Cloud NGFW on Azure

Organizations need a straightforward solution to implement cutting-edge network security for their expanding public cloud workloads. This includes robust Layer 7 identification and control to analyze application behavior and advanced security to mitigate modern cyberattacks, all while minimizing operational complexity for network security, cloud security, and DevOps teams.

Key Benefits of Cloud NGFW on Azure

Cloud NGFW on Azure combines industry-leading network security with the simplicity and scalability of a fully cloud-native service on Microsoft Azure. Built by Palo Alto Networks, this AI-powered solution defends against sophisticated cyberthreats while delivering unparalleled reliability and flexibility. With Cloud NGFW on Azure, organizations can:

- **Streamline operations with zero maintenance:** Experience the benefits of a fully managed Next-Generation Firewall (NGFW) service with automated elastic scaling and simplified deployment, eliminating the need for manual updates or infrastructure management.
- **Extend best-in-class security from on-premises to Azure:** Seamlessly integrate their cloud environment with Panorama® and Strata™ Cloud Manager to unify policy management and gain centralized visibility across all environments.
- **Secure Azure Virtual Networks (VNets):** Protect workloads with patented App-ID™ technology for precise Layer 7 identification and control of applications, Advanced Threat Prevention for real-time security, and ML-powered Advanced URL Filtering to block unknown threats instantly.
- **Enhance the Azure experience:** Access Cloud NGFW on Azure through Azure Marketplace, with deep integration into Azure Application Insights, Azure Virtual WAN, Azure Key Vault, and other native Azure services.
- **Flexible credit management:** Ensure dynamic resource allocation and efficient scaling across regions.

Why Cloud NGFW on Azure

As cloud adoption accelerates, organizations face increasing challenges in securing workloads at scale. Traditional security solutions often lack the agility, visibility, and advanced protections needed for dynamic Azure environments. Built for cloud-native workflows, Cloud NGFW on Azure directly addresses these challenges by offering:

- **Proactive threat prevention:** Stops evolving threats in real time with AI-powered protections against zero-day exploits, malware, and command-and-control (C2) attacks.
- **Comprehensive cloud security:** Delivers Layer 7 application identification and control to ensure granular awareness of application, user, and workload traffic across outbound, inbound, and VNet-to-VNet flows.
- **Seamless Azure Native Integration:** View Cloud NGFW performance and health information directly in the Azure Application Insights console. It integrates effortlessly into Azure services like Azure Virtual WAN, Azure Key Vault, and Azure Marketplace. Plus, it ensures operational consistency and simplicity for network security, cloud security, and DevOps teams.
- **Zero maintenance, full scalability:** Eliminates operational overhead with a fully managed service that offers automated scaling, high availability, and centralized management.
- **Flexible credit management:** Adapts quickly to changing needs with a dynamic credit allocation system, ensuring cost efficiency and scalability across regions.

Real-Time, Zero-Day Protection for Azure Virtual Networks

Cloud NGFW on Azure redefines cloud network security by using advanced, AI-powered services to protect applications from rapidly evolving cloud-based and network-based threats. It automatically detects and blocks malware, C2 traffic, and vulnerability exploits while managing traffic within and across VNets.

Internet Outbound Traffic

Cloud workloads often require access to external resources or the internet:

- **Challenges:** Outbound traffic exposes workloads to data exfiltration, malicious websites, phishing attempts, and nonweb-based attacks such as file transfers or encrypted traffic.
- **Solution:** Cloud NGFW on Azure integrates patented App-ID and Threat Prevention technologies to block both web and nonweb attacks with Layer 7 application controls for precise traffic enforcement.

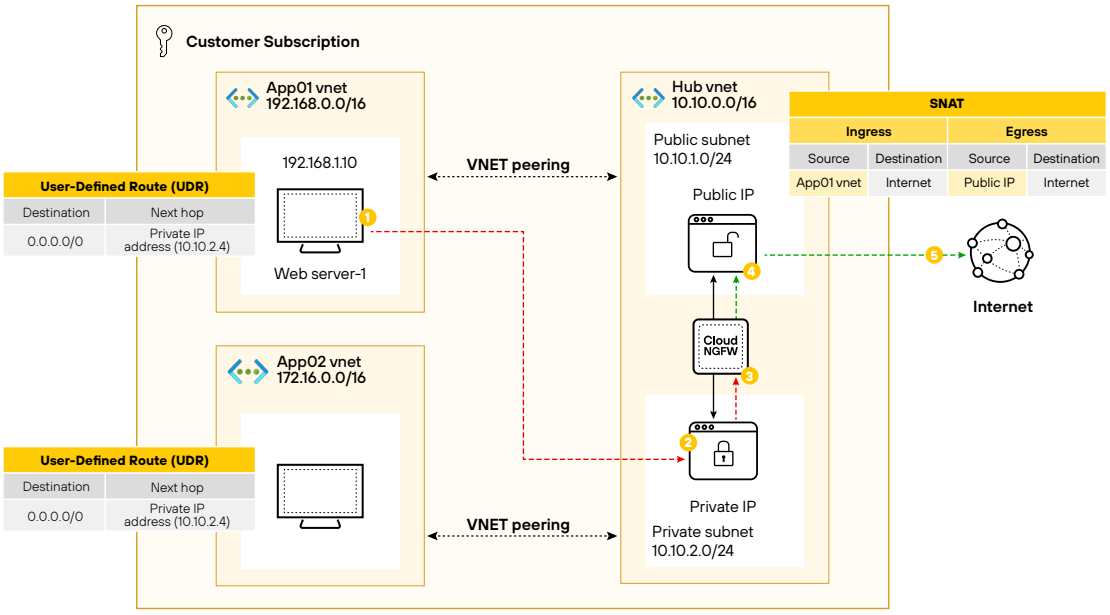

Figure 1. Application outbound traffic inspection

Internet Inbound Traffic

Applications exposed to the internet face constant threats, especially from unpatched vulnerabilities and sophisticated attack vectors:

- **Challenges:** Attackers exploit web-facing apps using remote code execution, SQL injection, and bypassing traditional web application firewalls (WAFs).
- **Solution:** Cloud NGFW on Azure integrates patented App-ID and Threat Prevention technologies to block both web and nonweb attacks with granular, application-layer controls.

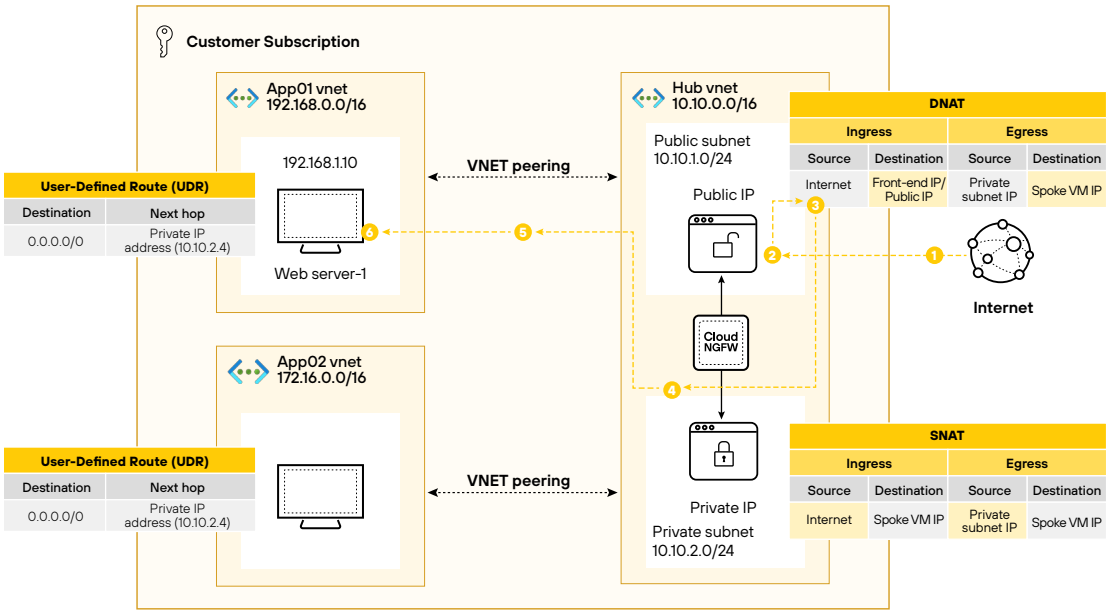

Figure 2. Internet ingress traffic inspection

VNet-to-VNet or Between Azure Subnets

Intracloud traffic between VNets or subnets presents a significant attack surface, especially if malware propagates laterally in a breach scenario:

- **Challenges:** Without proper segmentation, malicious actors can move laterally across workloads, exploiting trust relationships between applications.
- **Solution:** To prevent lateral movement, Cloud NGFW on Azure applies advanced segmentation, Threat Prevention, and App-ID for Layer 7-based segmentation and traffic control between VNet subnets.

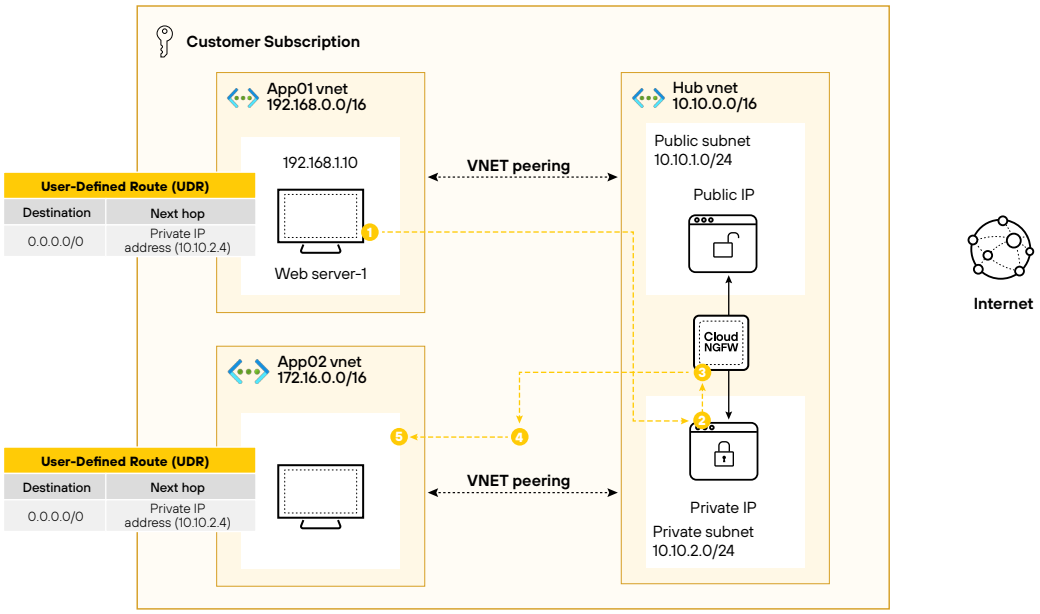

Figure 3. East-west traffic inspection

Internet Ingress via Azure Application Gateway

Some organizations deploy Azure Application Gateway for TLS termination, web application routing, or load balancing. While effective at Layer 7 routing, Application Gateway isn't designed to provide full NGFW capabilities such as deep packet inspection, advanced threat prevention, or protection for nonweb traffic.

- **Challenges:** Azure Application Gateway provides basic WAF functionality but lacks the deep security visibility and enforcement needed to prevent sophisticated attacks such as malware, C2 traffic, or protocol tunneling. It also doesn't protect nonweb traffic such as SSH, RDP, or FTPs.
- **Solution:** Cloud NGFW on Azure complements Application Gateway by delivering inline threat prevention and Layer 7 application identification and control after routing decisions are made. This deployment model enables organizations to retain Application Gateway's native routing benefits while enforcing granular traffic inspection and advanced security controls through a centralized NGFW.

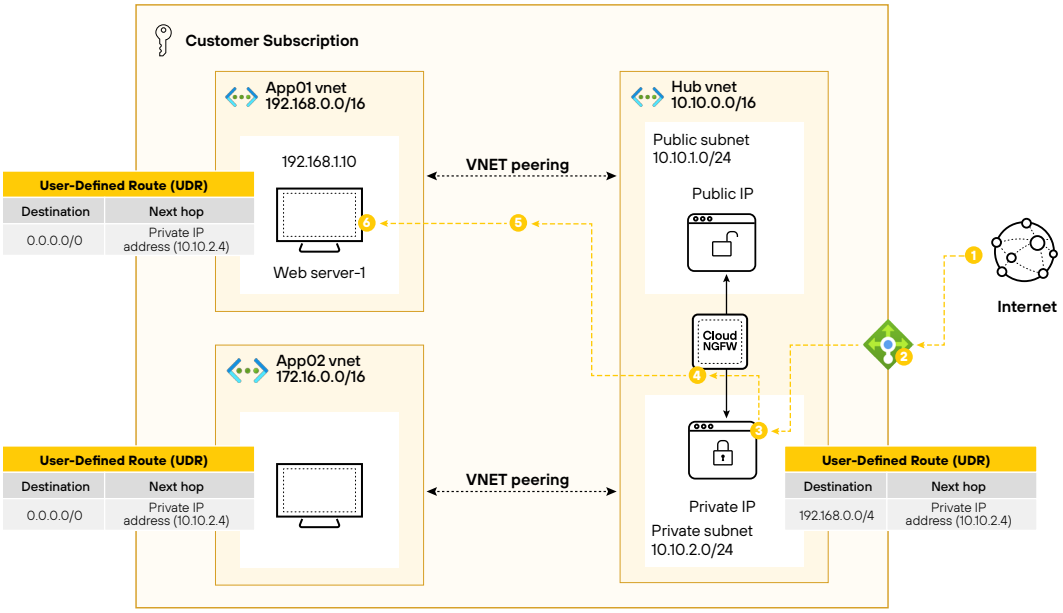

Figure 4. Internet ingress via Application Gateway

Azure Native Services and Management

Cloud NGFW on Azure integrates seamlessly with the Microsoft Azure Native ecosystem. It supports:

- **Application performance:** Azure Application Insights
- **Identity and security:** Microsoft Entra ID (Azure Active Directory) and role-based access control (RBAC), as well as Azure Key Vault
- **Networking and traffic management:** Azure Virtual Networks and Virtual WANs
- **Logging and threat visibility:** Azure Log Analytics workspace and Microsoft Sentinel
- **Infrastructure and automation:** Azure Portal, Azure Resource Manager (ARM), Azure CLI, PowerShell, SDK, Terraform, and REST APIs

This integration ensures seamless security enforcement, centralized management, and scalable cloud operations for Azure workloads.

Zero Infrastructure Overhead

Cloud NGFW on Azure doesn't require any internal infrastructure to manage, allowing organizations to focus on securing applications without the burden of maintaining hardware or software:

- **Fully managed service:** Palo Alto Networks handles deployment, scaling, updates, and maintenance.
- **Elastic scaling:** Dynamically scales to meet changing workload demands.
- **High availability and autoscaling:** Cloud NGFW on Azure automatically scales up to 100 Gbps for both VNet and Virtual WAN deployments.

The service ensures failover, redundancy, and autoscaling based on traffic demands, while maintaining a 99.99% uptime SLA.[1]

Flexible Procurement Options

Cloud NGFW on Azure offers multiple procurement models, ensuring seamless deployment and cost-effective scalability:

- **Free trial:** Start with a free trial through Azure Marketplace.
- **PAYG pricing:** Pay-as-you-go (PAYG) model with hourly and per-GB pricing.
- **Private offers:** Tailored pricing and deployment options for enterprises.
- **Flexible credit management:** Use Palo Alto Networks credits across AWS and Azure, covering Cloud NGFW, Panorama, Strata Cloud Manager, and Strata Logging Service.

Regional Availability

Cloud NGFW on Azure is accessible in most Azure commercial regions globally, ensuring consistent security regardless of an organization's workload location:

- **Global coverage:** The service is available in a wide range of Azure regions, enabling organizations to protect their applications and data in compliance with local and international regulations.
- **Expanding footprint:** Palo Alto Networks continues to extend availability into new Azure regions to support growing customer needs. For the most up-to-date list of supported regions, see the Cloud NGFW Supported Regions and Zones page.

Regulatory Compliance and Certifications

Cloud NGFW on Azure meets industry-leading compliance standards, including:

- PCI DSS, SOC 2, HIPAA, ISO 27001, 27017, 27018, and 27701
- CSA STAR, IRAP (Australia), and Germany C5

These certifications ensure adherence to security, privacy, and regulatory mandates, making Cloud NGFW on Azure ideal for highly regulated industries.

Support and Education

Palo Alto Networks provides robust support and educational resources to ensure Cloud NGFW on Azure customers can maximize the value of their investment. From onboarding to troubleshooting, our services deliver a smooth, secure, and scalable experience.

1. "Support Policies and SLAs," Palo Alto Networks, April 2022.

Premium Support Services

Ensure seamless deployment and continuous protection with 24/7 expert support and proactive monitoring:

- **LIVEcommunity access:** Tap into a vibrant customer community and knowledge base for quick answers to common questions.
- **Customer Support Portal:** Access technical documentation, troubleshooting guides, and ticketing services for personalized assistance.
- **Proactive monitoring:** Get real-time monitoring of your organization's Cloud NGFW instance to ensure optimal performance and uptime.
- **Callback support:** Receive callback assistance from Palo Alto Networks technical experts anytime, day or night, to address critical issues.

In-Product Help

Simplify troubleshooting and operations with built-in help features:

- **Get help within the product:** Quickly find solutions to common issues directly within the Cloud NGFW interface, reducing downtime and the need for external searches.
- **Azure expertise:** Speak with support engineers who have a deep knowledge of the Azure platform and ensure fast, accurate solutions tailored to cloud-native environments.

Education and Training

Empower teams with the knowledge and skills needed to secure Azure environments effectively:

- **Build expertise with on-demand training:** Access digital learning modules to gain proficiency in using Cloud NGFW on Azure, including configuration, management, and threat analysis.
- **Validate skills with industry-recognized certifications:** Achieve microcredentials that demonstrate expertise in securing Azure environments using Palo Alto Networks technologies.
- **Enhance operational efficiency with proactive insights:** Leverage operational metrics and notifications to monitor firewall performance and security trends, optimizing team workflows.

Start with a No-Obligation Free Trial

Experience Cloud NGFW on Azure today with zero commitment and discover how it can enhance your cloud network security. Get started with a free trial and explore how Cloud NGFW simplifies security for your Azure workloads.

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

strata_ds_cloud-ngfw-on-azure_092325