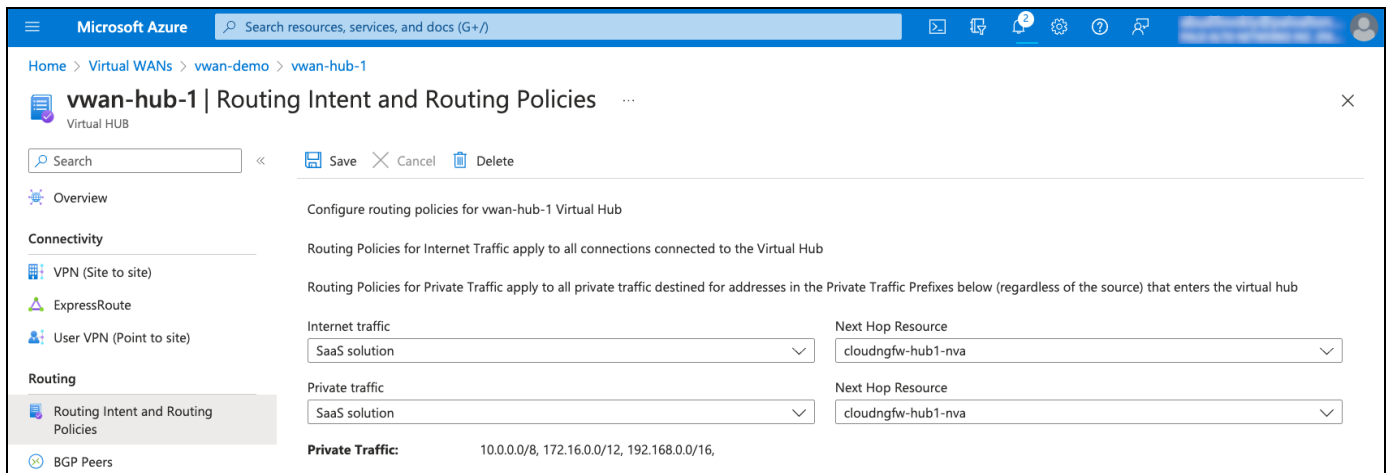
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Configuration
- Routes**

VWAN Deployment:

- Connect the spoke VNets to the Virtual Hub where the Cloud NGFW was deployed to as a SaaS
- Configure and save the Routing Intent and Policy to send the required traffic via the Cloud NGFW



3. Configure Networking

- Within the Cloud NGFW resource, configure DNAT rules to expose the workload for inbound flows
- Ensure SNAT is enabled for outbound flows

cloudngfw-vnet | Networking & NAT ☆ ...

Cloud NGFW by Palo Alto Networks

Search Save Discard

Overview
Activity log
Access control (IAM)
Tags

Settings
Networking & NAT
Rulestack
Log Settings
DNS Proxy
Rules
Properties
Locks

Support + troubleshooting
New Support Request

Monitoring
Alerts

Source Network Address Translation (SNAT)

Public IP Addresses: cloudngfw-vnet-public-ip

Enable Source NAT

Use the above Public IP addresses

Destination Network Address Translation (DNAT)

Search

+ Add Delete

Name	Protocol	Frontend IP	Frontend Port	Backend IP	Backe...
app1	TCP	cloudngfw-vnet-...	443	172.16.100.10	8443
app2	TCP	cloudngfw-vnet-...	8888	172.16.110.10	8889

- For the VNet deployment model, ensure that the NSG associated with the Hub VNet allows VNet-to-Internet traffic

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
<input type="checkbox"/> 100	AllowTagCustomAnyIn...	Any	Any	VirtualNetwork	Internet	<input checked="" type="checkbox"/> Allow

- Enable DNS Proxy for inspecting DNS traffic. This requires the spoke subnet to be configured with the DNS Server IP being the Cloud NGFW's Private IP address

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

Home > Virtual networks > spoke-vnet1

spoke-vnet1 | DNS servers

Virtual network

Search

- Microsoft Defender for Cloud
- Network manager
- DNS servers**
- Peerings
- Service endpoints
- Private endpoints
- Properties
- Locks

Warning: Virtual machines and Application gateways(v2 SKU) within this virtual network must be restarted to utilize the updated DNS server settings.

DNS servers ⓘ

Default (Azure-provided)

Custom

IP Address

10.1.0.4 ✓

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

Home > vnet-demo > cloudngfw-vnet

cloudngfw-vnet | DNS Proxy

Cloud NGFW by Palo Alto Networks

Search Save Discard

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings**
- Networking & NAT
- Rulestack
- Log Settings
- DNS Proxy**

DNS Proxy

DNS Proxy ⓘ

Disabled

Enabled

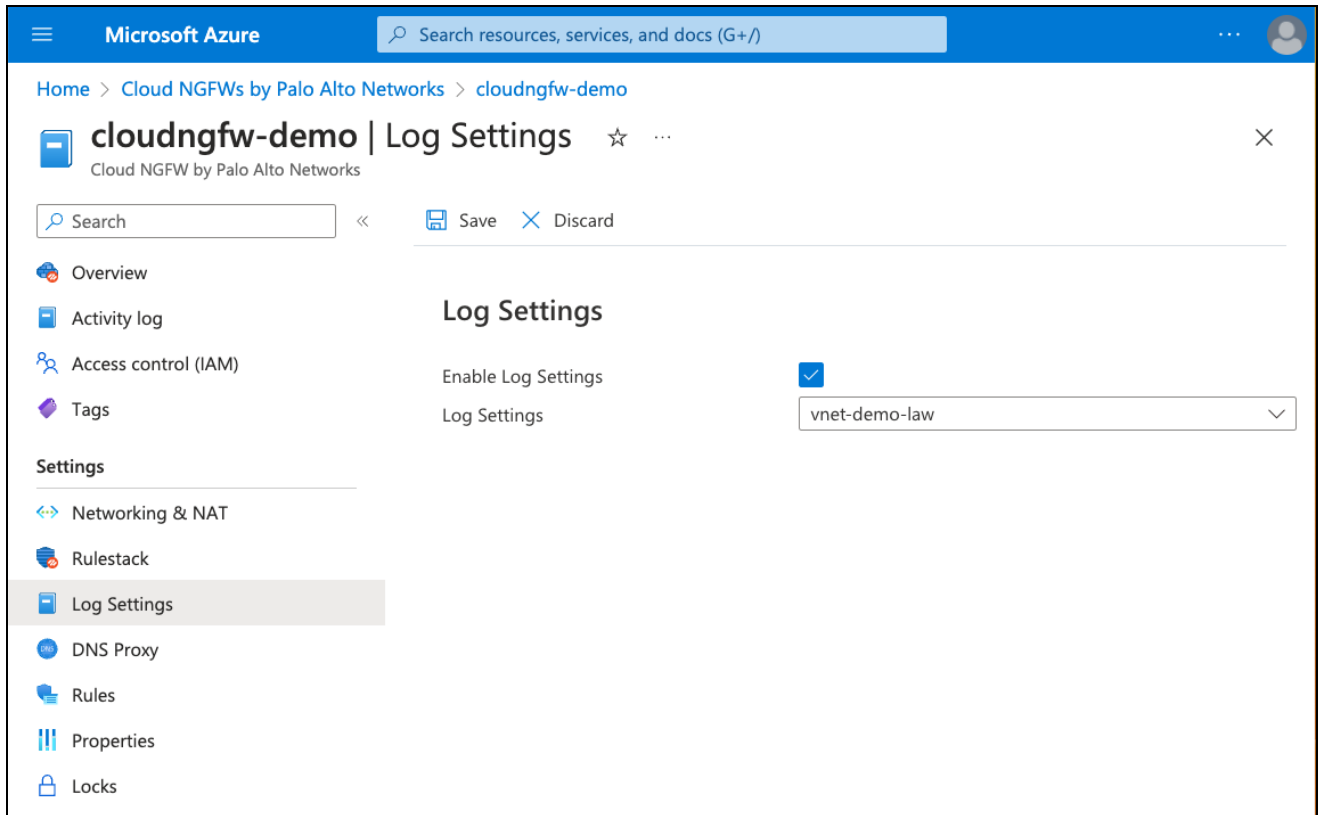
DNS Server

Default (Azure Provided)

Custom

4. Configure Logging

For Azure Portal managed Cloud NGFW, create a Log Analytics Workspace and associate it with the firewall resource.



When configuring the rules in the next step, make sure Logging is enabled on a per-rule basis.

Add Rule ✕

Define Rule Parameters

URL Category	<input checked="" type="radio"/> Any <input type="radio"/> Select
Match Criteria	<input checked="" type="radio"/> Any <input type="radio"/> Select
Protocol & Port	<input type="radio"/> Application Default <input checked="" type="radio"/> Any <input type="radio"/> Select
Match Criteria	<input type="radio"/> Allow <input checked="" type="radio"/> Deny <input type="radio"/> Drop <input type="radio"/> Reset both client and server
Actions	<input type="checkbox"/>
Actions	<input checked="" type="checkbox"/>
Egress Decryption	<input type="checkbox"/>
Logging	<input checked="" type="checkbox"/>

Validate
Cancel

5. Configure Firewall Rules

For Azure Portal managed Cloud NGFW locate the Local Rulestack and configure the Prefix Lists, FQDN Lists, and Rules as required. Use Application, URL Category, Port and protocol as filtering criteria.

Add Rule



Define Rule Parameters

Granular Controls

Application

Match Criteria

Any

Select

Applications

forticlient-update

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

Validate

Cancel

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

Home > Cloud NGFWs by Palo Alto Networks > cloudngfw-vnet > cloudngfw-example-rulestack

cloudngfw-example-rulestack | Rules ☆ ...

Local Rulestack for Cloud NGFW by Palo Alto Networks

Search << Refresh

Overview
Activity log
Access control (IAM)
Tags

Settings

Properties
Locks

Resources

Rules
Profiles
Prefix List
FQDN List
Certificates
Deployment
Managed Identity

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

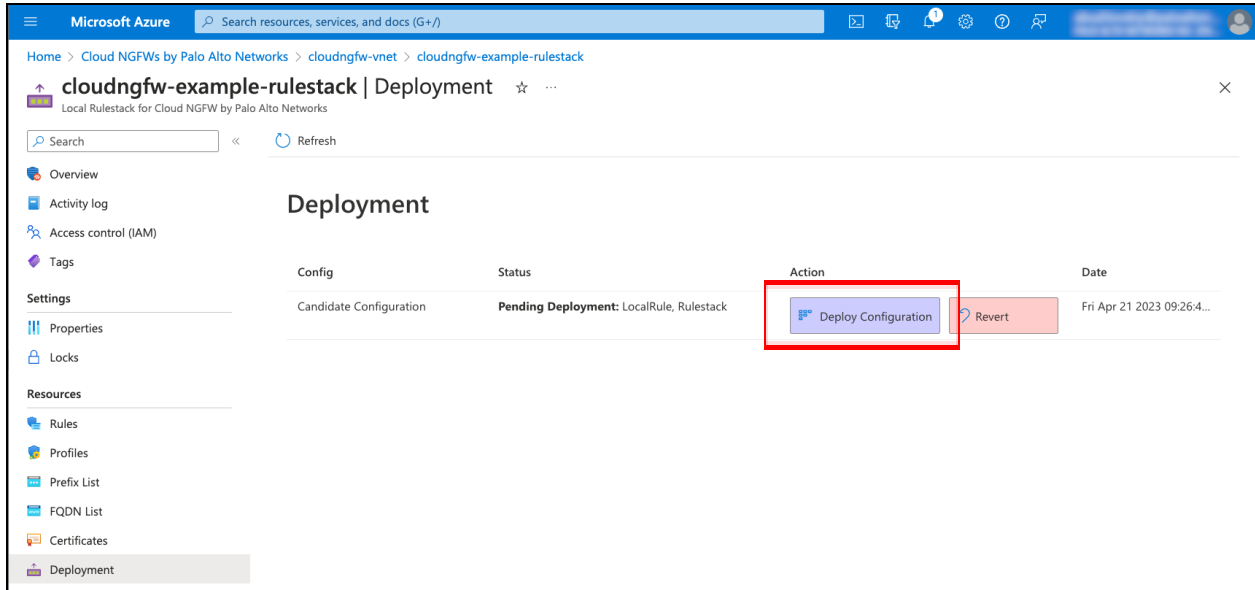
+ Add Edit Delete

Priority	Name	Source
100	block-url-categories	any
110	allow-web-browsing	any
120	allow-vnet-to-vnet-mongodb	match
130	allow-on-prem-rdp-to-vnet	match
900	deny-all	any

For Panorama-managed Cloud NGFW use the Device Group associated with the Cloud Device Group and configure the Prefix Lists, FQDN Lists, and Rules as required. Use Application, URL Category, Port and protocol as filtering criteria.

6. Deploy Configuration

- Deploy the candidate configuration under “Deployment”



- For Panorama-managed Cloud NGFW, locate the Template Stack associated with the Cloud NGFW and configure the security policies as required. Commit the configuration to Panorama and push it to devices
- Test the inbound flow scenario by accessing the firewall's public IP address in conjunction with the port configured in step 6 that exposes the test workload
- For the outbound flow scenario, access the test workload and test connectivity to the Internet
- For the lateral traffic scenario, test the appropriate scenarios for your environment between the workloads in the spoke VNets.