Palo Alto Networks
Cloud Next-Generation Firewall (NGFW)
Certified Secure Test Report

May 2025

DR250331C

Miercom
www.miercom.com

Table of Contents

1.0 Executive Summary 3

2.0 Test Summary 5

3.0 Introduction 6

4.0 How We Did It 7

5.0 Exploit Detection and Resistance 13

6.0 Malware Detection 14

7.0 Evasion 17

8.0 Administrator Experience (Admin UX) 19

9.0 About Miercom 23

10.0 Use of This Report 23

Copyright © Miercom 2025

1.0 Executive Summary

Cloud network firewalls are next-generation firewall (NGFW) solutions designed specifically for cloud environments. It combines traditional cloud network firewall protection with advanced security features. This integration allows the Cloud NGFW to offer enhanced visibility and control over cloud network traffic, ensuring secure access and protection against cyber threats. Optimized for cloud scalability and flexibility, the NGFW seamlessly integrates with cloud services, providing security without compromising network performance. This makes it an essential component for businesses aiming to secure their cloud infrastructure effectively.

Miercom performed an independent assessment of Palo Alto Networks Cloud NGFW solution alongside competitive offerings from Amazon Web Services (AWS) and Microsoft Azure. This report provides an analysis of the Palo Alto Networks Cloud NGFW, a managed FWaaS -Service solution, evaluating its effectiveness in providing security within cloud environments. This assessment focuses on the firewall's capabilities to detect and respond to critical, high and medium vulnerabilities (NIST CVSS).

Through rigorous testing, Miercom assessed each cloud NGFW's response to simulated attacks that mirror real-world threats. The firewall's performance was measured by its ability to detect, block and report incidents, providing a granular view of these defense mechanisms against each level of assessed threat.

Key Findings for Palo Alto Networks Cloud NGFW:

- 99% detection rate for critical vulnerabilities scoring of 9 to 10
- 99% detection rate for high vulnerabilities scoring of 7 to 8.9
- 87% detection rate for medium vulnerabilities scoring score of 4 to 6.9
- 95% overall detection rate against critical, high and medium CVSS vulnerabilities
- 100% detection rate against 15,134 malware samples
- Successfully detected and prevented sophisticated base evasion techniques
- Seamlessly integrates advanced threat protection features into cloud environments.
- Advanced Layer 7 security capabilities include IPS with TLS interception and decryption
- Powerful threat detection engines and threat intelligence provide Palo Alto Networks Cloud NGFW with a decisive competitive edge

Copyright © Miercom 2025

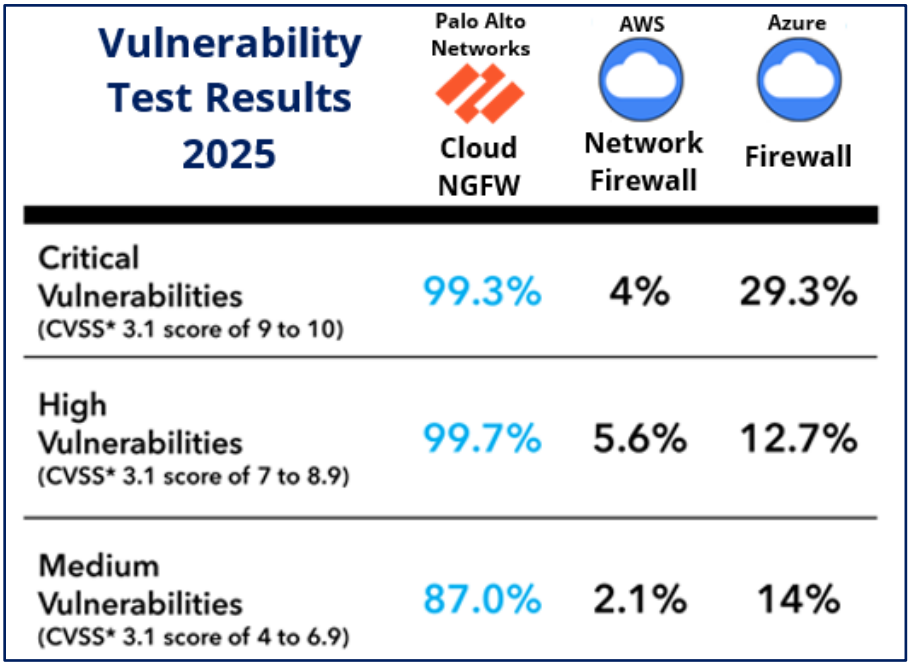
Based on our findings, Palo Alto Networks Cloud NGFW was validated for its protection against critical, high and medium exploits or strikes (NIST CVSS), ability to detect and block evasive malware, and its superior User Interface Experience earning the **Miercom Certified Secure** certification.

Robert Smithers

CEO, Miercom

Copyright © Miercom 2025

2.0 Test Summary



The Miercom 2025 vulnerability test results show Palo Alto Networks Cloud NGFW's superior effectiveness in blocking vulnerabilities compared to AWS Network Firewall and Azure Firewall. Palo Alto Networks significantly outperformed its competitors, blocking 99.3% of critical, 99.7% of high, and 87% of medium exploits as defined by the CVSS.

Cloud Next-Generation Firewall (NGFW) Competitive Assessment Test Summary				
Criteria	**Test Criteria**	**Palo Alto Networks Cloud NGFW**	**AWS Network Firewall**	**Azure Firewall**
1	5.0 Exploit Detection and Resistance	● Blocked 901 of 951 vulnerabilities	○ Blocked 36 of 951 vulnerabilities	○ Blocked 151 of 951 vulnerabilities
2	6.0 Malware Detection	● Prevented all 15,134 samples.	◔ Prevented 5750 of 15,134 samples.	○ Prevented 1665 of 15,134 samples.
3	7.0 Evasion	● Blocked all 150 samples	○ Allowed 142 of 150 samples	◔ Allowed 102 of 150 samples
4	8.0 Administrative Experience	●	◕	◔
	Result	●	◔	◔

Key				
●	◕	◑	◔	○
Fully Compliant	**Mostly Compliant**	**Marginally Compliant**	**Poorly Compliant**	**No Support**

Copyright © Miercom 2025

3.0 Introduction

Palo Alto Networks Cloud NGFW is a fully distributed, stateful, firewall service designed to deliver advanced protection capabilities, micro-segmentation, and comprehensive coverage to protect cloud workloads from internal and external threats. It supports a zero-trust security architecture by implementing stateful host-based enforcement on each workload. It simplifies the configuration and deployment process through network and hierarchical firewall policies, which can be attached to a resource hierarchy node, ensuring a consistent firewall experience across the cloud resource hierarchy. Palo Alto Networks Cloud NGFW provides granular control and micro-segmentation, using a combination of firewall policies and Identity and Access Management (IAM)-governed Tags to finely control traffic both north-south and east-west, down to the level of a single VM across Virtual Private Cloud (VPC) networks and organizations. It provides advanced layer 7 security capabilities, including intrusion prevention services (IPS) with transport layer security (TLS) interception and decryption, all while leveraging powerful engines from Palo Alto Networks.

This evaluation focuses on evaluating security efficacy, including the blocking of critical, high, and medium CVSS vulnerabilities exploits, evasion techniques, and malware, including zero-day threats. The user experience is also assessed, particularly the user interface experience (UIX), to ensure usability aligns with security functionality.

Products Tested

Vendor	Product
Palo Alto Networks	Cloud NGFW
Amazon Web Services	Amazon Network Firewall
Microsoft	Azure Firewall

Copyright © Miercom 2025

4.0 How We Did It

To evaluate the functionality of the System Under Test (SUT), a custom-built network was designed to simulate a real-world deployment environment. Malicious and benign traffic was generated and delivered through the network to assess the SUT's ability to detect, prevent, and respond to threats. All observations related to security efficacy and user experience (UX) were recorded.

The Miercom Cloud NGFW security efficacy strike test was conducted using the BreakingPoint Virtual Edition tool. Each testbed required a dedicated BreakingPoint installation to ensure platform-specific testing consistency.

All BreakingPoint instances were updated to the latest firmware, strike packs, and malware libraries prior to testing.

The following criteria were applied when selecting strikes from BreakingPoint Virtual Edition:

- Strikes dated from 2018 to 2024, reflecting current applications and vulnerabilities.
- Both client- and server-initiated attacks were included.
- CVSS 9.0–10.0 (CRITICAL): 150 unique strikes.
- CVSS 7.0–8.9 (HIGH): 431 unique strikes.
- CVSS 4.0–6.9 (MEDIUM): 370 unique strikes.

Evasion techniques were not included in this round of testing; the Evasions setting in BreakingPoint was left at default.

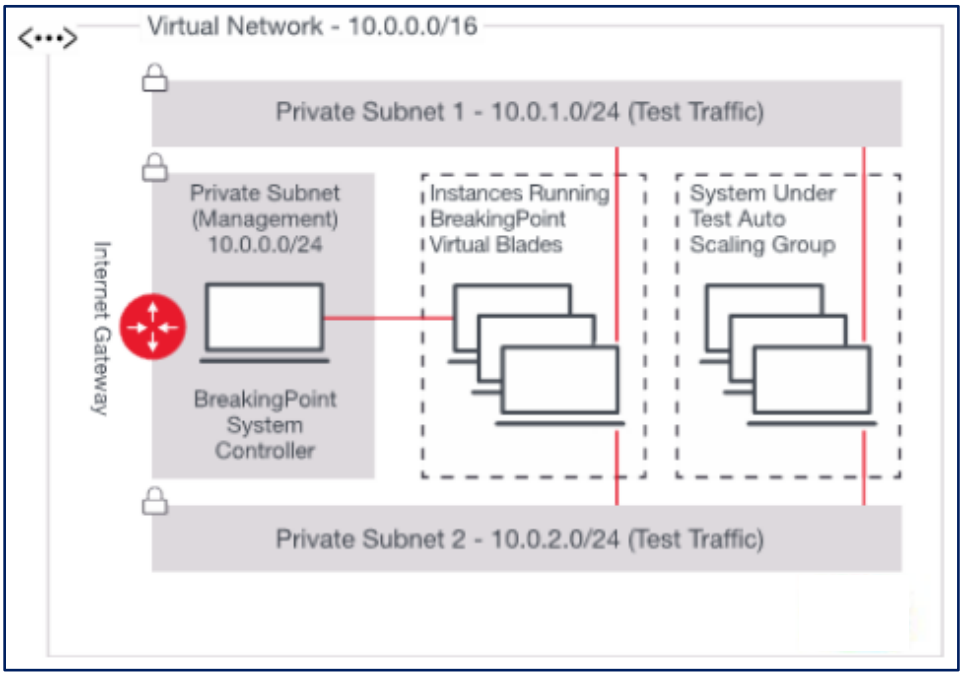
All strike tests were executed using BreakingPoint's Security test module. A single test case was created and configured with CVSS-based strike lists, then exported and imported across all BreakingPoint instances to maintain consistency. Testing was conducted in single-strike mode, where each strike was executed sequentially.

BreakingPoint was configured with one client and one server IP address. Testers confirmed that no IP-based filtering or blocks were in place, ensuring that detection was based solely on signatures or behavioral heuristics.

The BreakingPoint Application Simulator was used to generate benign traffic and test for false positives. Dedicated test runs using only the simulator were conducted in each environment to confirm that legitimate application traffic was not improperly blocked.

Copyright © Miercom 2025

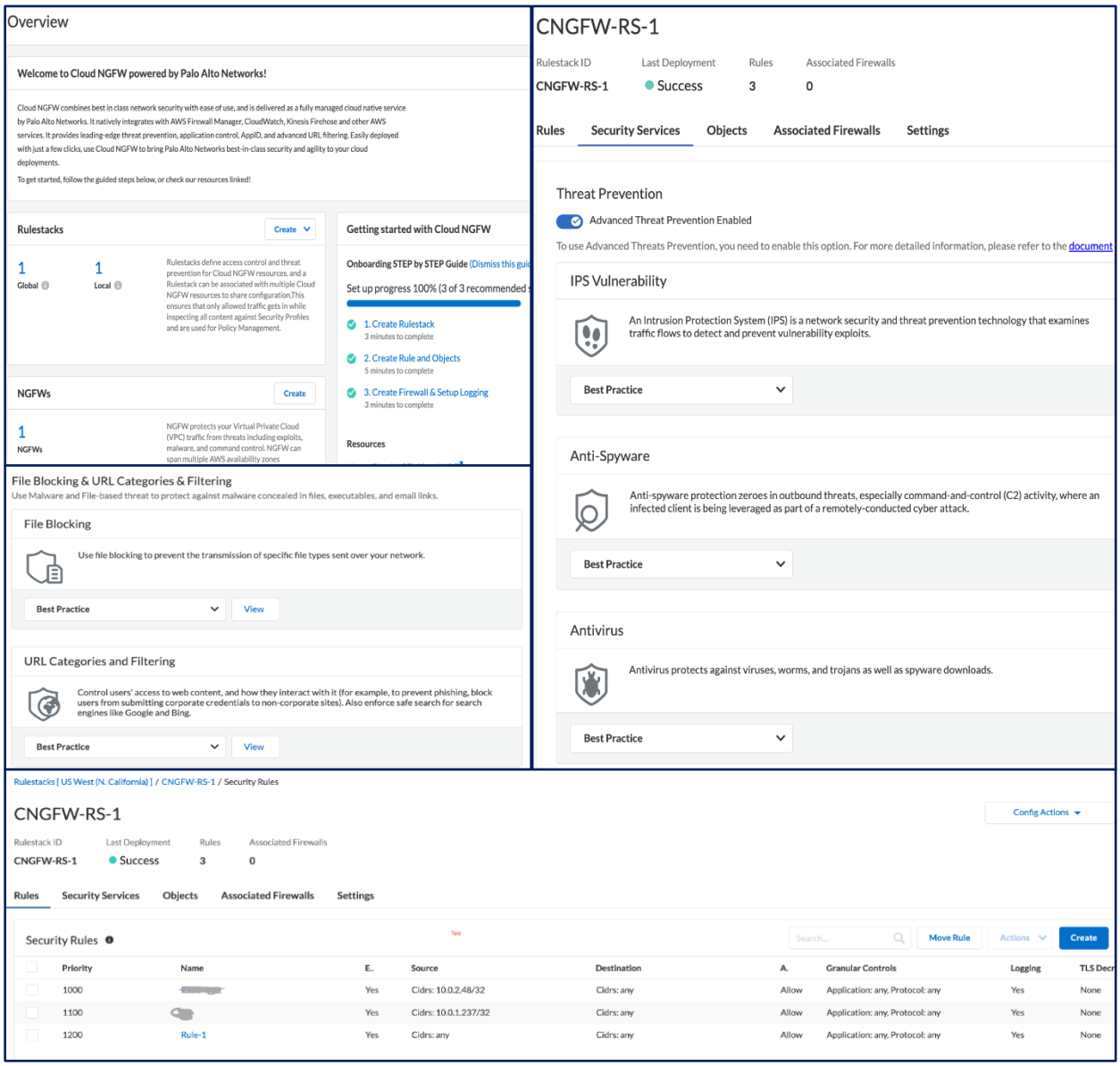
Test Environment



This diagram illustrates the test environment topology used to simulate a real-world deployment of each cloud network firewall. It highlights the structured layout of virtual networks and subnets designed to evaluate the security efficacy of the firewall system under traffic scenarios.

Copyright © Miercom 2025

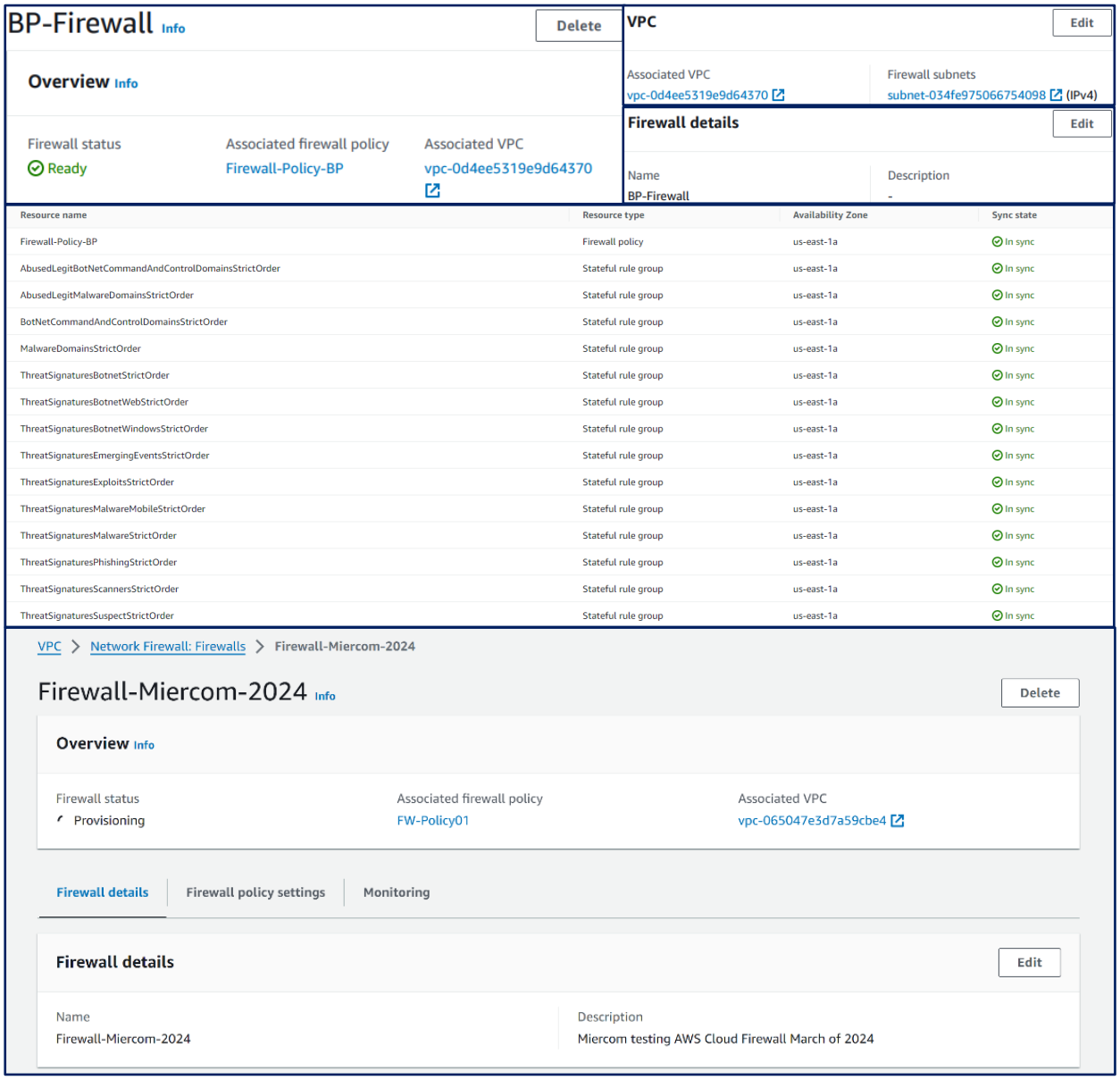
Palo Alto Networks Cloud NGFW Configuration



Configuration overview of Palo Alto Networks Cloud NGFW deployment on AWS, showing the RuleStack with security rules, threat prevention settings (IPS, Anti-Spyware, Antivirus), file blocking, URL filtering, and logging enabled.

Copyright © Miercom 2025

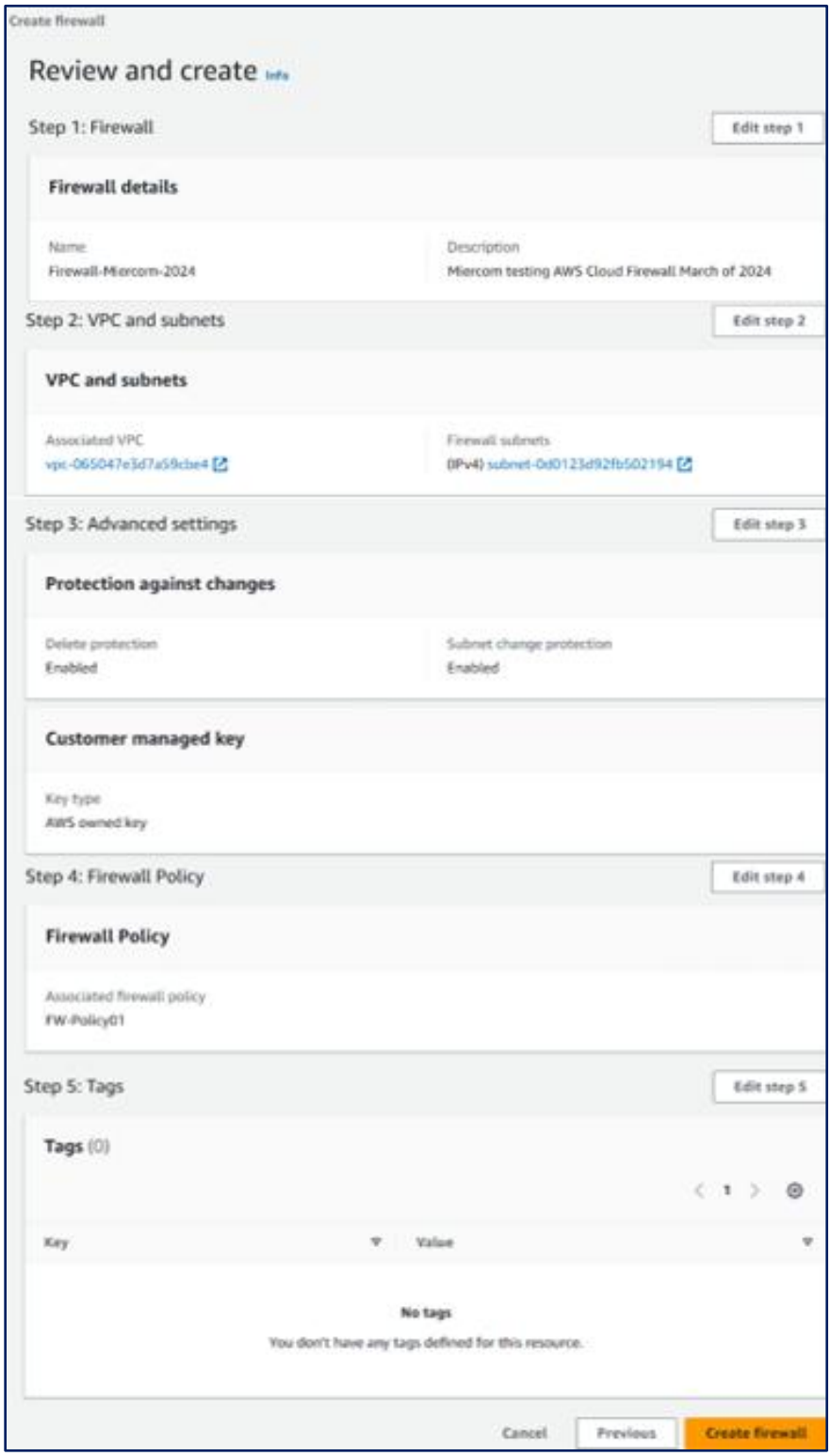
AWS Network Firewall Configuration



This view displays the configuration details of the deployed firewall, including its associated VPC, firewall policy and subnets. It also lists the attached stateful and stateless rule groups, confirming their deployment status across availability zones. The final confirmation screen indicates successful firewall creation.

Copyright © Miercom 2025

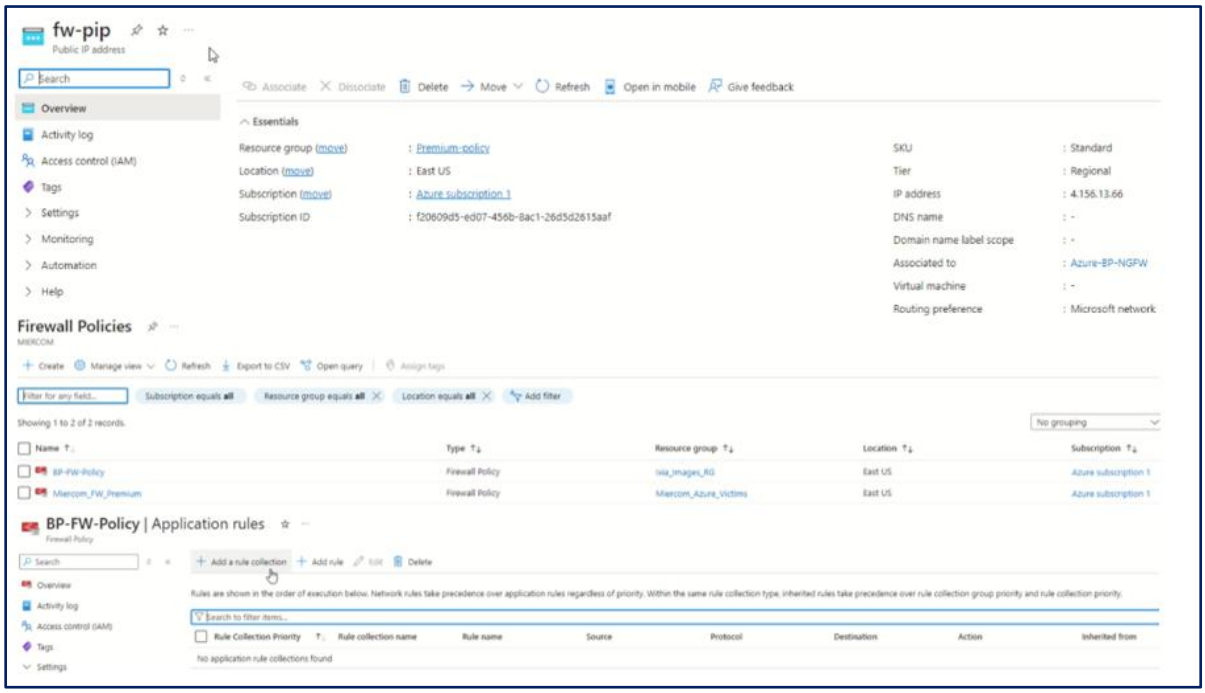
AWS Guided Firewall Creation



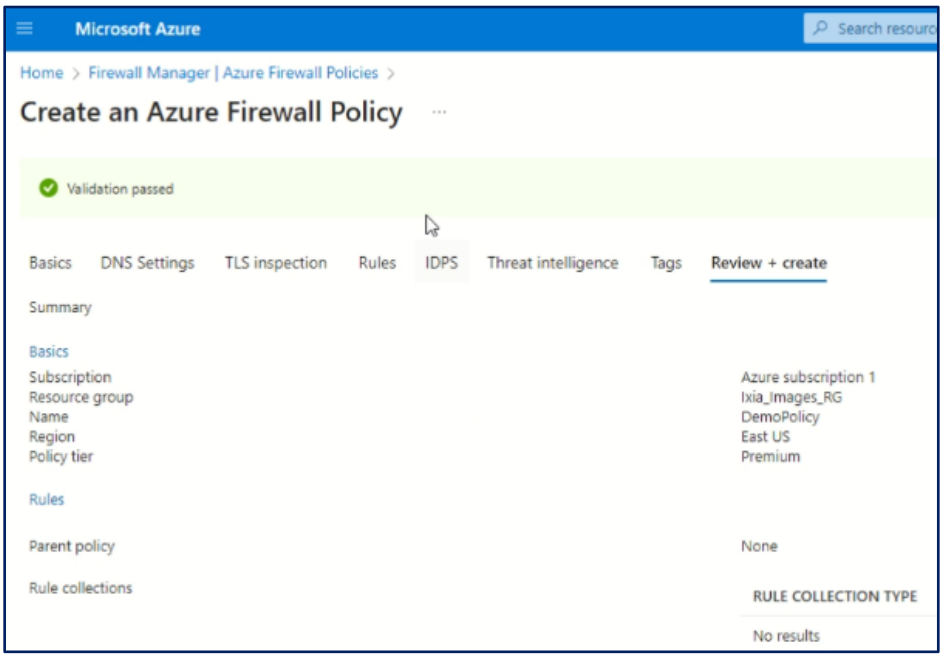
This image summarizes all firewall configuration parameters prior to deployment, including VPC association, subnet selection, policy assignment, protection settings, and tags. It reflects AWS's step-by-step wizard, designed to streamline setup and prevent misconfiguration.

Copyright © Miercom 2025

Azure Firewall Configuration



This composite image combines three views of the configurations of an Azure Firewall instance. The top section shows metadata for the public IP associated with the firewall. The middle section displays a list of deployed firewall policies and their associations. The bottom section presents the application rule editor for the selected policy, where administrators can define rules collections to manage traffic flows.

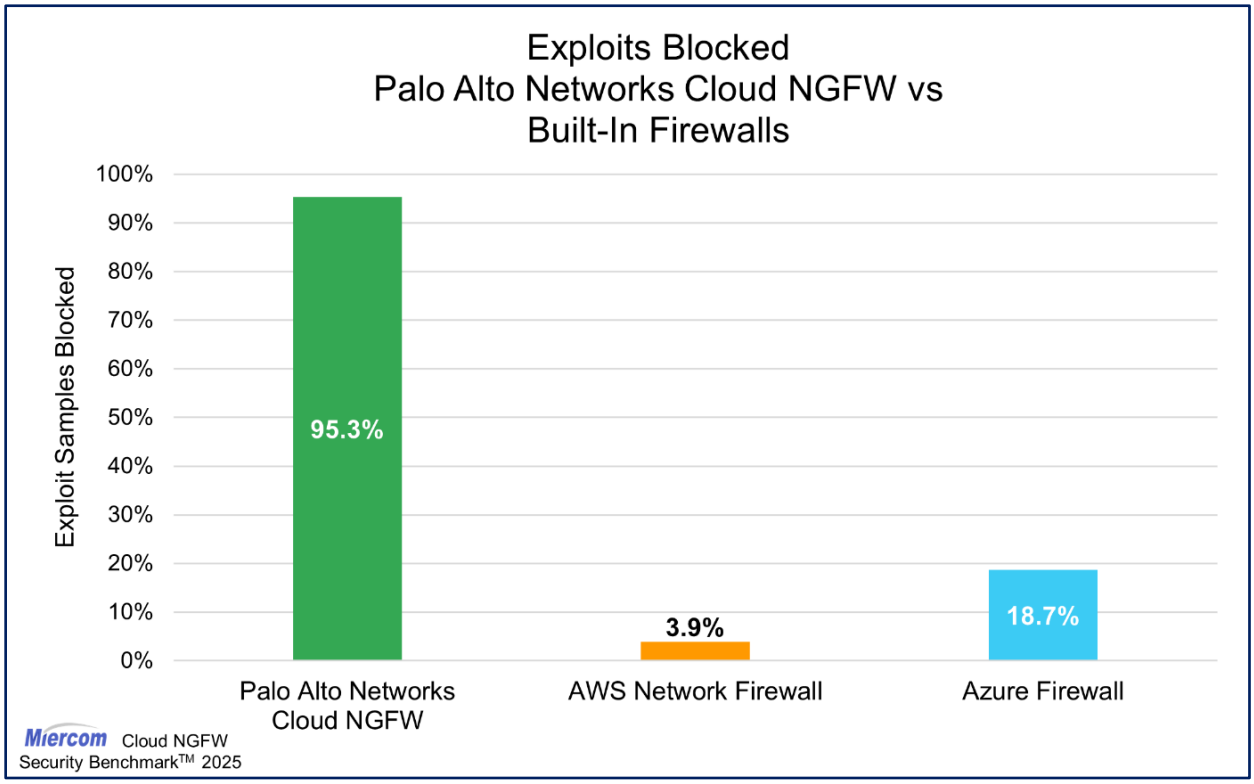


This image show the final validation and summary step before deploying an Azure Firewall policy It includes the policy name, associated subscription and resource group, region and selected policy tier (Premium). This structure highlights the available configuration categories, such as DNS settings, TLS inspection and threat intelligence.

Copyright © Miercom 2025

5.0 Exploit Detection and Resistance

In the evaluations conducted, testing covered a total of 951 vulnerabilities with CVSS 3.1 scores ranging from 4 to 10—medium, high, and critical vulnerabilities.



The effectiveness of Palo Alto Networks, AWS, and Azure in blocking CVSS vulnerability exploits. Palo Alto demonstrates the highest blocking rates across all categories, significantly outperforming AWS and Azure.

Exploit Detection and Resistance	
Evaluate the ability of the cloud network firewall to block vulnerabilities with CVSS 3.1 scores ranging from 4 to 10—medium, high, and critical vulnerabilities.	
●	**Palo Alto Networks Cloud NGFW** – Successfully blocked 901 out of 951 vulnerabilities, translating to a blocking rate of 94.7%. Palo Alto Networks was approximately five times more effective in blocking vulnerabilities than Azure Firewall. Against AWS Network Firewall, Palo Alto's performance was significantly higher, with an increased effectiveness of roughly 24 times.
○	**AWS Network Firewall** – Blocked 36 out of 951 vulnerabilities translating to a blocking rate of 3.9%. It was the least effective solution evaluated performing significantly lower than Palo Alto Networks.
○	**Azure Firewall** – Blocked 151 out of 951 vulnerabilities translating to a blocking rate of 18.7%. It was more effective than AWS but was significantly outperformed by Palo Alto Networks.

Key				
●	◕	◑	◔	○
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support

Copyright © Miercom 2025

6.0 Malware Detection

Testing focused on the protection against the threat categories listed below. The Miercom malware server simulates a hacker's attack server which hosts thousands of malware samples that characterize the breadth of coverage provided by Palo Alto Networks Cloud NGFW solution.

Samples from the Miercom malware server are used in industry-wide studies of malware detection for network security devices. Common malware types include botnets and Remote Access Trojans. An emphasis is placed on active threats, advanced evasion techniques and advanced persistent threats which are more complex and challenging categories for security solutions to identify. Detection results highlight each vendors approach and depth in identifying diverse malware threats.

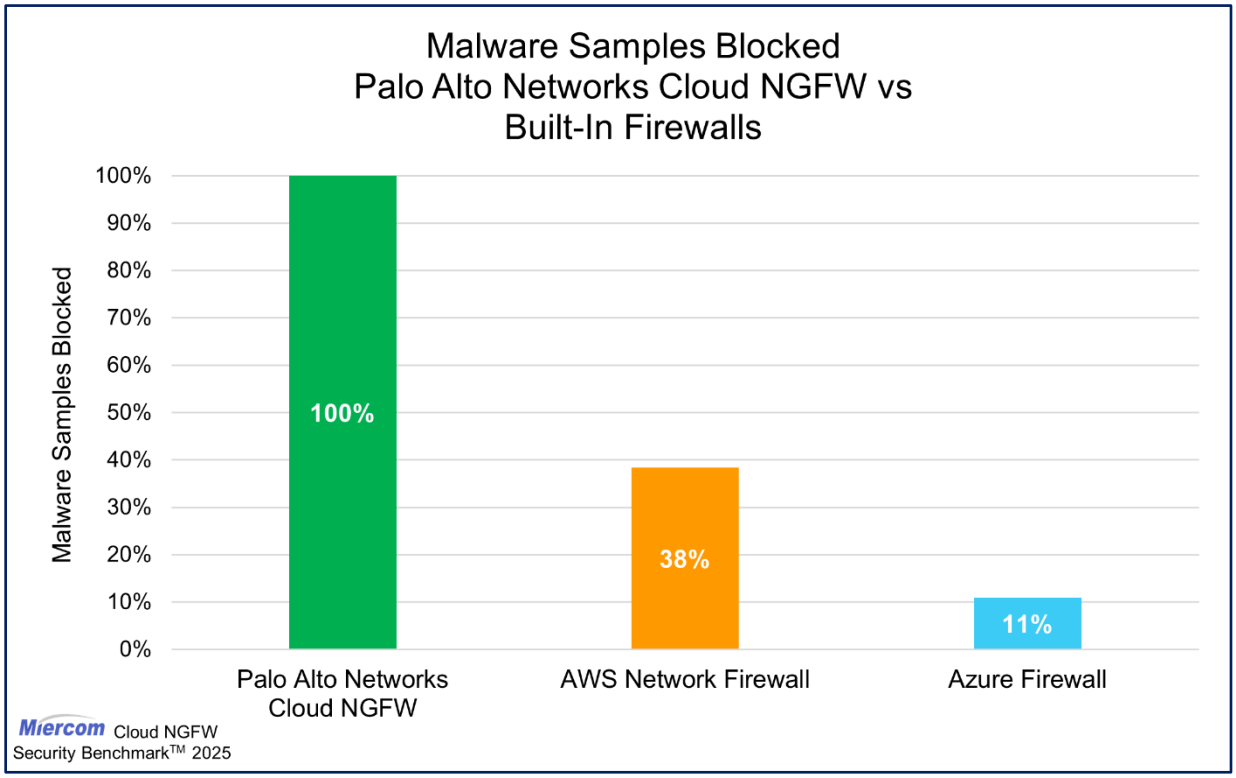
The SUT was an intermediary between untrusted and trusted zones of the simulated network. A simulated attack from the untrusted zone consisted of an attempted download of a malicious file. A successful block was logged when the simulated victim client cannot download the malware sample.

Standard Malware
Active Threat These involve real-time exploitation of known vulnerabilities. Attackers actively leverage laws to install malware, steal data or disrupt systems. Timely detection is crucial, as delays allow attackers to persist within networks undetected.
Backdoor Backdoors are hidden entry points into systems, often planted via trojans, rootkits or exploited vulnerabilities. Once inside, attackers can bypass authentication to exfiltrate or maintain control. Their stealthy nature makes detection challenging without behavior-based monitoring.
Botnets A botnet is a collection of infected devices remotely controlled by an attacker. Botnets enable large-scale attacks like DDoS, credential theft, and crypto mining. Detection focuses on identifying anomalous outbound communication patterns from infected endpoints.
Legacy Older, well-documented malware strains expected to be caught by signature-based tools. However, unpatched or outdated systems may still be vulnerable, highlighting the need for continuous endpoint visibility and coverage—even for "known" threats.
Malicious Documents Files like .doc, .xls, or .pdf can carry embedded code—often macros or scripts—that execute malware when opened. Detection depends on deep file inspection and sandboxing, as malicious behavior is typically triggered post-delivery.
Remote Access Trojans (RATs) RATs masquerade as legitimate software and give attackers remote control of a compromised system. They are used for surveillance, data theft, and deploying secondary malware. Detection is difficult due to their covert operation and ability to mimic trusted processes. Notable Examples: DarkComet: Captures keystrokes, webcam footage, and system files. Ghost RAT: Used in Operation GhostNet for geopolitical espionage across over 100 countries.
The Onion Router (TOR) Attackers distribute trojanized TOR browsers that steal data while appearing to offer anonymity. These often collect personal info and reroute it to C2 servers. Detection involves monitoring outbound traffic to known TOR exit nodes or suspicious C2 destinations.

Copyright © Miercom 2025

Zero Day Malware These threats exploit vulnerabilities not yet known to vendors or defenders. With no existing signature, detection requires advanced heuristics, behavioral analytics, or machine-learning-based anomaly detection.
Mobile Malware Targets smartphones and tablets, exploiting app vulnerabilities or mobile OS weaknesses. As mobile use grows, so does its attack surface. Threats include spyware, SMS trojans, backdoors, and droppers—often spread via third-party app stores or phishing.
Advanced Threats
Advanced Evasion Techniques (AETs) These techniques mask malicious traffic to bypass firewalls or IDS. AETs blend fragmented packets, obfuscated protocols, or encryption to slip through defenses unnoticed. Effective detection requires deep packet inspection and contextual correlation. Examples: IP Fragmentation – Splits payloads to evade filtering TCP Segmentation – Obscures attack signatures Protocol Violations – Confuses rule-based detection
Advanced Persistent Threats (APTs) APTs are long-term, stealthy attacks often conducted by nation-state actors. They combine social engineering, RATs, and privilege escalation to extract high-value data or disrupt operations. Detection hinges on long-term behavioral baselining and lateral movement monitoring. Examples: DarkComet – Used by state-sponsored actors for spying CryptoWall – Ransomware used in prolonged data extortion campaigns
Modified Malware Variants of known malware that are altered to bypass existing signatures. Modifications may include payload obfuscation or delivery method changes. Detection relies on sandboxing and code similarity analysis. Examples: Modified TOR Browser Exploits – Appear legitimate while sending data to attackers Diamond Sleet Supply Chain Attack – Altered installer with secondary malicious payload
Polymorphic, Zero-Day Malware Polymorphic malware constantly mutates its code, evading signature-based detection. Often combined with zero-day tactics, these threats require behavior and memory analysis for detection. Examples: Storm Worm – Changed code every 30 minutes CryptoWall – Ransomware that built unique binaries per victim BeeBone – Malware with up to 19 daily code changes to maintain persistence and avoid detection

Copyright © Miercom 2025



This chart compares the effectiveness of malware blocking by Palo Alto Networks, AWS, and Azure across different threat levels: critical high, medium, and low. Palo Alto Networks demonstrates 100% block rate across all categories, while AWS shows varied effectiveness, and Azure exhibits lower performance in detecting and blocking malware.

Malware Detection	
Evaluate the ability of the cloud network firewall to protect against samples from the Miercom Malware Set including Advanced Threats.	
●	**Palo Alto Networks Cloud NGFW** – Successfully blocked 100% of the samples tested. It blocked more than two times the samples that AWS Network Firewall blocked. Against Azure Firewall, Palo Alto's performance was significantly higher, blocking over nine times the amount of samples.
◔	**AWS Network Firewall** – Blocked 38% of the samples tested. It blocked more than three times the amount of samples Azure Firewall was able to block but was not nearly half as effective as Palo Alto.
○	**Azure Firewall** – Blocked 11% of the samples tested. It performed significantly lower than both Palo Alto Networks and AWS.

Key				
●	◕	◑	◔	○
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support

Copyright © Miercom 2025

7.0 Evasion

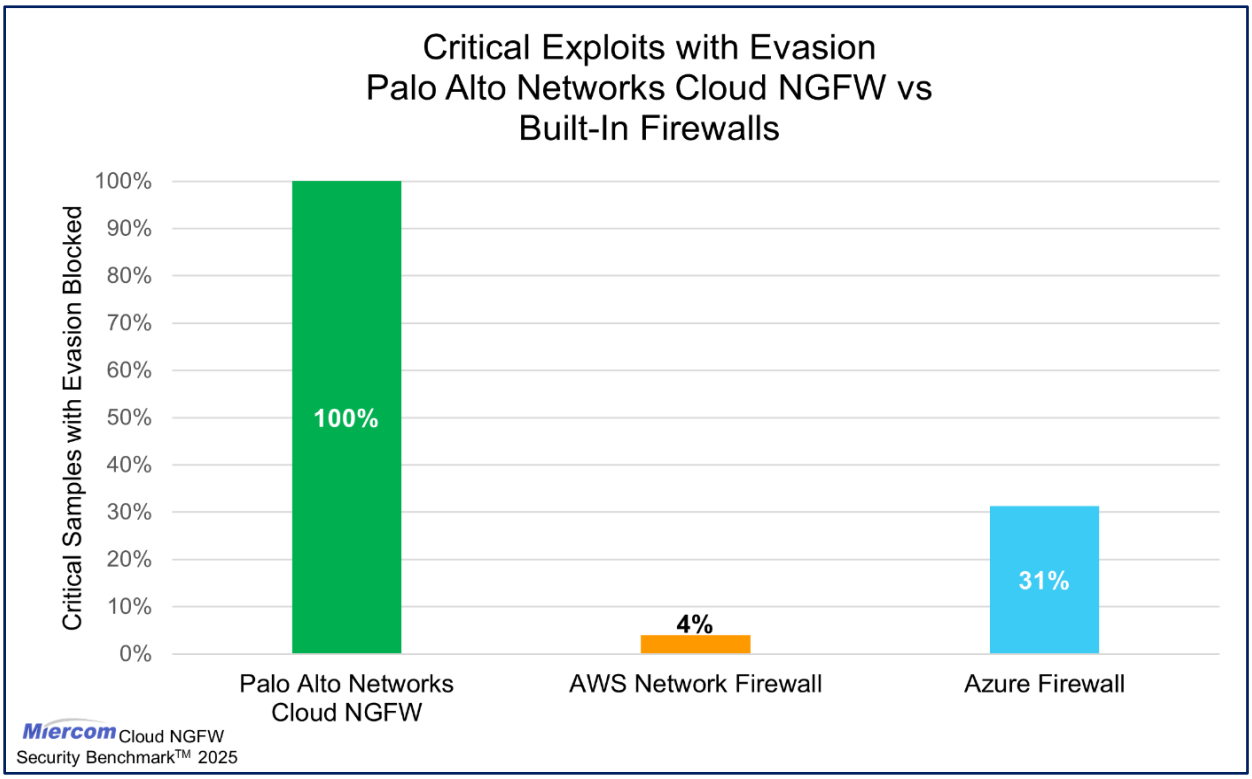
Cybersecurity evasions are tactics used to conceal malicious activity during transit or execution, allowing threats to bypass detection. As attackers evolve their methods, traditional defenses like signature-based detection often fail, especially against zero-day exploits. While dynamic analysis offers deeper insight, it is resource-intensive and prone to false results. Advanced evasion techniques also demand specialized expertise, adding complexity for defenders.

To counter these threats, organizations need a layered approach—combining signature-based tools with behavioral analysis, heuristics, machine learning, and anomaly detection. Staying current with threat intelligence and adopting proactive defense strategies are essential for identifying and blocking modern evasion techniques.

In Miercom testing, Palo Alto Networks Cloud NGFW block 100% of critical exploits using evasion techniques, compared to 4% for AWS Network Firewall and 31% for Azure Firewall *(see chart)*. This underscores the challenge built-in firewalls face when confronting modern evasive threats.

Miercom Evasive Malware
Environmental Awareness Malware detects virtualized environments by scanning for sandbox indicators like hypervisor DLLs, system configurations or usernames (e.g., "VirtualBox," VMware"). If detected, it may suspend malicious behavior to avoid detection.
Time-Based Method Targeting short sandbox execution windows, malware may: • Use extended sleep cycles (e.g., 10+ minutes) to delay execution. • Employ logic bombs to trigger specific dates. • Run CPU-stalling code to waste processing time and exit before payload delivery.
User Interaction Some malware waits for specific human behaviors—mouse movement, clicks, app use—before executing, making it harder to detect in automated test environments.
Domain, IP Identification and Internet Connection Certain threats verify live internet connectivity or target-specific IPs before loading their payload or contacting command-and-control (C2) servers, delaying or halting execution in isolated test setups.
Stegosploit This method embeds malicious scripts within image files, enabling browser exploits to be delivered through seemingly harmless content—an evasion approach difficult to detect with traditional scanners.
Code Obfuscation, Encryption or Compression To hinder analysis, malware may encrypt or compress code and only decrypt it at runtime. This prevents static tools from identifying malicious functionality. Banking trojans like *Lampion* and *URSA* use these method to hide C2 details, commands and API calls.

Copyright © Miercom 2025



This chart compares the effectiveness of blocking critical exploits with evasion techniques. Palo Alto Networks Cloud NGFW blocked 100% of evasive exploits while AWS Network Firewall's 4% and Azure Firewall's 31% block rate were notably lower.

Evasion	
Basic evasion techniques were used via the obfuscation setting options in the BreakingPoint Test System.	
●	**Palo Alto Networks Cloud NGFW** – Successfully blocked 100% of evasive exploits. Significantly outperforming Azure and especially AWS.
○	**AWS Network Firewall** – Blocked 4% of evasive exploits. Demonstrating a severe lack of ability in blocking the most basic evasion techniques.
◔	**Azure Firewall** – Blocked 31% of evasive exploits outperforming AWS but only demonstrating less than a third of the block rate shown by Palo Alto Networks.

Key				
●	◕	◑	◔	○
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support

Copyright © Miercom 2025

8.0 Administrator Experience (Admin UX)

Description – The SUT should have a high standard for overall usability, clarity, responsiveness and efficiency of the management interface and supporting administrative workflows of a Cloud NGFW solution. It encompasses the quality and intuitiveness of the user interface (UI), the ease of performing common administrative tasks, such as policy creation, rule modification, threat monitoring and system configuration, as well as the effectiveness of documentation and support tools that assist in these operations.

Impact – A well-designed Admin UX is critical for operational efficiency and security assurance. Administrators are tasked with managing increasingly complex environments and any friction in the interface or lack of clarity in configuration can lead to misconfigurations, policy gaps, or delayed response to threats. Streamlined workflows, intuitive dashboards and accurate visibility into traffic and policy enforcement reduce human error and greatly improve the ability of teams to respond quickly and effectively to network security events.

Evaluation Procedure – Each SUT was deployed in a simulated real-world environment, following best practices as outlined by the vendor's official documentation and, where applicable, with guidance from vendor support. This evaluation specifically emphasized administrative operations, performing common configuration and management objectives using the native management interface. Miercom assessed usability features, clarity of workflows and the effectiveness of integrated tools such as reporting exports, third-party dashboard integrations and wizards.

Observation and Rating – Administrator Experience (Admin UX)

Palo Alto Network Cloud NGFW delivers a streamlined deployment experience with clear documentation and minimal setup operating cost. The provisioning process follows a guided three-step workflow: activating the service through the vendor's cloud portal, creating rule stacks, and deploying the firewall. Administrators are prompted through concise console steps—selecting cloud accounts, VPCs, rule stacks, and optional subnets. Once deployed, the firewall appears as a VPC endpoint, requiring only a route table update for traffic flow.

The firewall operates transparently and does not require infrastructure management or software maintenance. Default best-practice security profiles are automatically applied, ensuring baseline protection. Advanced configurations are supported via CloudFormation, REST APIs, and Terraform.

Configuration modifications are made through a rule stack interface. Rules are defined using descriptive names, priorities, and object-based matching, with dropdown selectors for setting actions and profiles. Real-time enforcement and rule activity are visible via CloudWatch. Security profiles can be customized or cloned for granular control of malware, URL filtering, and file types.

Logs are structured into Traffic, Threat, and Decryption categories and are exported in real time to CloudWatch Logs, S3, or Kinesis. Each log includes actionable metadata (IPs, ports, verdicts, etc.) and threat severity ratings. Audit logs are configured in the console and forwarded to a specified CloudWatch Log Group after a one-time CloudFormation update.

Copyright © Miercom 2025

Policy enforcement can be enhanced using dynamic threat feeds, which are easily applied to rules. Optional integration with Panorama offers centralized visibility across deployments, including filtering by rule hits and threat activity.

Cloud NGFW supports automation through IaC tools and includes prebuilt CloudFormation and Terraform templates for onboarding up to 100 accounts. Documentation is well-organized with step-by-step guidance. During evaluation, Palo Alto Networks' support team was responsive and helpful, contributing to a smooth onboarding experience.

Amazon Web Services (AWS) provides a default firewall offering, but its capabilities are more in line with a traditional, legacy firewall. While basic rules sets and limited signature support can be configured without incurring additional cost, extending its functionality to meet the baseline of a modern Next Generation Firewall (NGFW) requires manual configuration that is both non-intuitive and complex. As a result, most enterprises will find it more practical and secure to deploy a third-party NGFW solution such as Palo Alto Networks.

Deploying a third-party NGFW within AWS, however, demands security personnel familiar with both vendor-specific configurations and the operational nuances of cloud deployments. During our evaluation of the AWS native firewall—configured using publicly available documentation—we observed significant shortcomings in threat prevention. The firewall blocked fewer than 6% of attacks in CVE-based strike testing (Critical, High, and Medium).

The configuration process also proved cumbersome. Documentation lacked comprehensive, end-to-end guidance, and several basic features required direct engagement with AWS support to enable. These findings highlight the need to carefully weigh operational complexity and security effectiveness when choosing between AWS's native firewall and third-party NGFW solutions.

Azure's administrative experience presented several usability challenges. While core infrastructure remained stable, managing firewall services and networking components often felt cumbersome. Routine tasks, like editing VM settings, required navigating nested menus—unlike AWS or Palo Alto Networks, which support direct edits from root views—slowing operations and complicating basic tasks. Resource deletions, such as VNets, were also hindered by dependency errors without links or guidance to resolve them.

Identifying the correct firewall SKU added confusion. "Firewall" defaults to a limited offering, while NGFW features require manually selecting the "Premium" SKU. Searches for "NGFW" returned mostly third-party solutions, further complicating onboarding. Some configurations lacked clarity. A static route using "0.0.0.0/0" failed silently; only after contacting support was it corrected to a specific subnet. No error or log flagged the issue.

Traffic visibility and logging were also behind peers. Azure lacks tools equivalent to AWS Palo Alto. Network Watcher and Connection Monitor require multi-step setup, and enabling firewall logs involves configuring Log Analytics, workspaces, and monitoring policies.

Though Azure was functionally sound, its admin experience lacked the clarity, efficiency, and visibility provided by other platforms**.**

Copyright © Miercom 2025

Ease of Initial Configuration	
Evaluates how intuitive and streamlined the setup process is when initially deploying the firewall solution.	
●	**Palo Alto Networks** –Delivers a highly accessible deployment experience through a simple, guided interface. Creating a firewall requires only a few inputs—name, cloud account, VPC, and rule stack—followed by automatic provisioning of the endpoint. Users can optionally define subnets or availability zones, and once deployed, the firewall appears as a VPC endpoint requiring only basic route table updates. The minimal manual input and intuitive flow make initial configuration fast, predictable, and admin-friendly.
◕	**AWS** – Provided a relatively simple initial setup, but with limited rule sets and features unless upgraded to a third-party NGFW.
◑	**Azure** – Initial setup was less intuitive, requiring users to navigate modules and unclear firewall tier distinctions during deployment.
Moves, Adds and Changes (MAC)	
Assess how easily admins can modify configurations, such as updating firewall rules, routes or VM policies.	
●	**Palo Alto Networks** – Provides a clear, modular interface for updating firewall rules and security profiles. Admins can make changes quickly using object-based rule creation, dropdown match criteria, and editable best-practice profiles. Policy changes are immediately validated through real-time logging, and the workflow avoids the complexity or silent failures seen in other platforms. The overall experience is efficient, predictable, and admin-friendly.
●	**AWS** – No complications. Standard administrative tasks were straightforward.
◔	**Azure** – Configuration changes were cumbersome and nested; one routing configuration was accepted by the UI but failed silently, requiring support assistance.
Traffic and Visibility	
Measures the clarity and accessibility of monitoring tools that distinguish between allowed traffic and blocked threats.	
●	**Palo Alto Networks** –Streamlined and accessible traffic visibility through pre-defined log types and seamless cloud integration. Logs are easy to configure, rich in detail and instantly usable for monitoring allowed and blocked activity, providing both operational clarity and strong security oversight.
●	**AWS** – Administrators can configure logging through predefined log types each providing actionable insight into firewall behavior. Logs are natively integrated simplifying real-time monitoring and long-term analysis without requiring additional setup.
○	**Azure** – Lacked an integrated tool like for real-time visibility, relying instead on complex setup of Network Watcher and Connection Monitor.
Export Reporting	
Examines the ability to export logs and security reports for further analysis.	
●	**Palo Alto Networks** –Straightforward, audit-grade log exports via CloudWatch with minimal configuration steps. While initial setup requires updating the CloudFormation template, the export process is well-documented and tightly integrated into the cloud ecosystem, making log access and external analysis highly accessible.
●	**AWS** – Log exports were supported and could be pushed to S3 or accessed via the UI.
◕	**Azure** – Exporting firewall and network logs required setting up multiple support services, making the process more complex than necessary.

Copyright © Miercom 2025

Policy Conflict Detection and Configuration Safety	
Evaluates whether the system identifies conflicting or ineffective configurations.	
◕	**Palo Alto Networks** – Palo Alto Cloud NGFW enables detailed and threat-informed policy creation using intelligent feeds and central management via Panorama, supporting effective enforcement. While post-deployment log analysis is strong, the lack of built-in real-time configuration conflict detection leaves room for improvement in UX.
◔	**AWS** – While logs provide context for post-deployment troubleshooting, real-time alerts or guided validation during configuration are limited, making misconfigurations possible if admins are not vigilant.
○	**Azure** – The platform allowed invalid route configurations without alerting the user, resulting in silent failure and additional troubleshooting.
Ease-of-Use Enhancements (Wizards, Templates, Bulk Tools)	
Looks for interface features that simplify or accelerate configuration, like wizards or templates.	
●	**Palo Alto Networks** –Extensive ease-of-use features, including guided setup, CloudFormation and Terraform templates and bulk onboarding tools, enabling fast, scalable, and consistent policy deployment.
●	**AWS** – A guided setup is available directly in the AWS Console, walking users through key steps like creating firewalls and defining rule groups. It provides prebuilt CloudFormation templates that automate deployments and support common architectures. Administrators can also leverage AWS-managed rule groups to apply preconfigured threat protections without manual rule creation.
○	**Azure** – No wizards or ease-of-use features were identified; configuration was tedious and repetitive.
Documentation and Online Support Resources	
Evaluates clarity, comprehensiveness, and accessibility of vendor-provided documentation, help portals, and online support resources.	
●	**Palo Alto Networks** – Clear documentation and responsive support made configuration and troubleshooting straightforward.
◑	**AWS** – Documentation lacked comprehensiveness, often requiring support engagement for basic functionality.
◔	**Azure** – Documentation was unclear, with ambiguous firewall definition and misleading search results directing users to third-party NGFWs.
Onboarding Experience	
Evaluates the clarity, completeness and accessibility of official documentation, in-product guidance and searchable online resources that assist administrators with configuration and troubleshooting.	
●	**Palo Alto Networks** – Provides clear, well-documented onboarding process supported by guided steps and responsive technical support.
◑	**AWS** – Onboarding was manageable, but limited feature exposure and documentation gaps impacted early experience quality.
◔	**Azure** – The onboarding experience was hindered by unclear UI structure, ambiguous firewall naming and insufficient guidance during initial deployment.

Key				
●	◕	◑	◔	○
Excellent UX	Good UX	Fair UX	Poor UX	No Support

Copyright © Miercom 2025

9.0 About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

10.0 Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation, or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness, or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading, or deceptive or in a manner that disparages us or our information, projects or developments.

Miercom's Fair Test Policy allows for any vendor evaluated to challenge or retest these results in accordance with Miercom Terms of Use Agreement if there are any disagreements in our findings presented here.

Miercom did not acquire products for this review, nor has Miercom agreed to any vendor's End User License Agreement (EULA) or any other overly restrictive agreements that limit free press, product evaluations, editorial works, or publishing product reviews. We believe in providing accurate information to assist customers make informed purchasing decisions.

By downloading, circulating, or using this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.

© 2025 Miercom. All Rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors. Please email reviews@miercom.com for additional information.