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

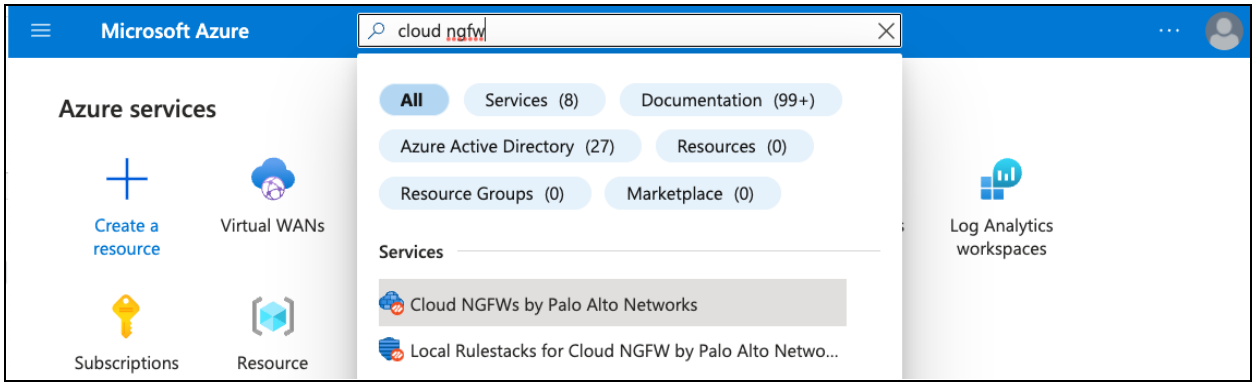
Logging

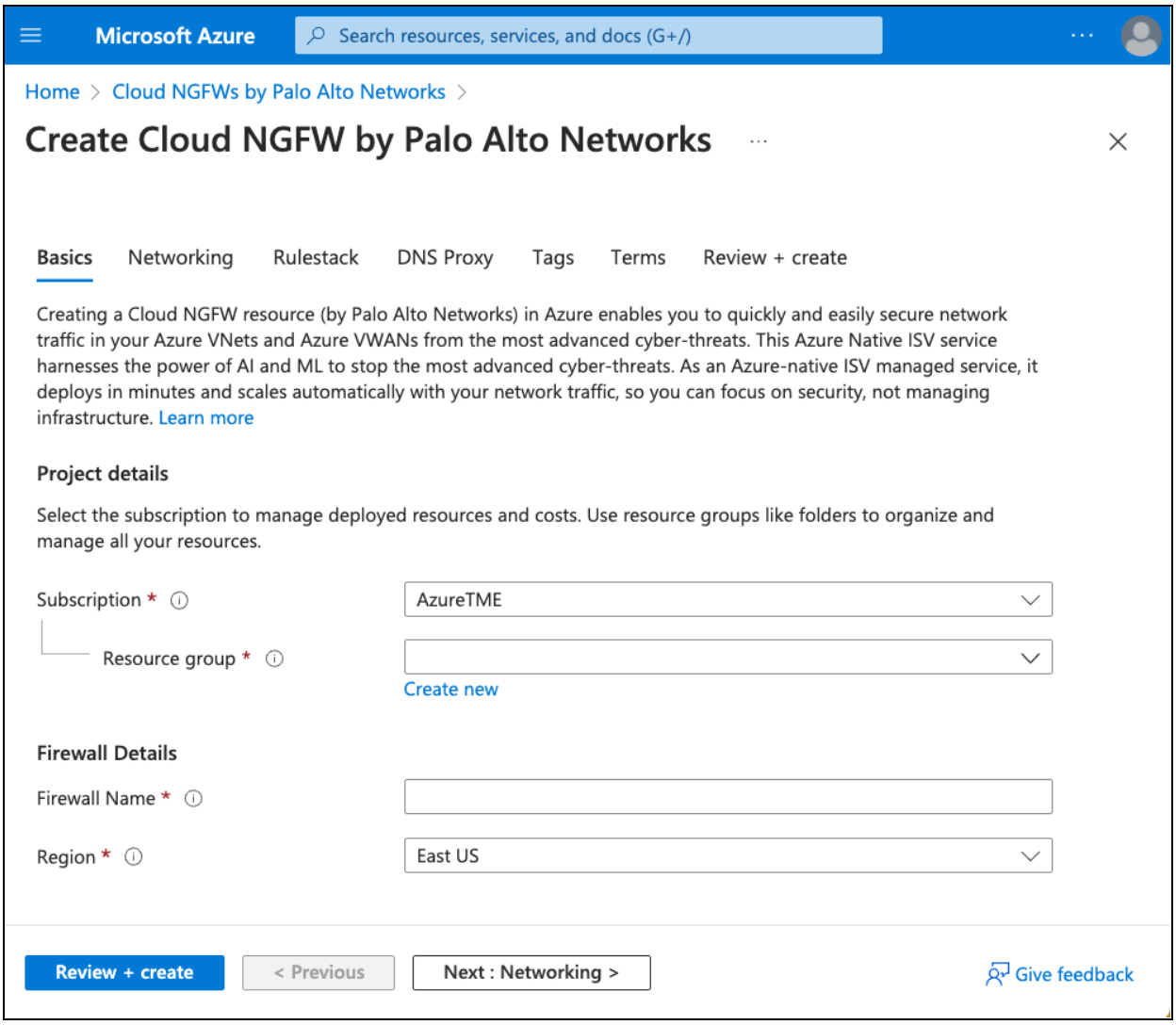
- Azure Log Analytics Workspace - Azure-managed
- Panorama Log Collector - Panorama-managed

Steps

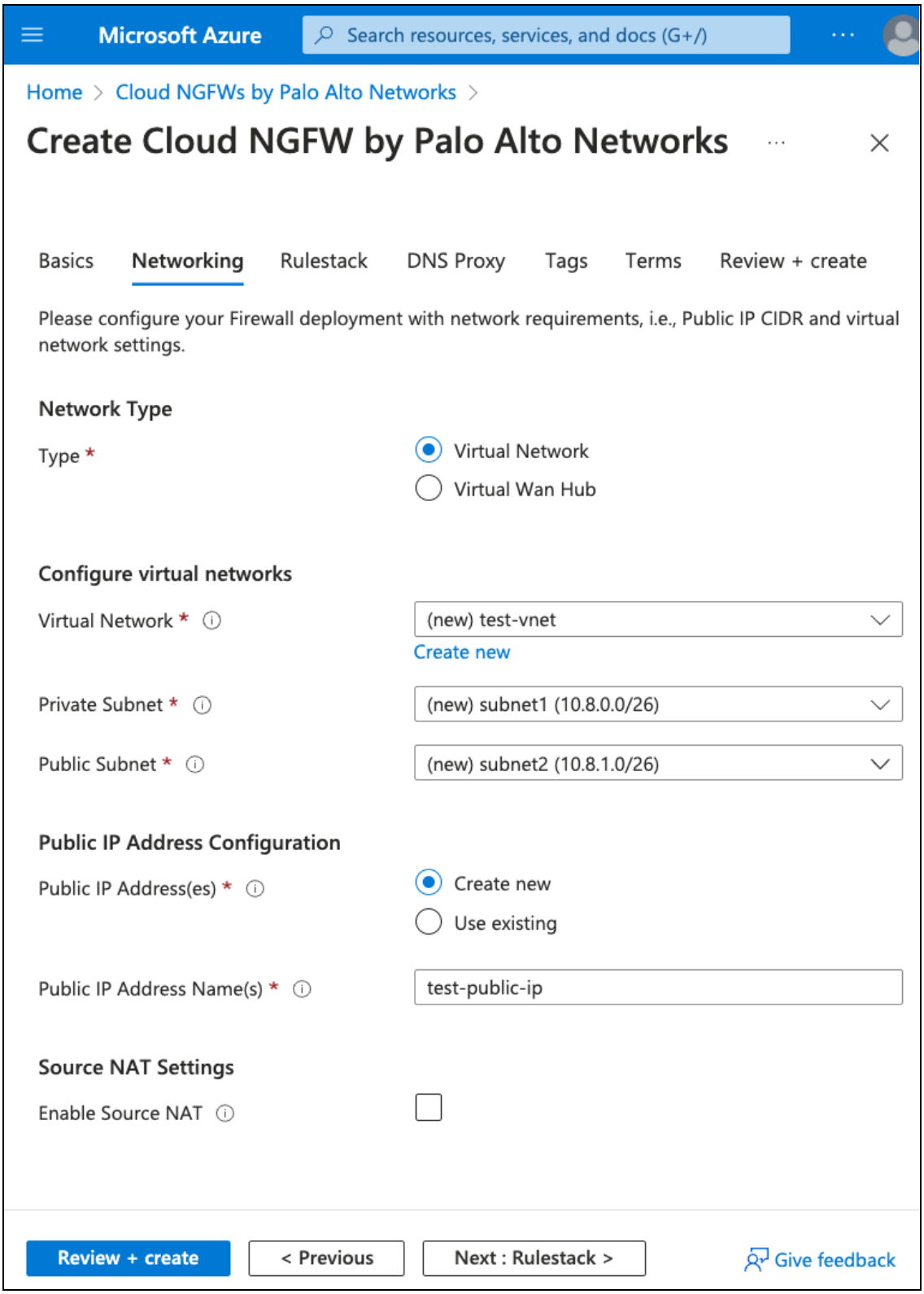
1. Create Cloud NGFW

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

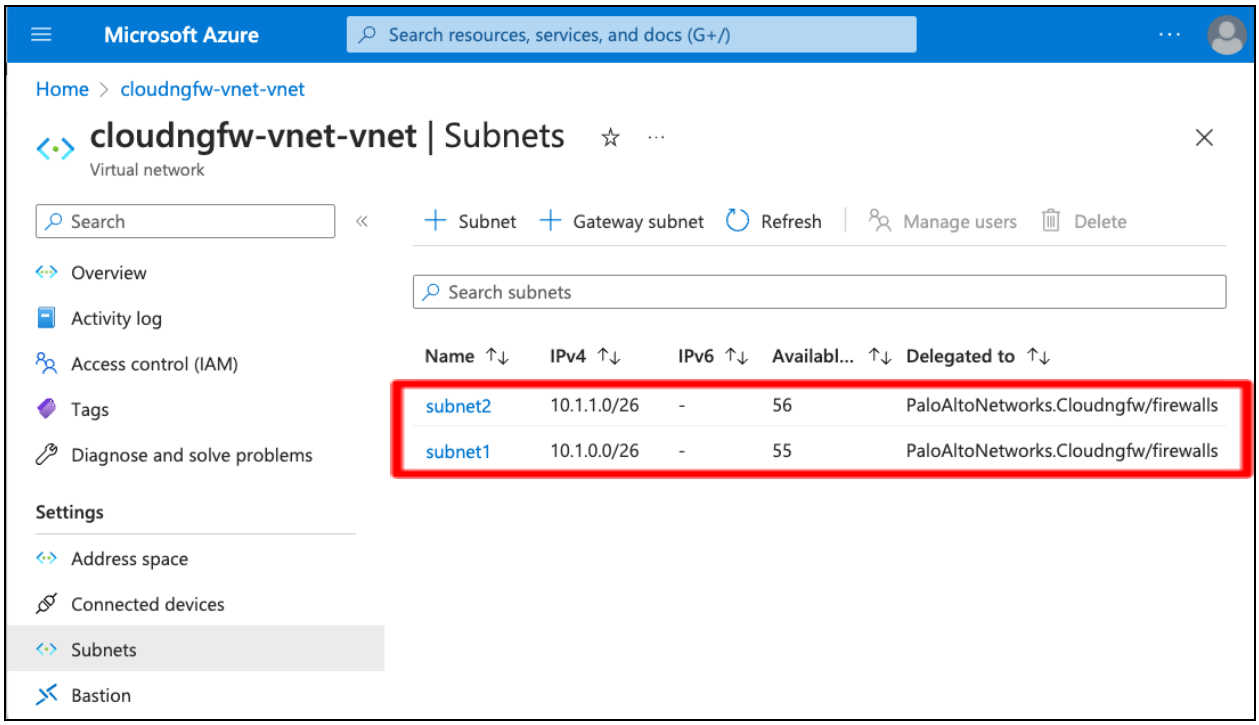




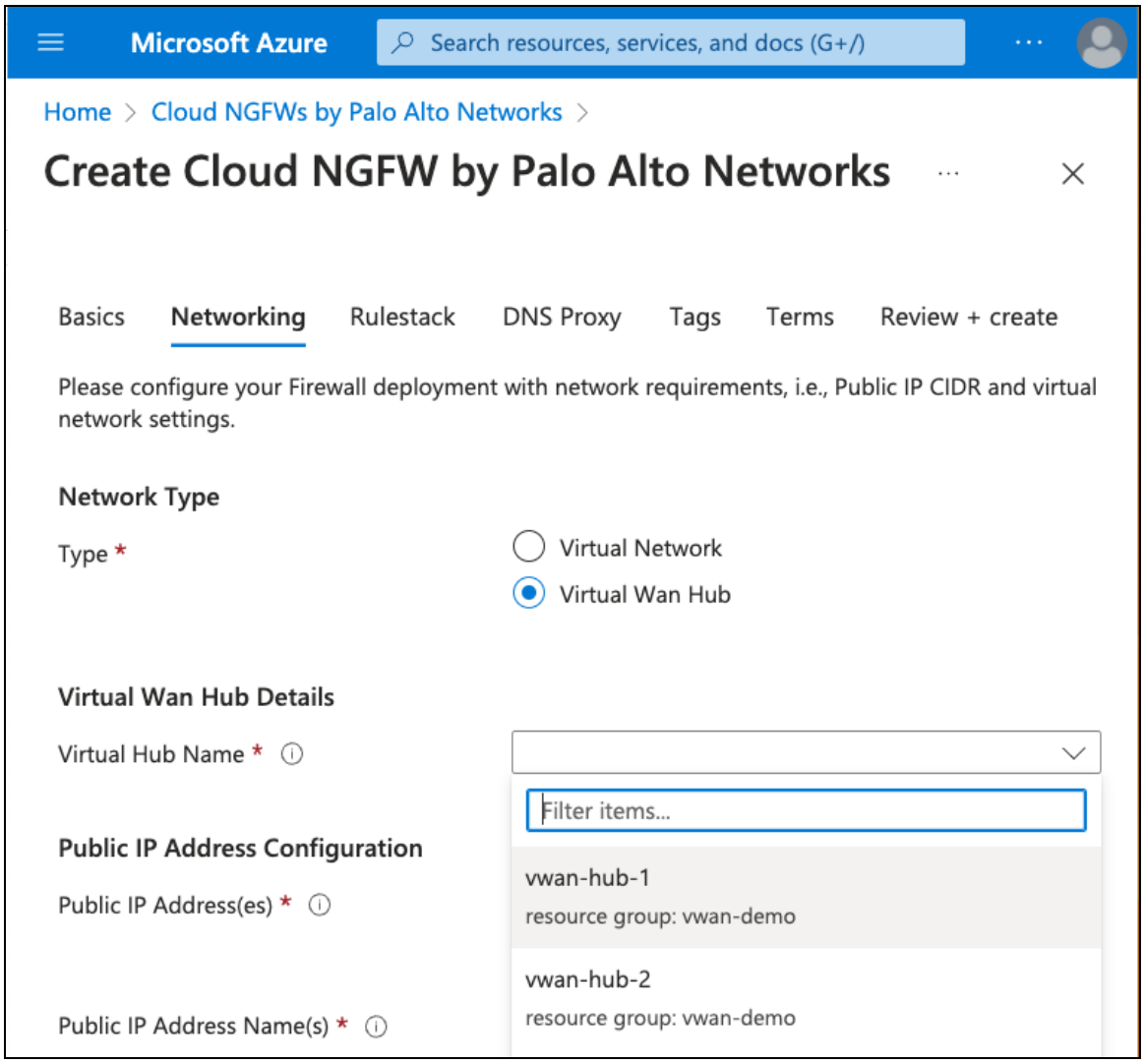
For hub-and-spoke deployment model select or create a Hub VNet with Public and Private subnets


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

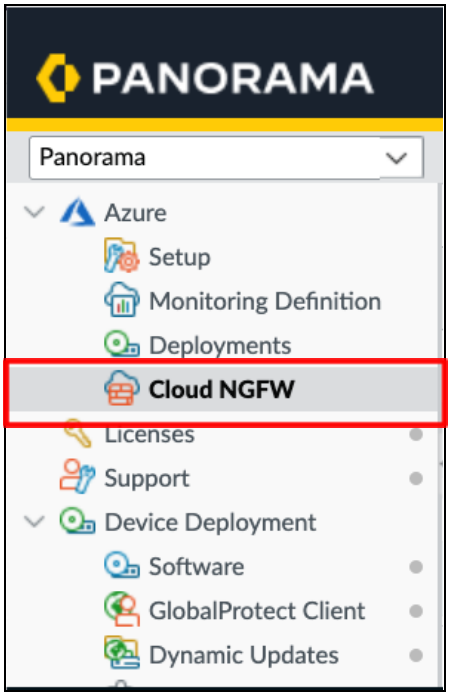
If you are using an existing Hub VNet (minimum size of /25), make sure to have the required Public and Private subnets (minimum size of /26) and delegate them to “PaloAltoNetworks.Cloudngfw/firewalls” service

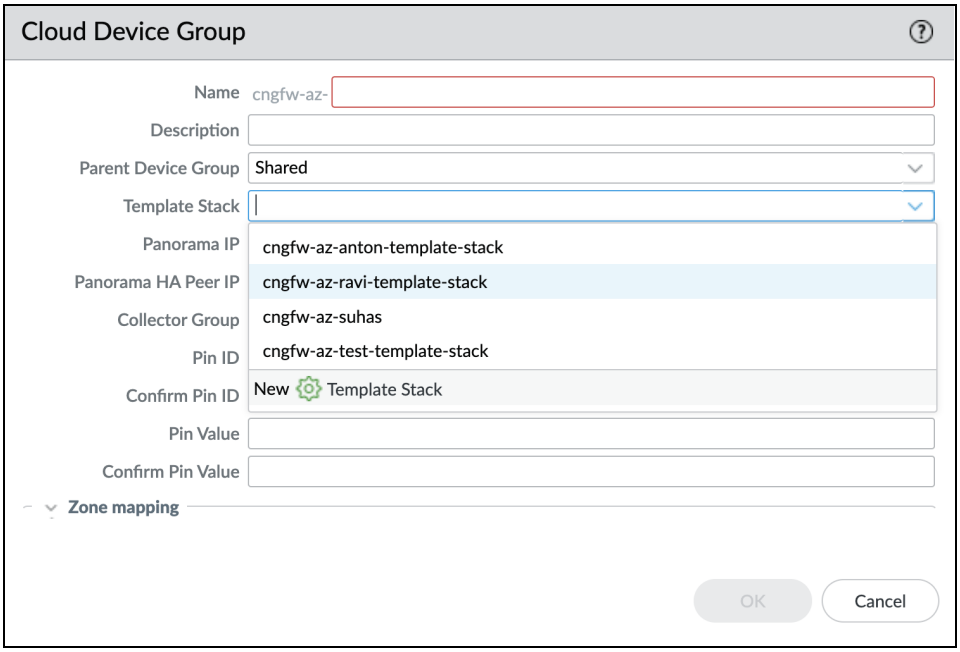


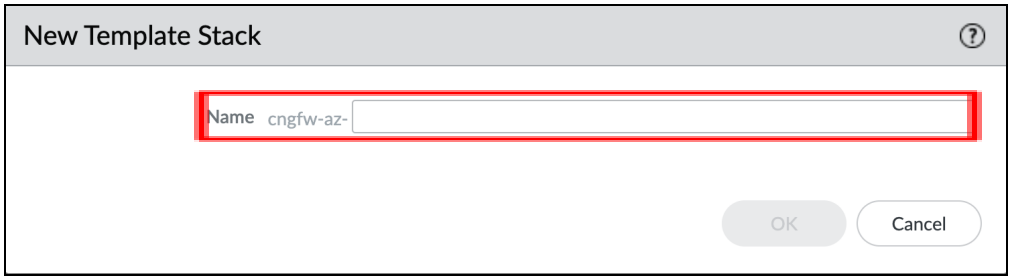
For the VWAN deployment model, select a pre-existing virtual hub.



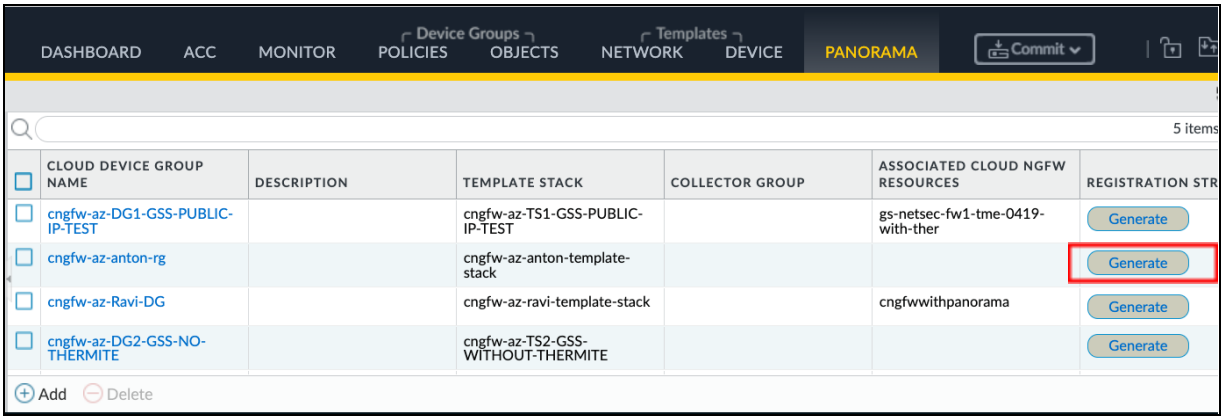
For Panorama management, under the Azure Plugin add a Cloud Device Group and associate the Device Group, create a Template Stack, and specify the Device Certificate PIN.

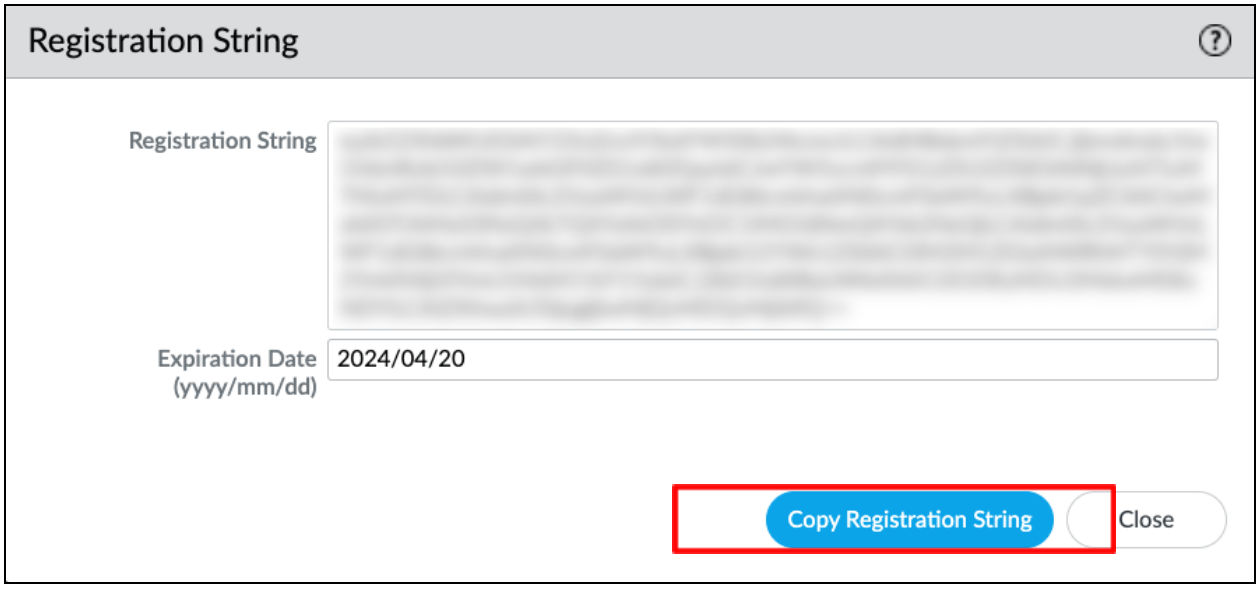




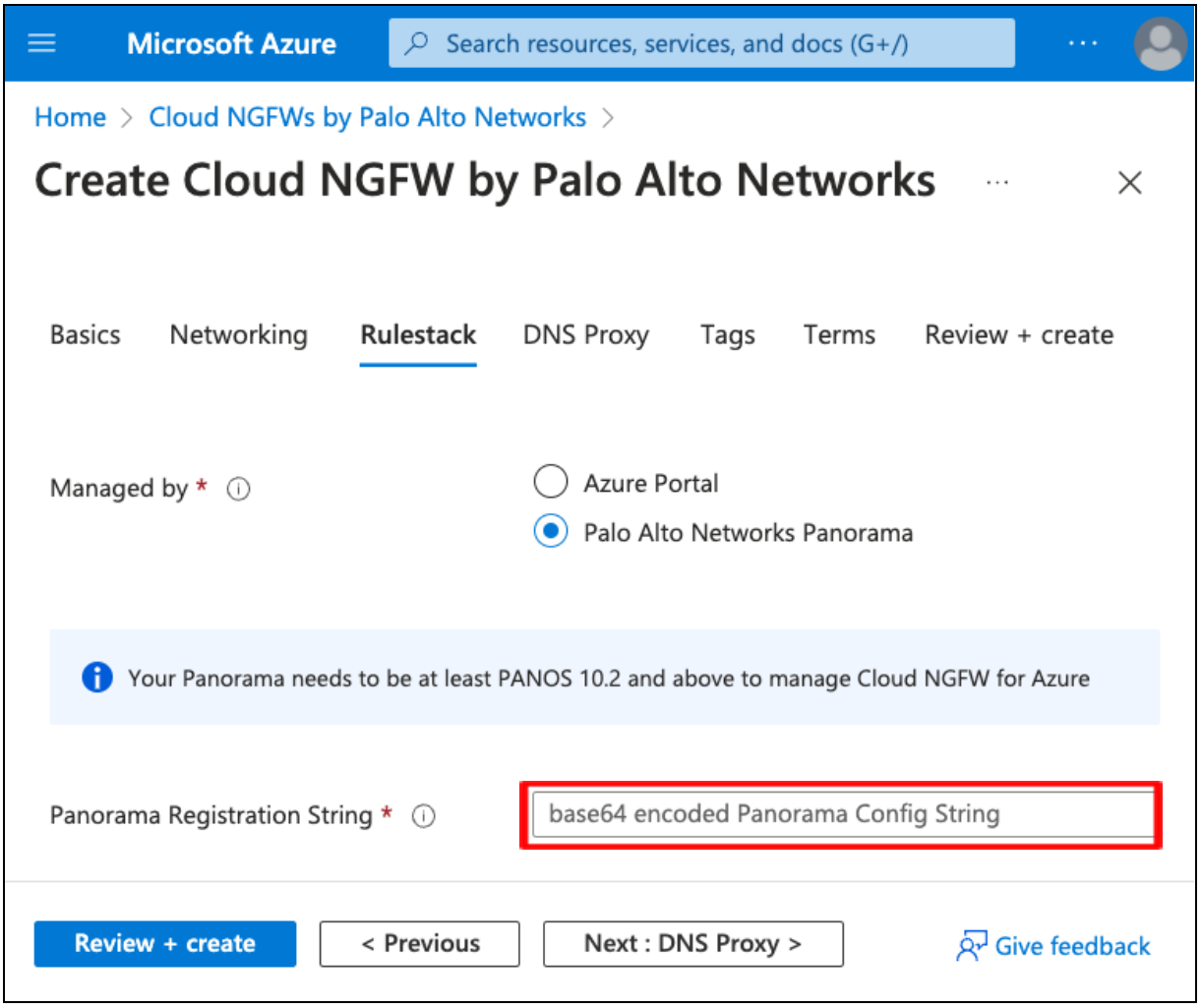


Generate the Registration string and copy it to the clipboard.





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

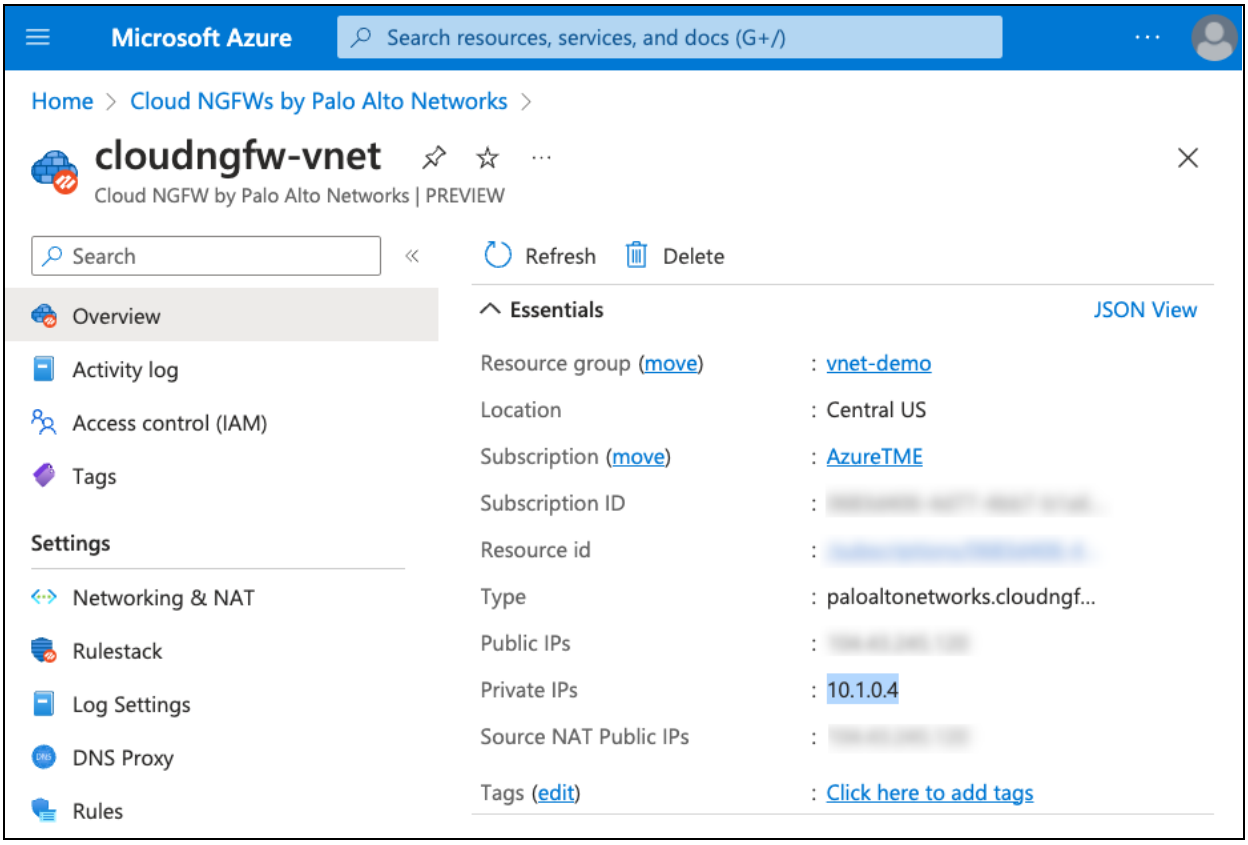


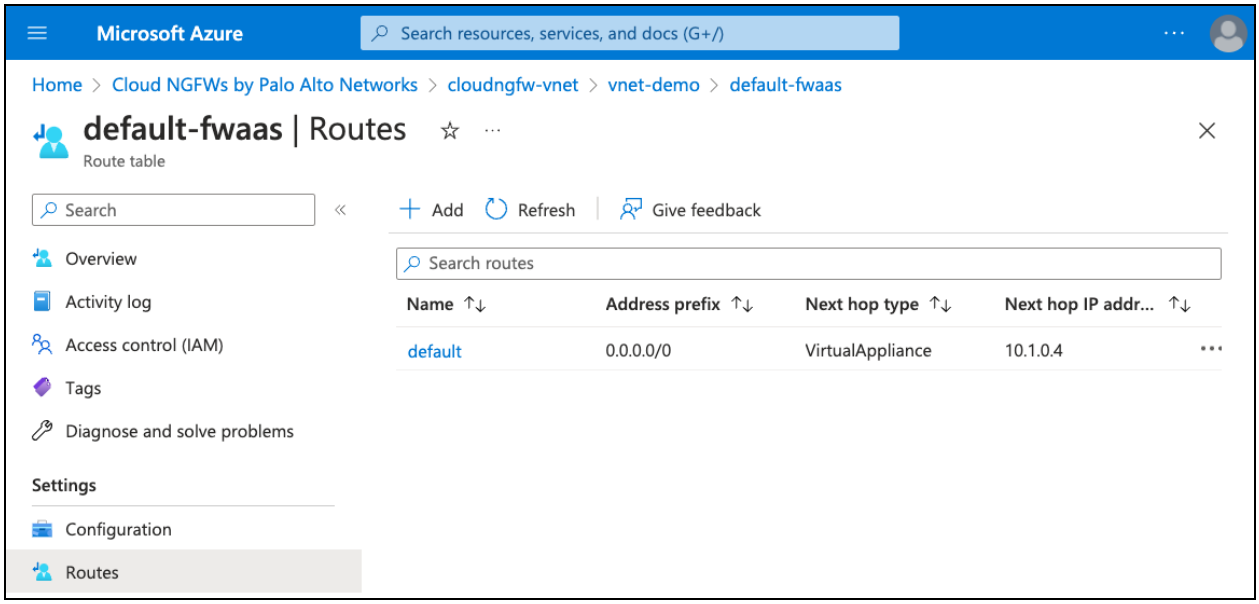
The Cloud NGFW creation process takes approximately 20 minutes.

2. Connect to Cloud NGFW

VNet Deployment:

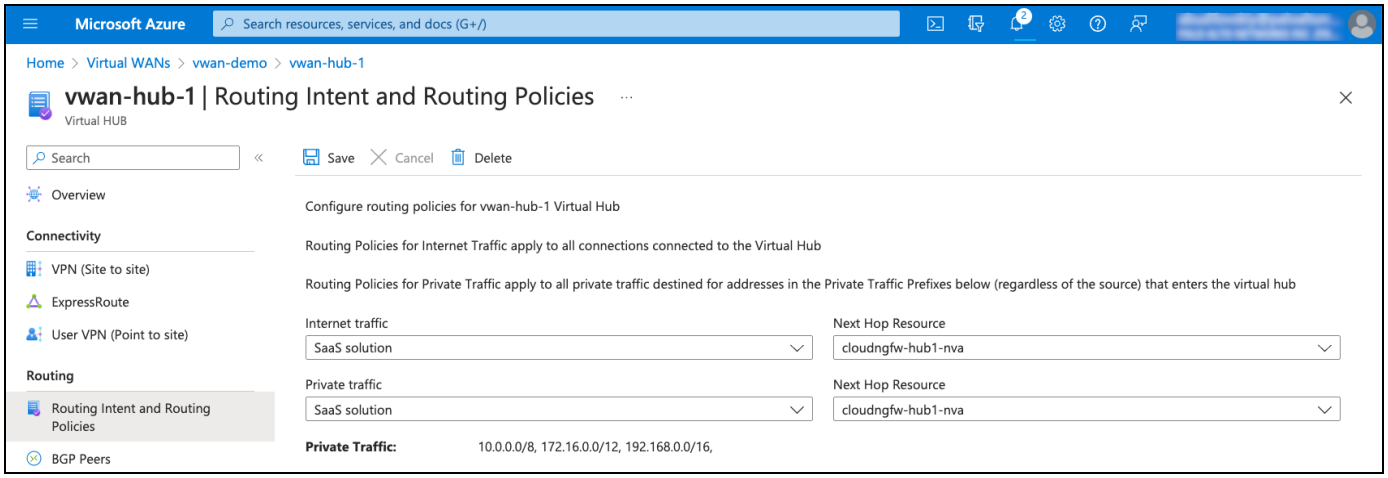
- Peer the spoke VNets with the Hub VNet where the Cloud NGFW was deployed to
- Create a Route Table with a default 0.0.0.0/0 route pointing to the Cloud NGFW Private IP address
- Associate the Route table to the spoke subnets


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 :
Resource id :
Type : paloaltonetworks.cloudngf...
Public IPs :
Private IPs : 10.1.0.4
Source NAT Public IPs :
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
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Routes
Search routes
Name
Address prefix
Next hop type
Next hop IP addr...
default
0.0.0.0/0
VirtualAppliance
10.1.0.4

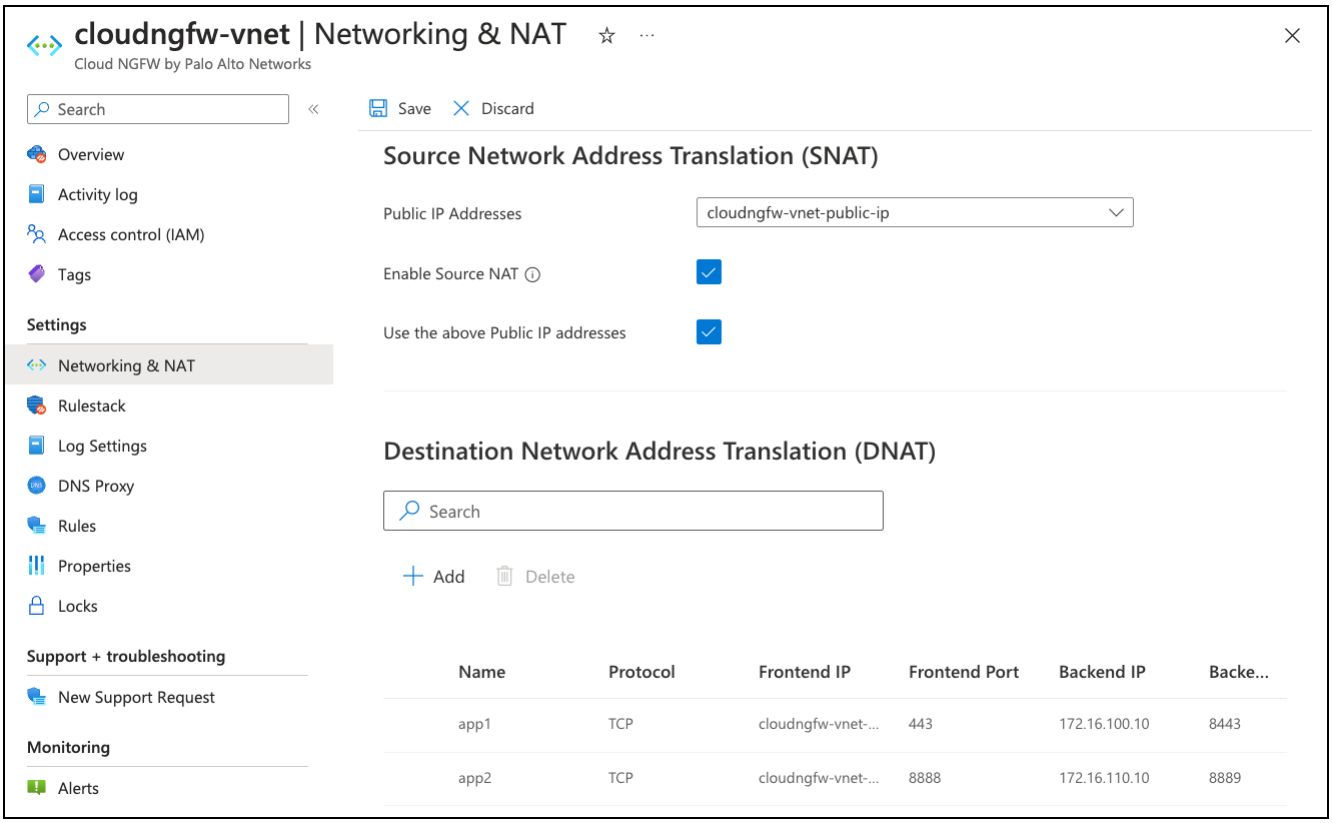
VWAN Deployment:

- 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



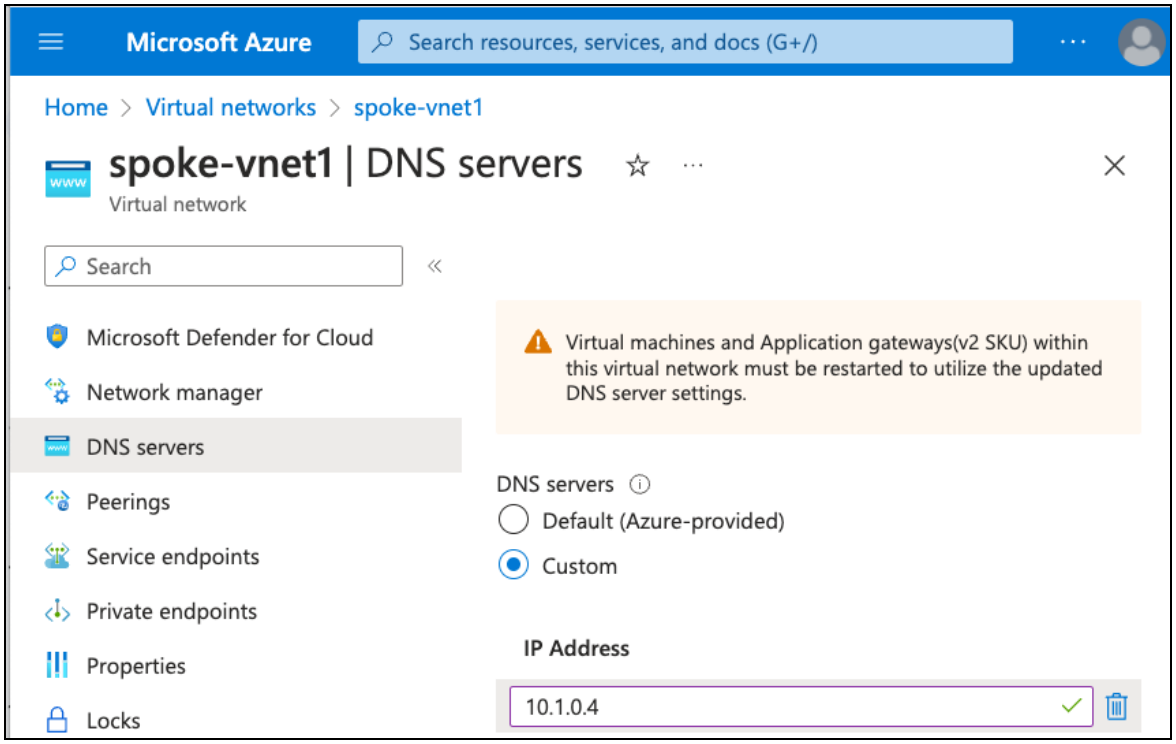
3. Configure Networking

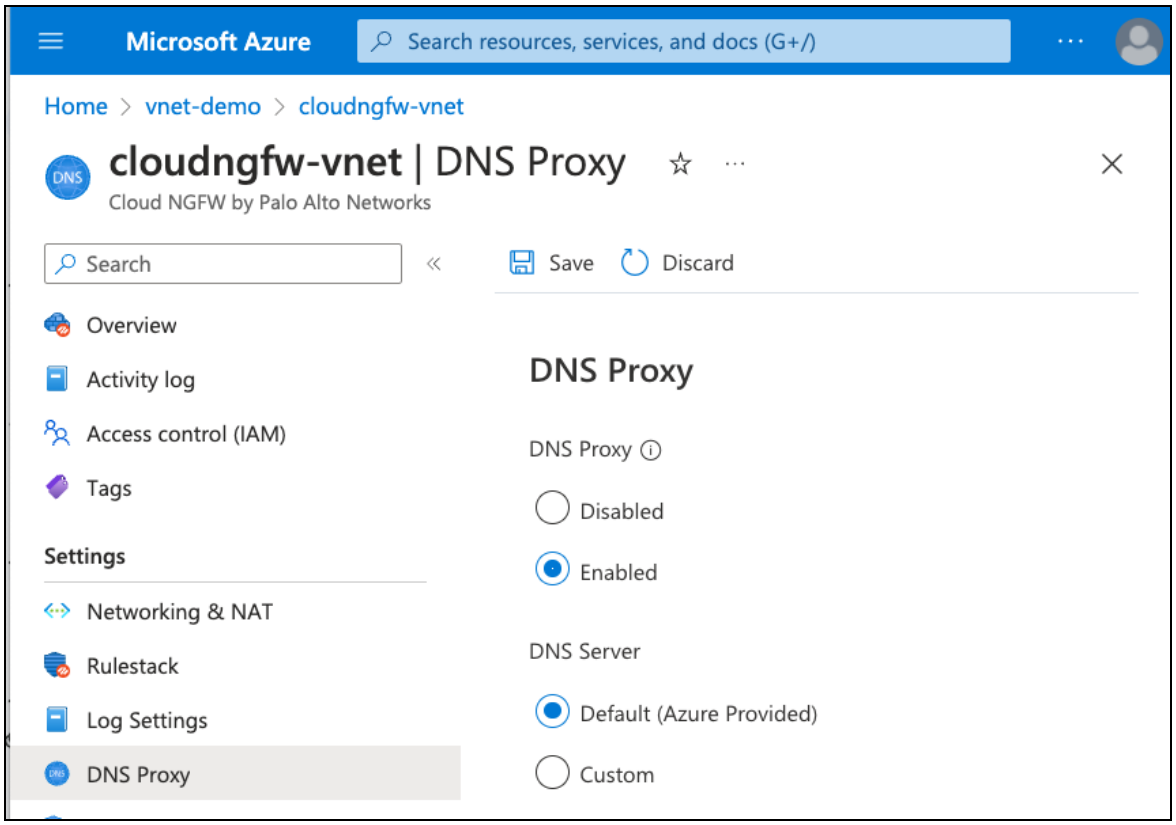
- Within the Cloud NGFW resource, configure DNAT rules to expose the workload for inbound flows
- Ensure SNAT is enabled for outbound flows



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

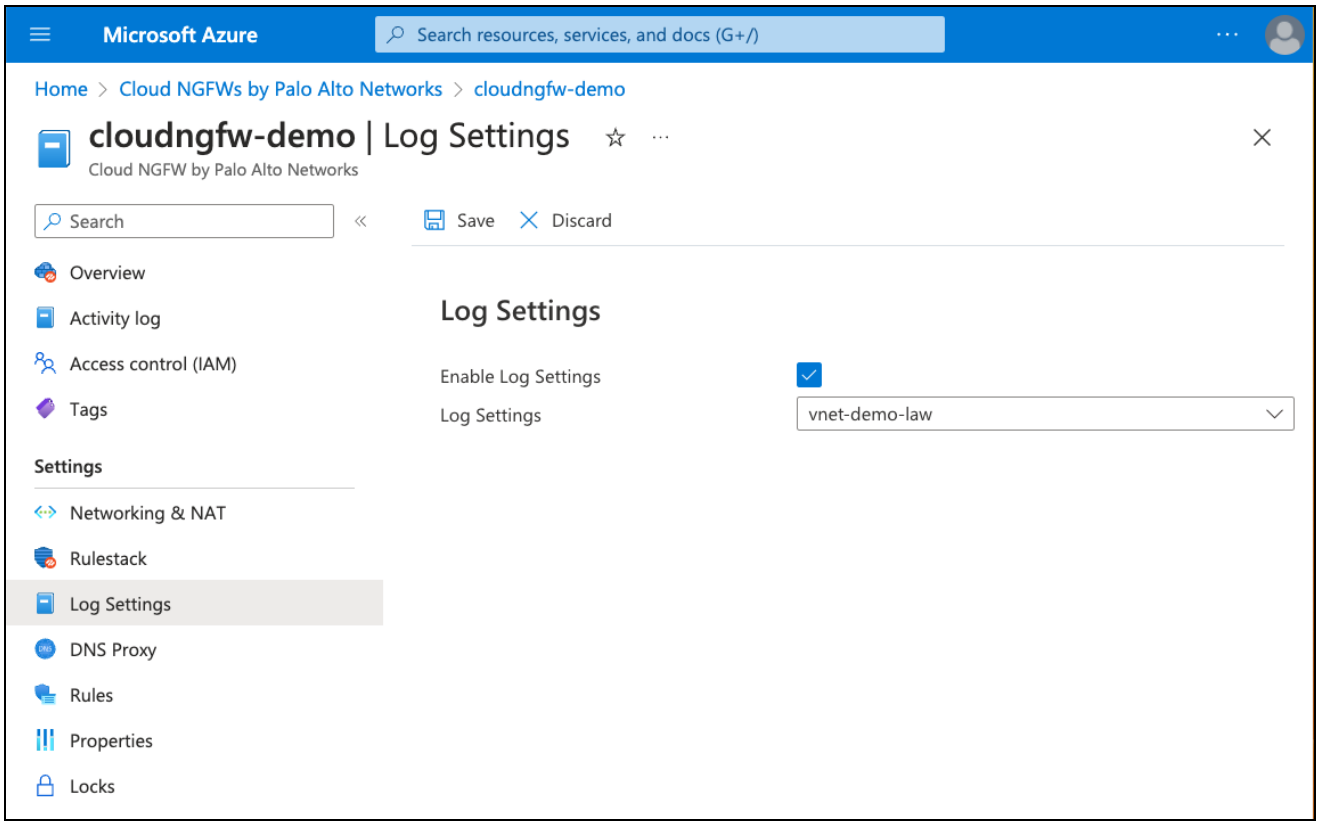
- Enable DNS Proxy for inspecting DNS traffic. This requires the spoke subnet to be configured with the DNS Server IP being the Cloud NGFW's Private IP address


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
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

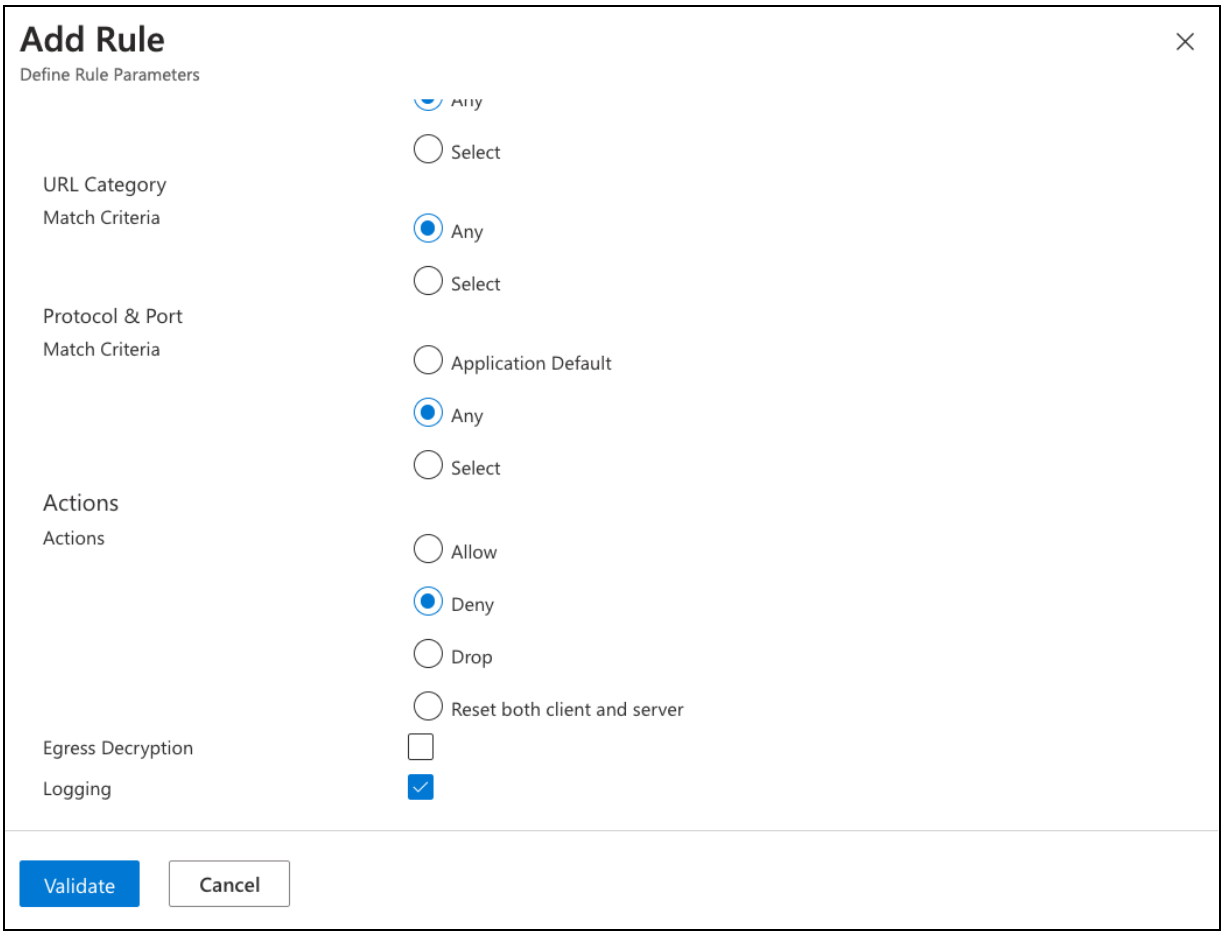

Microsoft Azure
Search resources, services, and docs (G+/)
Home > vnet-demo > cloudngfw-vnet
cloudngfw-vnet | DNS Proxy
Cloud NGFW by Palo Alto Networks
Search
Save
Discard
Overview
Activity log
Access control (IAM)
Tags
Settings
Networking & NAT
Rulestack
Log Settings
DNS Proxy
DNS Proxy
DNS Proxy
Disabled
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.

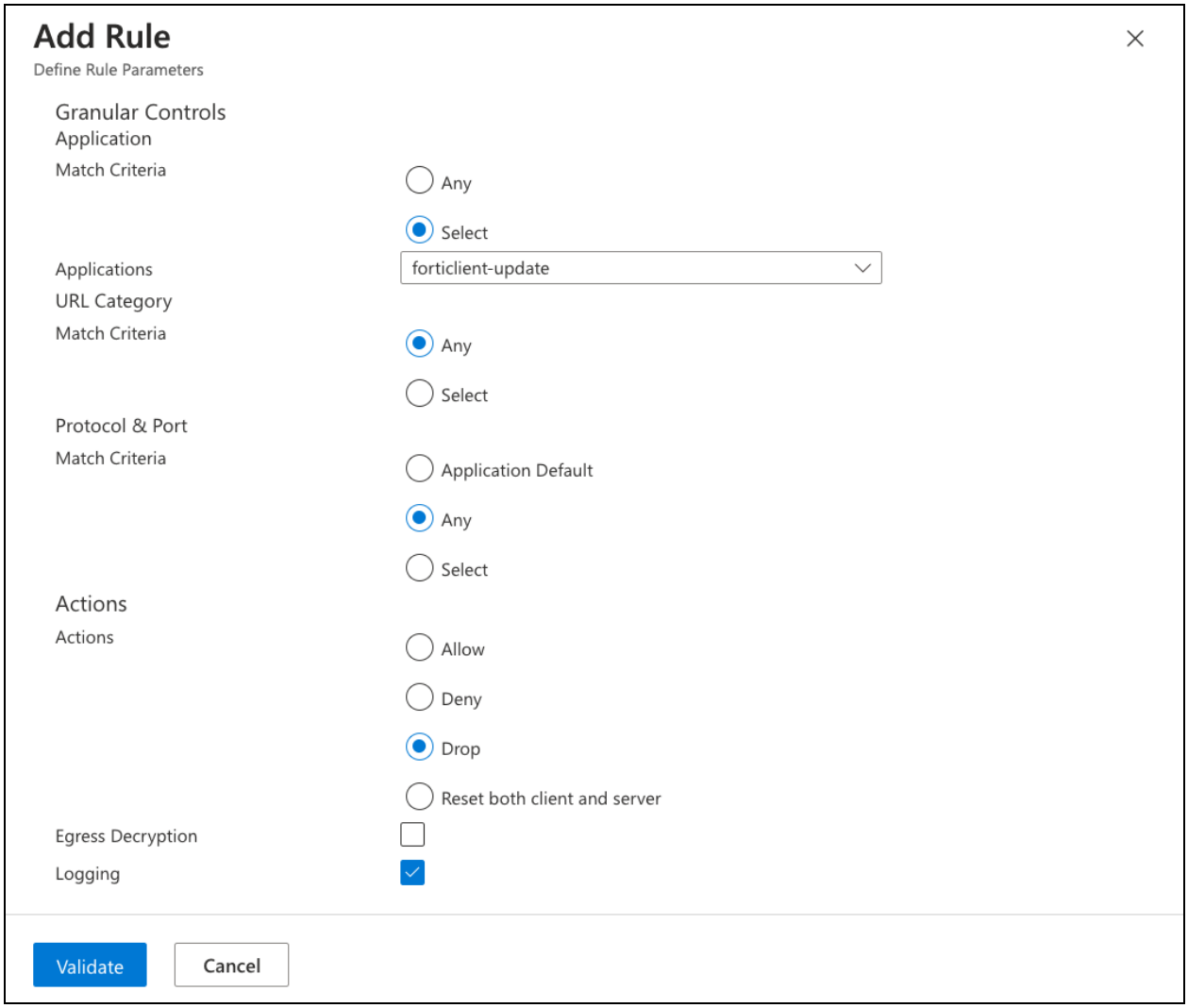


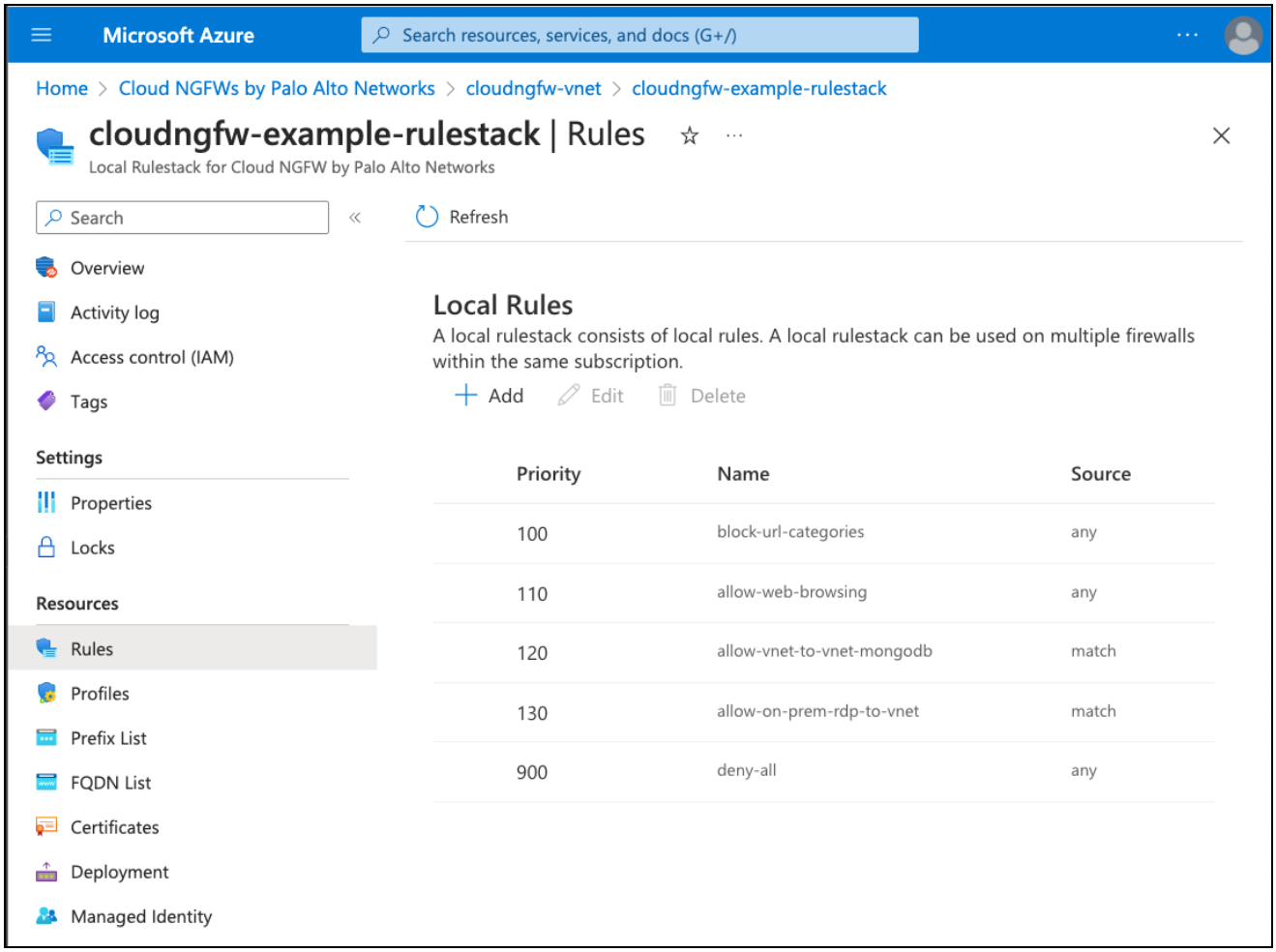
When configuring the rules in the next step, make sure Logging is enabled on a per-rule basis.



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.

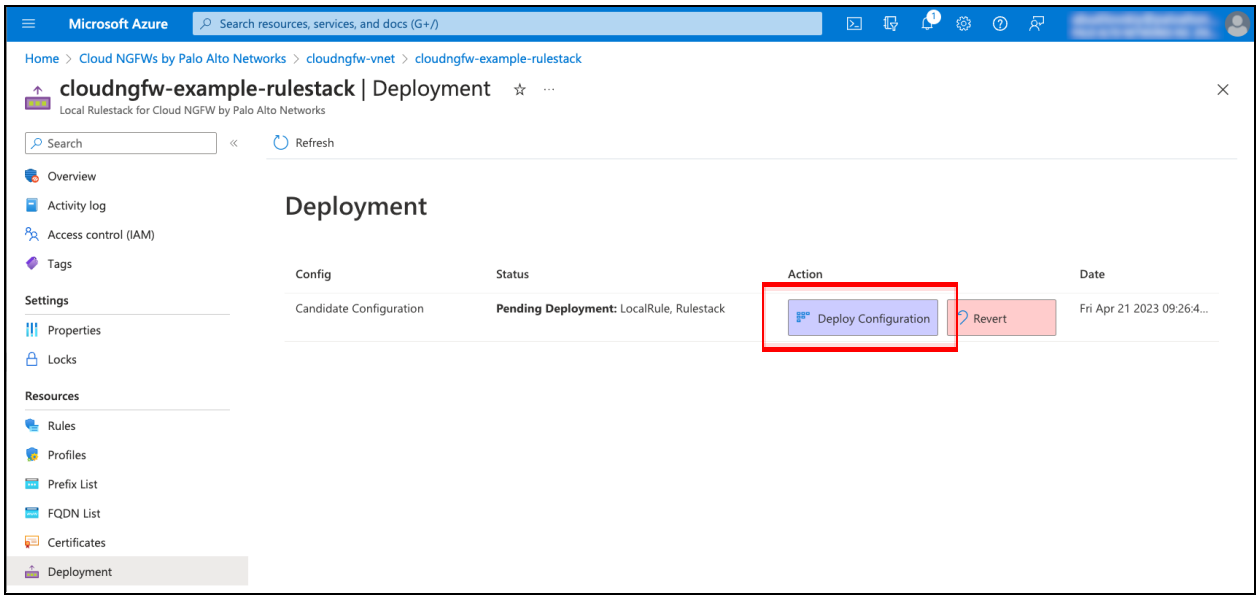

Add Rule
Define Rule Parameters
Granular Controls
Application
Match Criteria
Any
Select
Applications
forticlient-update
URL Category
Match Criteria
Any
Select
Protocol & Port
Match Criteria
Application Default
Any
Select
Actions
Actions
Allow
Deny
Drop
Reset both client and server
Egress Decryption
Logging
Validate
Cancel



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.