Cloud NGFW for Azure Customer FAQ

TABLE OF CONTENTS

Product

Q: What is Cloud NGFW for Azure?
A: Cloud NGFW for Azure is a managed cloud-native next-generation firewall service delivered by Palo Alto Networks on the Azure platform. Cloud NGFW for Azure protects your Azure workloads by offering best-in-class security with the ease of use of a cloud native service.

Q: What are the key benefits of Cloud NGFW for Azure?
A: With Cloud NGFW for Azure, customers get both best-in-class security and an easy, managed cloud-native experience.

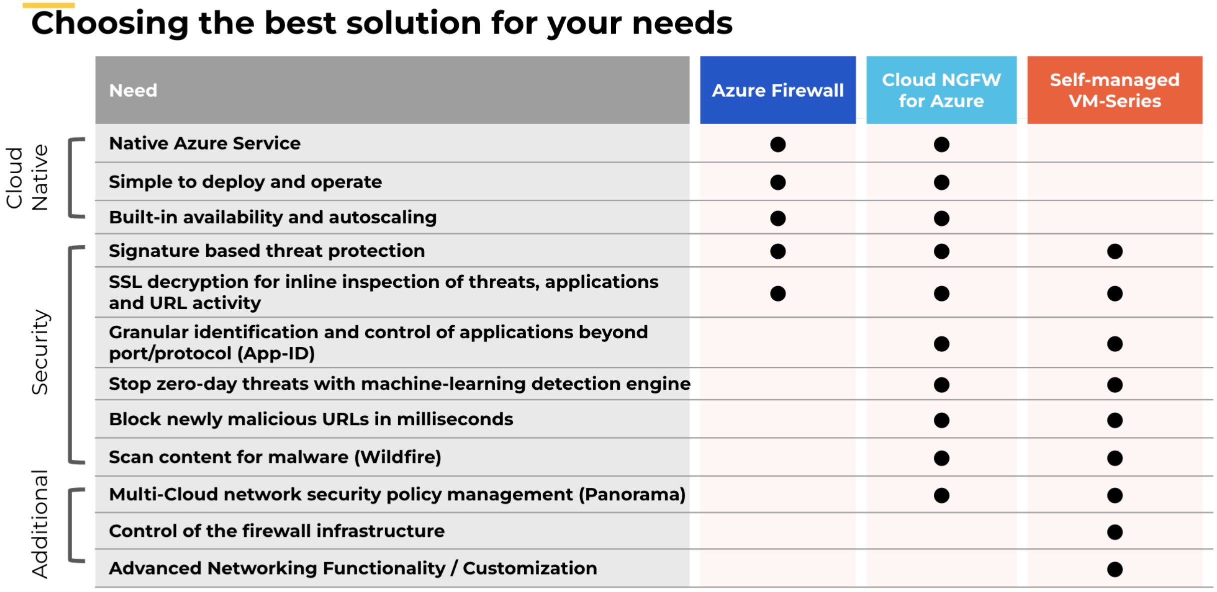
- Customers no longer have the operational overhead of managing the infrastructure, scaling, availability, resiliency, and software/content updates associated with a network virtual appliance solution.
- Cloud Security teams can now deploy this service with ease and speed at scale in their Azure environment by using the Azure Portal and Azure automation tools.
- Network Security teams have the flexibility to use Panorama for centralized security policy management and logging..
- Cloud NGFW seamlessly integrates with Azure services (e.g., Azure Portal, Azure Key Vault, Azure Log Analytics). These out-of-the-box integrations reduce the operational burden for security teams. They no longer need to maintain custom solutions or specialized expertise to provision and operationalize NGFWs.

Q: What is the difference between Cloud NGFW for Azure and VM-series on Azure?

A: Cloud NGFW for Azure is a fully managed service while the VM-series is managed by the customers. With Cloud NGFW for Azure customers do not need to worry about the design and management of the underlying infrastructure (i.e Virtual Machines, Load Balancers), PAN-OS software and content updates, scaling, and high availability deployments. The VM-series is a Network Virtual Appliance (NVA) that a customer uses to build a self-managed NGFW using Azure infrastructure components. The customer is responsible for managing the infrastructure, software, high availability, and scaling.

Q: What is the difference between Cloud NGFW for Azure and Azure Firewall?

A: Cloud NGFW for Azure is built using the well-renowned Palo Alto Networks' NGFW technology and provides advanced security functionality, including App-ID, Advanced Threat Prevention, Advanced URL Filtering, file sandboxing (WildFire), and DNS Security. On the other hand, Azure Firewall provides basic network traffic controls (port/protocol), signature-based IPS, and basic URL filtering. For more details see the table below.



Choosing the best solution for your needs

	Need	Azure Firewall	Cloud NGFW for Azure	Self-managed VM-Series
Cloud Native	Native Azure Service	●	●	
	Simple to deploy and operate	●	●	
	Built-in availability and autoscaling	●	●	
Security	Signature based threat protection	●	●	●
	SSL decryption for inline inspection of threats, applications and URL activity	●	●	●
	Granular identification and control of applications beyond port/protocol (App-ID)		●	●
	Stop zero-day threats with machine-learning detection engine		●	●
	Block newly malicious URLs in milliseconds		●	●
	Scan content for malware (Wildfire)		●	●
Additional	Multi-Cloud network security policy management (Panorama)		●	●
	Control of the firewall infrastructure			●
	Advanced Networking Functionality / Customization			●

Q: Who manages the Cloud NGFW for Azure firewall service?

A: Palo Alto Networks owns and manages the service. You can find the service listed on the Azure Marketplace. You can also find Cloud NGFW directly in the Azure portal (search for "Cloud NGW"), and when creating an Azure Virtual WAN Hub.

Q: Does Cloud NGFW for Azure offer a Service Level Agreement?
A: Cloud NGFW for Azure offers an uptime Service Level Agreement (SLA) of 99.99%. During the Public Preview period, this SLA is not guaranteed and customers will not be eligible to claim compensation if there is an outage.

Q: What is the difference between "Public Preview" and "General Availability"?
A: Cloud NGFW for Azure launched in Public Preview on May 2, 2023. During Public Preview, the service is fully supported by Palo Alto Networks and Microsoft Azure. We will strive to meet our SLA commitment of 99.99%, but it is not guaranteed and no refunds will be provided in the event of an outage. During the Public Preview period, Cloud NGFW is available at a 50% discount to the list price. When Cloud NGFW moves to General Availability (GA) (planned for Aug 2023), the SLA commitment will be in place and the price will change to the regular price.

Q: In what Azure regions is Cloud NGFW for Azure available?
A: You can find the latest information on Azure region availability in the Cloud NGFW for Azure documentation. Rapid expansion to additional regions is planned.

Q: Is Cloud NGFW for Azure available in Azure Government?
A: Not at this time. Expansion to Azure Government is under consideration.

Q: What is expected from customers to maintain software updates and dynamic content updates from Palo Alto Networks cloud-delivered services, such as threat signatures and URL categories?
A: Customers do not need to do anything to use the latest threat content from Palo Alto Networks. Cloud NGFW will automatically download the latest content from the Palo Alto Networks cloud to deliver the most up-to-date threat protection. Customers will not be responsible for managing the software updates for the NGFWs either. Cloud NGFW will roll out the software updates for the NGFWs using Azure's rolling upgrade infrastructure.

Q: Can Panorama be used to manage Cloud NGFW for Azure service?
A: Yes. With Cloud NGFW for Azure, the VM-Series instances that make up the Cloud NGFW resources connect directly to Panorama. This allows Panorama to send security policies directly to the VM-Series, unlocking the majority of the security policy functionality available in Panorama, including Dynamic Address Groups (DAGs). It also means that the VM-Series can send logs directly to Panorama. Note that Cortex Data Lake is NOT supported today.

Q: What Cloud Delivered Security Services (CDSS) are available for Cloud NGFW for Azure?
A: CDSS availability depends on how the security policy is being managed:

- Azure portal: If Cloud NGFW is managed through the Azure portal, Advanced Threat Prevention (ATP) and Advanced URL Filtering (AURL) are available.
- Panorama: If Cloud NGFW is managed through Panorama, Advanced Threat Prevention (ATP), Advanced URL Filtering (AURL), WildFire (WF), and DNS security are available.

Q: When will there be full feature parity between Cloud NGFW and VM-Series?
A: At launch on May 2, 2023, Cloud NGFW for Azure will be integrated with Panorama, with majority of the VM-Series security functionalities included. There are some routing and advanced VM-Series features that are not supported today, such as BGP routing, VPN termination, and Global Protect.

Q: Will my network traffic be isolated from the network traffic of other customers?
A: Yes. The data plane is dedicated per tenant, so network traffic processing is kept separate from other customers.

Q: What compliance certifications does Cloud NGFW have?
A: Cloud NGFW for Azure is SOC 2 Type 2 compliant. SOC 2 compliance provides assurance that Palo Alto Networks is securing data and ensuring privacy according to industry best practices. The standard is based on the following Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy. Customers can request the report here.

Getting Started - Deployment

Q: How do I get started using Cloud NGFW for Azure?
A: You can start using Cloud NGFW from the Azure Marketplace. You can also find Cloud NGFW directly in the Azure portal, and when creating an Azure Virtual WAN Hub.

Q: How do I protect my VNET deployments?
A: Cloud NGFW for Azure can protect your VNET deployments. Please see the VNet documentation for additional details.

Q: How do I protect my VWAN deployments?
A: Cloud NGFW for Azure can protect your VWAN deployments. Please see the VWAN documentation for additional details.

Q: What is a Cloud NGFW tenant?
A: A tenant is an instantiation of the Cloud NGFW service associated with a customer. The tenant is created when the first Cloud NGFW resource is created, and is associated with the Azure customers' account that created the resource.

Q: What is a Cloud NGFW rulestack?
A: A rulestack defines Cloud NGFW resource's advanced access control (App-ID, Advanced URL Filtering) and threat prevention behavior. A rulestack includes a set of security rules and the associated objects and security profiles. To use a rulestack, associate the rulestack with one or more NGFW resources.

Working with Cloud NGFW for Azure

Q: Where can I send logs generated by Cloud NGFW for Azure?
A: The logging destination depends on how the security policy is being managed:

- For Azure Portal, logs can be sent to an Azure Log Analytics Workspace
- For Panorama, logs can be sent to Panorama or a Panorama log collector.

Q: What is the maximum throughput of a Cloud NGFW resource?
A: A Cloud NGFW resource can scale up to 50 Gbps.

Q: What is the cold-start capacity of a Cloud NGFW resource?
A: Each Cloud NGFW resource starts with a cold-start capacity of 9 Gbps, and provides redundancy across three Availability Zones (where available).

Q: Does Cloud NGFW for Azure support automation?
A: Support for the Azure Infrastructure as Code (IaC) tools is planned for GA. These include the Azure API/CLI/SDK, ARM Templates, and Terraform provider.

Pricing and Licensing

Q: Can customers purchase Cloud NGFW for Azure through the Azure Marketplace?
A: Yes. Cloud NGFW for Azure is available on Azure Marketplace on a Pay-As-You-Go basis. During the Public Preview period, the price is 50% of the regular price. At GA, it will be the regular price.

Q: How is Cloud NGFW for Azure priced?
A: Cloud NGFW for Azure is priced the same way as other Azure virtual networking resources - Per Hour plus Per GB of traffic. With Cloud NGFW for Azure, customers pay an hourly rate for each Cloud NGFW resource. Data processing charges apply for

each GB processed by the Cloud NGFW resource. Customers can use additional security capabilities such as Advanced Threat Prevention and Advanced URL Filtering as an add-on to the Per Hour and Per GB prices. Additional information on pricing can be found in the Cloud NGFW for Azure documentation.

Q: Does Cloud NGFW for Azure have a Free Trial option?
A: Yes. Cloud NGFW is available with a Free Trial via the Pay-as-you-go listing in Azure Marketplace. Customers are automatically enrolled in the 30-day free trial period upon subscription. The free trial allows customers to use two NGFW resources with full features to secure 1 TB of traffic at no cost to the customer. After 30 days, the free trial converts to pay-as-you-go billing, consistent with the terms of the listing.

Q: Can customers deploy Cloud NGFW for Azure using Software NGFW credits?
A: We recognize the value of enabling customers to use Software NGFW credits to consume this service and are looking into adding Cloud NGFW to the FW-Flex program. Look for an update close to Aug 2023.

Q: Can customers deploy Cloud NGFW for Azure using their VM-Serles ELA?
A: No. Cloud NGFW for Azure cannot be deployed using the VM-Series ELA.

Support

Q: How can customers get customer support for Cloud NGFW?
A: Premium support is included with Cloud NGFW. Customers must register their Cloud NGFW for Azure tenant to their CSP account. They can do this in the Azure portal on the page where they create and manage Cloud NGFWs.

Q: Who provides support for Cloud NGFW for Azure?
A: Palo Alto Networks is responsible for providing support for Cloud NGFW for Azure. If needed, Palo Alto Networks will work with Microsoft Azure to resolve any customer support issues.