Miercom

April 2023
DR230116E

FORTINET

Fortinet FortiGate 200F v. Palo Alto Networks PA-460 NGFW Security Efficacy Assessment

Table of Contents

1.0 Executive Summary

Fortinet commissioned Miercom to conduct a next-generation firewall (NGFW) test. NGFW security testing is an essential part of ensuring the effectiveness of an NGFW in protecting against cyber threats. Fortinet FortiGate 200F outperformed the Palo Alto Networks PA-460 on all security tests in the $5K to $10K price band.

We simulated various attacks - measuring the firewall's ability to detect and prevent them. NGFW testing can include evaluations of a firewall's effectiveness against malware, viruses, hacking attempts, and other types of cyber vulnerability threats. It may include testing the firewall's ability to block malicious traffic, protect against data leakage, and enforce access controls. The results can be used to identify vulnerabilities in a firewall's security posture, leading to necessary improvements. With regular NGFW security testing, organizations ensure that their networks are protected against a wide range of cyber threats - maintaining the confidentiality, integrity, and availability of their data.

Independent Testing Key Findings

- **Many cybersecurity vendors claim best of breed and real-time protection with AI/ML. The results show a difference.**
- **Superior Performance on BreakingPoint Strike Test Level 3:** Fortinet FortiGate outperformed Palo Alto Networks on the BreakingPoint Strike Level 3 test on all metrics including high-risk vulnerabilities such as worms and backdoor exploits.
- **Superior Performance on BreakingPoint Strike Test Level 5:** Fortinet FortiGate outperformed Palo Alto Networks on the BreakingPoint Strike Level 5 test on all metrics - including vulnerabilities such as worms, backdoors, probes, and DDoS flaws.
- **Malware Detection:** With FortiGuard security subscriptions using AI/ML, Fortinet FortiGate blocked 5.4 times more malware and Zero Days than Palo Alto Networks in all malware detection security testing. Fortinet also had better Zero+1 Day and Zero+3 Day Malware Detection Efficacy. FortiGuard is more capable against malware - versus Palo Alto Networks Cloud Delivered Services and Unit42.
- **Ransomware Detection:** Fortinet FortiGate blocked more ransomware than Palo Alto Networks on all signature-based ransomware detection security efficacy testing.

The Fortinet FortiGate Next-Generation Firewall was validated for its protection against malware, malicious URLs, and data loss by testing within a simulated office network deployment. Its security extension across a distributed workforce was easily implemented with a single configuration, offering protection that earned it the Miercom Certified Secure certification.

Miercom Certified Secure.

Robert Smithers
CEO, Miercom

1.1 Summary of the Security Efficacy Testing

		Fortinet	Palo Alto Networks	Industry Average
Security	BreakingPoint Strike Pack Test 3	98%	84%	76%
	BreakingPoint Strike Pack Test 5	95%	84%	72%
	BreakingPoint Malware	79%	15%	35%
	BreakingPoint Ransomware	81%	0%*	45%
	Miercom AOST Zero Day +1 Day Malware Test Results	70.5%	41.4%	25%
	Miercom AOST Zero Day +3 Day Malware Test Results	94%	71.4%	75%

* For the PAN testing Ransomware, blocking by file type was disabled. Otherwise, PAN will block all the files used in testing, including the benign white samples.

2.0 Introduction

Miercom evaluated two Next Generation Firewall products (NGFW): Fortinet FortiGate 200F and Palo Alto Networks PA-460. We used real-world scenarios to compare the appliance's performance - measuring any degradation seen from security enablement.

Testing focused on the following:

- BreakingPoint Critical Strike Test Level 3 & 5
- BreakingPoint Malware & Ransomware
- Miercom Advanced Offensive Security Test (AOST) Zero Day, Day 1 & Day 3

2.1 Products Tested

Fortinet FortiGate 200F

The FortiGate 200F series provides an application-centric, scalable, and secure SD-WAN solution with next gen firewall (NGFW) capabilities for mid to large-sized enterprises deployed at the campus or enterprise branch level. Fortinet's Security-Driven approach provides tight network integration and next gen security protections. Their solution integrates a battery of AI-powered security services including best of breed IPS, Antivirus, Anti-Botnet and C&C protection, Sandbox, Application Control, URL, DNS & Video Filtering and other capabilities.
The solution also features system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, easy-to-deploy solution.

Additional information for the Fortinet FortiGate 200F series can be found:
Data Sheet:
https://www.fortinet.com

Palo Alto Networks PA-460

The Palo Alto Networks PA-460 is part of the PA-400 Series Next-Generation Firewall family.
We implemented Advanced Threat Prevention and Wildfire. We endeavored to enable every security feature for PAN except for indiscriminate block by file type.

Additional information for the Palo Alto Networks PA-460 series can be found:
Data Sheet:
https://www.paloaltonetworks.com

3.0 How We Did It

Keysight BreakingPoint Test System is a network security testing platform designed to help organizations and System Administrators assess the performance and security of their network infrastructure and applications. It simulates real-world network traffic and security threats, like malware, DDoS attacks, and network congestion, in a controlled environment. This enables organizations to test the resilience of their systems and identify vulnerabilities that may impact the performance and security of their networks. The platform offers a range of features and capabilities, including custom test scenarios, generating traffic at high speeds, and analyzing results in real-time. Engineers examined the throughput performance of Fortinet and Palo Alto Networks appliances in configurations with security services first disabled and then enabled. This testing was intended to measure the effect of security services enablement on firewall throughput performance. Miercom used the default configuration on all the devices tested, unless specified under each section.

Keysight (Ixia) BreakingPoint
Version 9.20.115.112
This appliance delivers increasing loads of TCP traffic to the test network through the DUT to determine maximum throughput rates. It also provides a robust and realistic environment for security testing, capable of over 30,000 malware samples and optimization of next generation firewalls, IPS and secure web gateways.

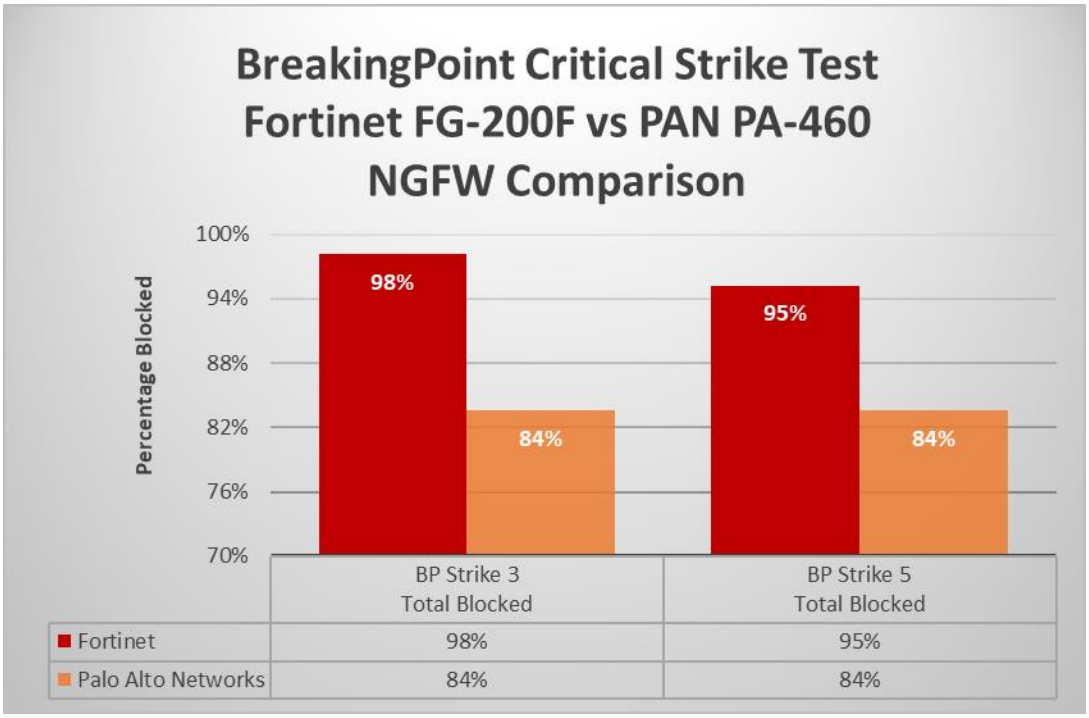
3.1 Products Evaluated

Vendor	Product	Version	Feature
Fortinet	**Fortinet FortiGate 200F**	**7.2.2 build 1255**	**IPS, Advanced Malware Protection that includes Antivirus, Anti-Botnet and C&C protection and Sandboxing, and separately, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium). All part of the Unified Threat Protection (UTP) package.**
Palo Alto Networks	**Palo Alto Networks PA-460**	**PAN-OS 10.2.0**	**Adv TP, Adv Wildfire, Adv URL, DNS Security, SD-WAN Premium Support**

4.0 BreakingPoint Critical Strike Tests

Miercom tested malware and ransomware using BreakingPoint by Keysight. We used Strike 3 and Strike 5 testing. Strike 3 Tests include all high-risk vulnerabilities, worms, and backdoors. This list contains approximately 480 strikes and usually completes in less than three minutes. Strike 5 tests target all vulnerabilities, worms, backdoors, probes, and denial of service flaws. This list contains approximately 2,400 strikes and usually completes within 30 minutes.

4.1 BreakingPoint Critical Strike Tests Percentage Blocked



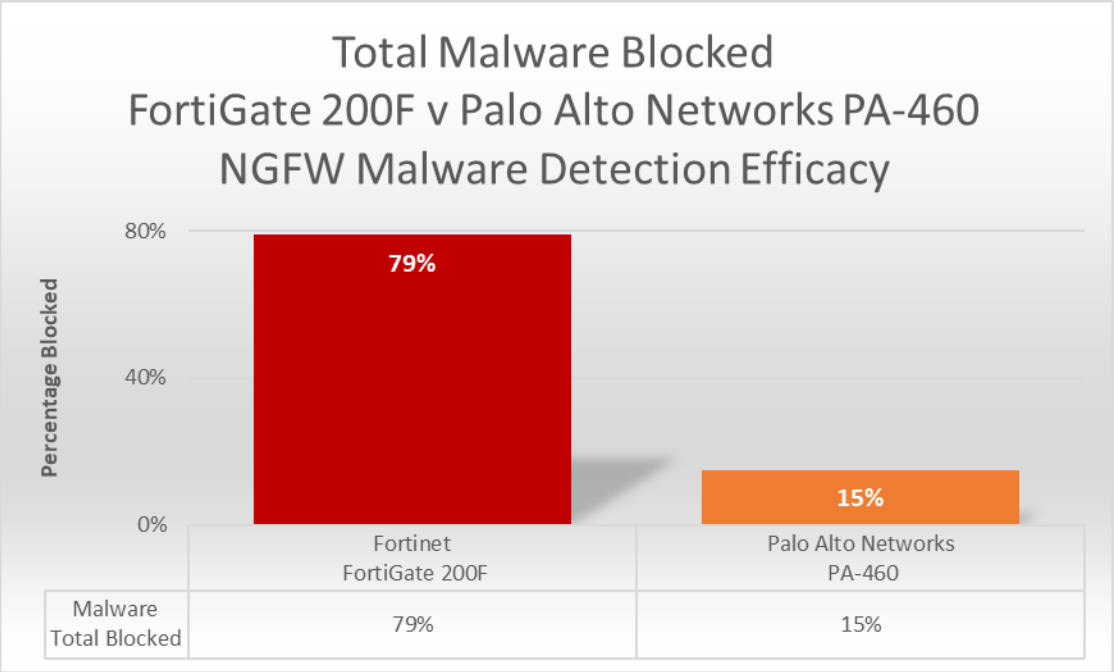
Fortinet FortiGate 200F outperformed the competition on all BreakingPoint Critical Strike 3 and 5 tests critical vulnerabilities delivered by Keysight Technologies BreakingPoint. Fortinet showed an additional 14% blocked for BP critical strike 3 and an additional 11% for critical level 5 attacks. Fortinet's improved security efficacy was noted while providing 1.5x better throughput during these tests.

5.0 BreakingPoint Ransomware and Malware Tests

The BreakingPoint ransomware and malware tests are designed to determine the point at which a system or network becomes overwhelmed by ransomware or malware attacks. The goal is to measure the ability of the DUT to detect and block malware and identify any vulnerabilities that could be exploited by attackers.

During these tests, the system or network is subjected to increasingly intense or complex ransomware and malware attacks. These tests are conducted using specialized software that simulates the behavior of ransomware or malware. NGFWs are considered to have reached their BreakingPoint when the system or network can no longer function normally or defend against attacks.

5.1 BreakingPoint Malware Test Results

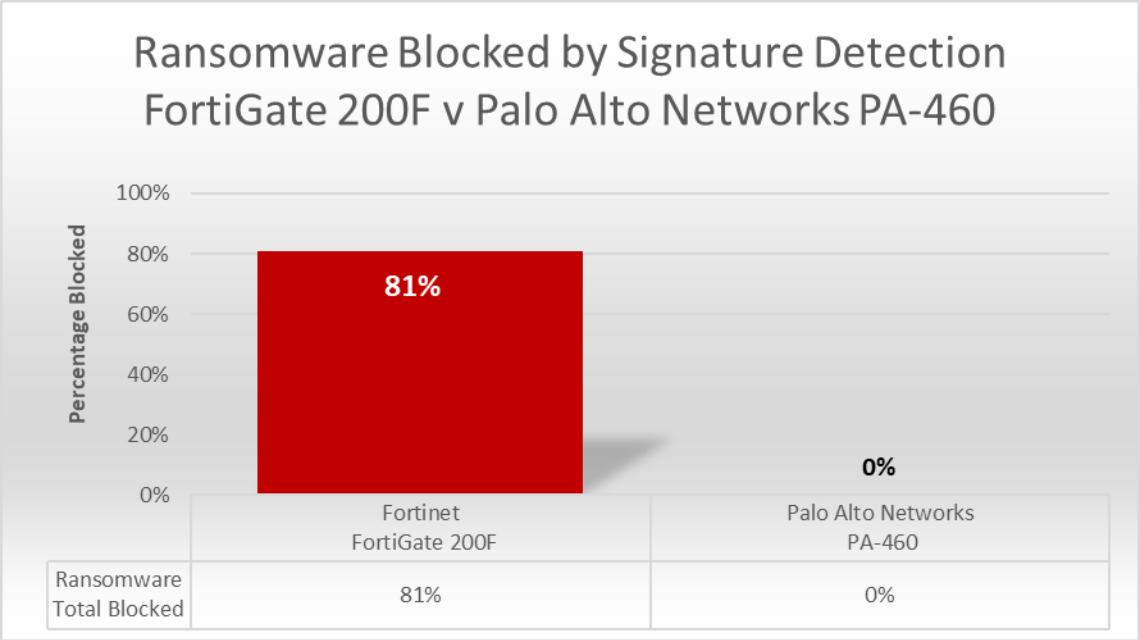


]

Fortinet FortiGate 200F provided 5.4 times better malware protection than competing product tested with the KeySight BreakingPoint system. Of the 1,500 malicious samples (strikes) on both vendors' products, Fortinet FortiGate blocked 1,187 samples, while Palo Alto Networks blocked 204 samples. Note with PAN when AI/ML was enabled, we observed 15% block rate. Without AI/ML enabled we observed 14% block rate. For this test we can attribute 1% improvement for the AI/ML for PAN.

5.2 BreakingPoint Ransomware Blocked by Signature Test Results

Ransomware is a malware that prevents you from accessing your device and the data stored on it - usually by encrypting your files. Security is never static. New threats are ever present, and misconfigurations can compromise your network in an instant. By safely simulating the entire kill chain on the production network, we were able to measure the protection provided by both Fortinet and Palo Alto Networks.



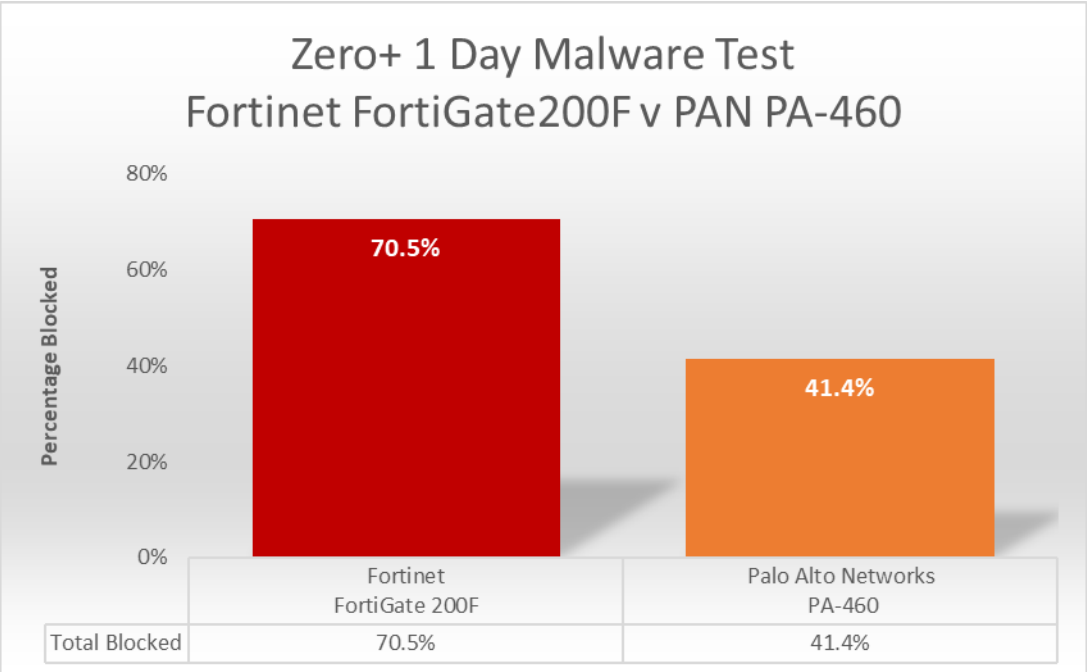
Palo Alto Networks has a "File Block" feature when it blocks all malicious and benign files. It indicates PAN does not have heuristics or signatures for detecting and protecting against malicious files without disrupting the good files flowing in a network daily. Fortinet FortiGate provided 5.4 times better than Palo Alto Networks on blocking ransomware from BreakingPoint. Of the 642 malware samples (or strikes) on both vendors' products, Fortinet FortiGate blocked 541 samples, while Palo Alto Networks blocked 0 samples.

6.0 Miercom Advanced Offensive Security Suite (AOST) Tests

In modern SOC operations, it's vital for security teams to measure both mean time to detect (MTTD) and mean time to resolve (MTTR). Many security vendors claim the application of AI/ML technologies to enhance efficacy and provide real-time protection against signature-based, polymorphic, and zero-day malware. It's essential to know MTTD and MTTR statistics when it comes to detected malware and zero-days threats.

Miercom uses the Advanced Offensive Security Suite (AOST) to assess security products for their malware detection and data loss prevention techniques for real-world scenarios. Our comprehensive testing process replicates a real network environment, with controlled, induced replicated catastrophic breach events. Miercom AOST consists of zero day malware samples collected from honeypots from locations around the world. Miercom also has custom vulnerability and attack scripts for conducting white hat penetration testing.

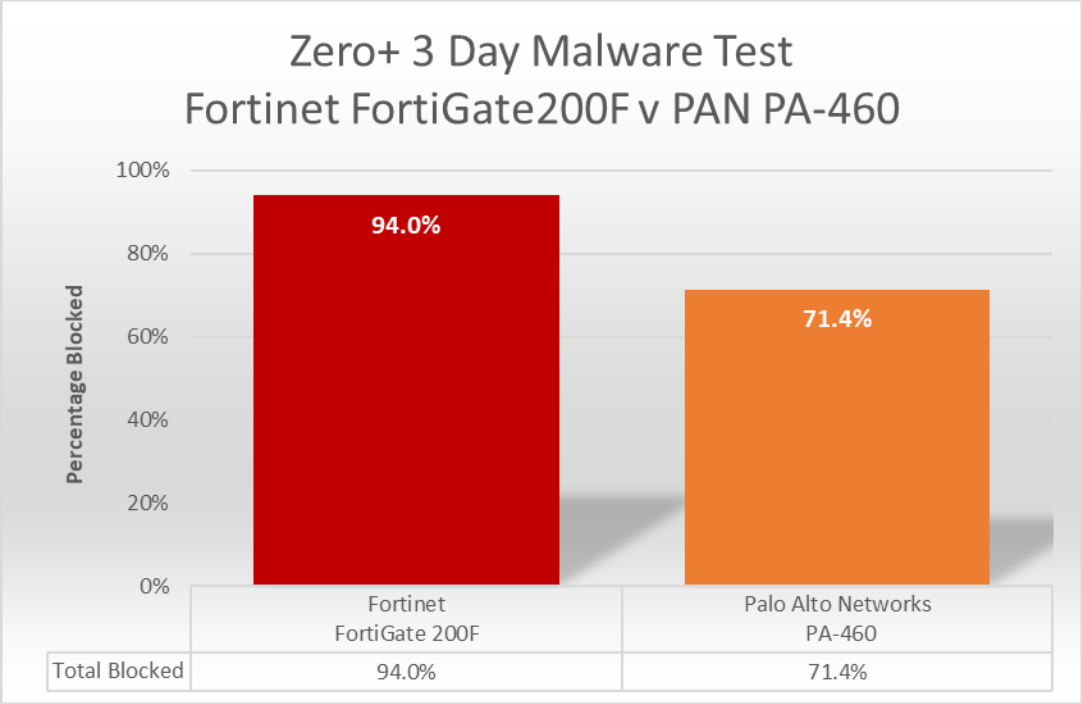
6.1 Zero+1 Day Malware Test Results



Miercom evaluated the Fortinet FortiGate and the Palo Alto Networks NGFW for blocking Zero+1 Day Malware. PAN AI/ML for all the ransomware malware testing. Fortinet FortiGate provided 1.7 times better protection than Palo Alto Networks on blocking the Miercom AOST malware set.

The next test shows the results of malware and zero-day on the FortiGate and PAN NGFW appliances on days one and three - showing the results for day 1 for real-time protection. On day 3, we encountered something new where the threat lab and AI/ML needed additional time to identify malware. The next test also shows what was either missed entirely, or would cost time or issues on the appliance – given the threat labs capabilities.

6.2 Zero+3 Day Malware Test Results



Miercom tested the Fortinet FortiGate and the Palo Alto Networks NGFW for blocking Zero+3 Day Malware. Fortinet FortiGate performed 1.3 times better than Palo Alto Networks on blocking the Miercom AOST Z+3 Day malware set.

7.0 About the FortiGuard Labs and FortiGuard Security Services on FortiGate

Security is not a product. Enabling a feature does not provide 100% protection. It is important to know that security protection is a process.

7.1 Fortinet FortiGuard Labs

What sets apart the FortiGuard Labs team? Three key differentiators: 1) scale and breadth of visibility into the threat landscape, 2) Innovative use of AI and ML, and 3) rapid delivery of actionable threat intelligence to the Fortinet Security Fabric. Some specifics:

- **Scale** – With more network firewall sensors installed than any other competitor, FortiGuard Labs operates on a massive amount of threat data and telemetry. Over 200-B threat events are seen every day, and 1-B security updates are shared with our customers every day. The FortiGuard Labs threat research team consists over 500 researchers, located across the globe.
- **Quality –** The efficacy of Fortinet solutions are validated over and over through internal and third-party testing. Unlike competitor research teams, FortiGuard Labs is directly involved in the development, enhancement and continual updating of high-quality detection and protection technologies for known and unknown threats.
- **Top notch ML/AI** - FortiGuard Labs has been researching and applying AI/ML methodologies and tools for over ten years. AI and Machine Learning are critical to the real-time proactive protection against known and unknown threats across all our customer network edges, through a single mesh architecture spanning data centers, branches, home offices, campuses and multiple clouds. Many ML and AI models are implemented to support FortiGuard Labs operations and improve performance. FortiGuard Labs' AI/ML research has led to product innovations such as FortiNDR, FortiSandbox and solutions that leverage local and global AI and ML applications.
- **Zero-day research** – The extent of Fortinet's reporting of zero-day threats (discovered vulnerabilities before they become discovered exploits) shows the effectiveness of FortiGuard Labs' research, proactive analysis and applied intelligence. The thousand-plus vulnerabilities FortiGuard Labs has discovered so far has set us apart from our competitors.

Highlights

- Co-founder of Cyber Threat Alliance (CTA) in 2014
- Co-founder of the World Economic Forum's Center for Cybersecurity created in 2018.
- Member of the computer incident response organization FIRST since 2012
- Contributor to the development of STIX/TAXII protocols, as well as the MISP platform. Receives and processes over 200 individual sources of threat intelligence from partners.

7.1.1 FortiGuard Intrusion Prevention

Fortinet's solution combines industry-leading threat intelligence from FortiGuard Labs with the FortiGate NGFW to identify emerging threats and prevent them from entering your network. IPS signatures are one such method for delivering the latest protection. FortiGuard Labs uses AI and Machine Learning (ML) to analyze billions of events every day. FortiGuard Labs also proactively performs threat research to discover new vulnerabilities and exploits, producing signatures to identify such threats. These IPS signatures are delivered to each FortiGate daily, so that the IPS engine is always armed with the latest countermeasures.

7.1.2 FortiGuard AI-based Detection

The AV Engine AI malware detection model integrates into regular AV scanning to enhance detection of potentially malicious Windows Portable Executables (PEs) and mitigate zero-day attacks. Previously, this type of detection was handled by heuristics that analyzed file behavior. With the AV Engine AI package, the module is trained by FortiGuard AV against many malware samples to identify file features that make up the malware. The AV Engine AI package can be downloaded by FortiOS via FortiGuard on devices with an active AV subscription.

7.1.3 FortiGuard Outbreak Prevention

The FortiGuard Virus Outbreak Protection Service (VOS) allows the FortiGate antivirus database to be subsidized with third-party malware hash signatures curated by FortiGuard. The hash signatures are obtained from FortiGuard's Global Threat Intelligence database. The antivirus database queries FortiGuard with the hash of a scanned file. If FortiGuard returns a match, the scanned file is deemed to be malicious.

7.2 About the Fortinet FortiGate NGFW Family

The FortiGate combines AI-powered security and machine learning to deliver Threat Protection at any scale. It allows for deeper visibility into your network and lets you see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks.

Universal ZTNA automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users. Ultra-fast Threat Protection and SSL Inspection provides security at the edge you can see without impacting performance.

Further configuration instructions for each test are provided below in more detail. The Fortinet FortiGate 200F is a next-generation firewall (NGFW) that provides advanced security and networking capabilities for small to medium-sized businesses. It is designed to protect against a wide range of cyber threats, including malware, viruses, and hacking attempts. Some key features of the FortiGate 200F include:

- Network security: The FortiGate 200F provides numerous security features, such as antivirus, intrusion prevention, and web filtering, to protect against network-based threats. It also supports virtual private network (VPN) technologies for secure remote access.
- Network connectivity: The FortiGate 200F supports a wide range of networking protocols and technologies, along with support for 10G SFP+, 1G SFP, and high density 1G RJ45, It also has advanced routing capabilities to help optimize network traffic.
- Management and reporting: The FortiGate 200F include a user-friendly management interface that allows administrators to easily configure and manage the firewall. It also provides various reporting and analytics tools to help administrators monitor and troubleshoot network issues.
- High availability and redundancy: The FortiGate 200F is designed for high availability and can be configured in a cluster or in a high availability (HA) pair to ensure that the firewall remains online and operational.

- Virtual Domain: help support multiple admins in separate access and uses of security policies and domains.

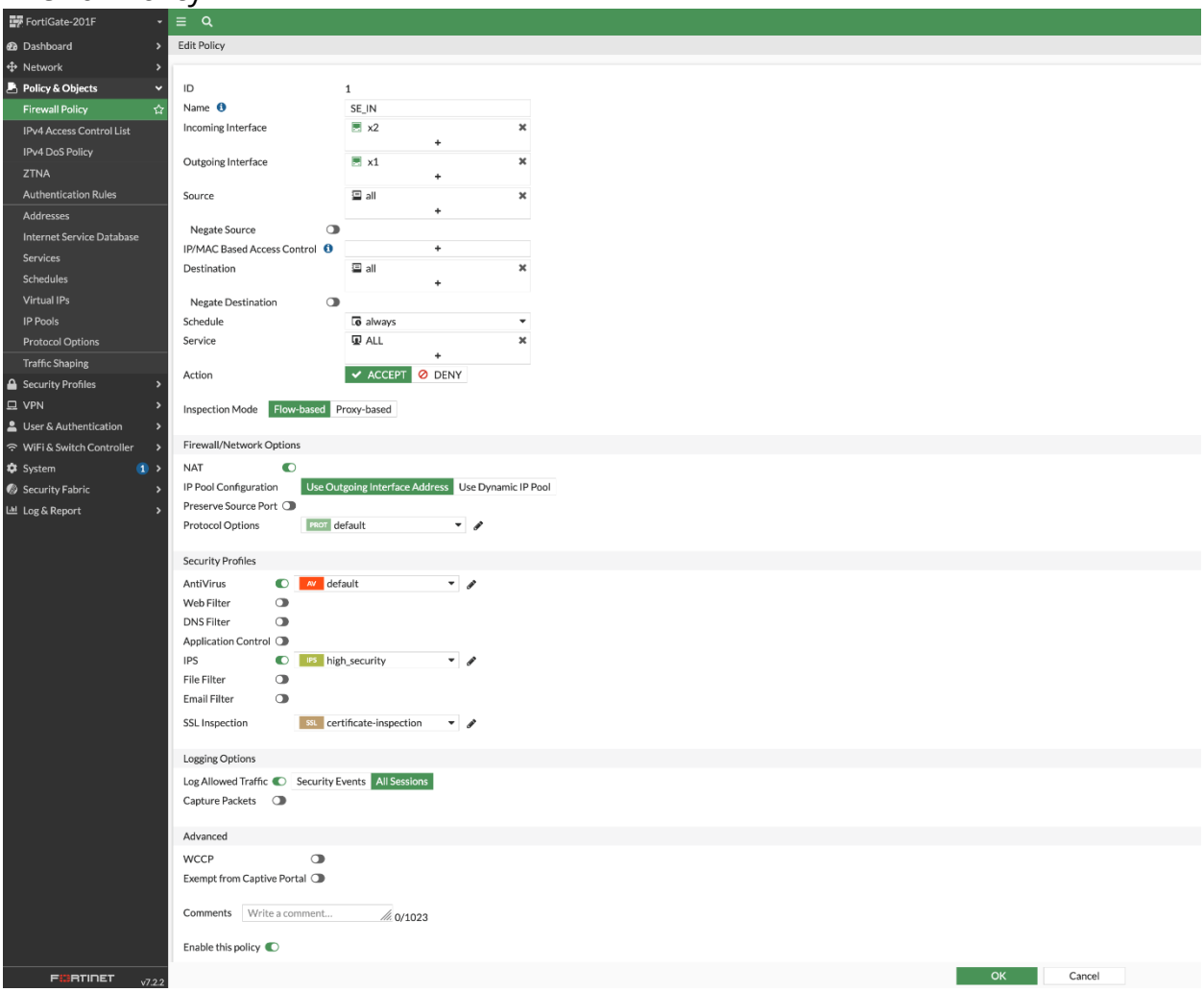
To configure the FortiGate 200F, you will need to access the web-based management interface and follow the steps provided in the product documentation. The exact configuration steps will depend on your specific networking and security needs.
https://www.fortinet.com/fortiguard/labs

8.0 Device Under Test Configuration

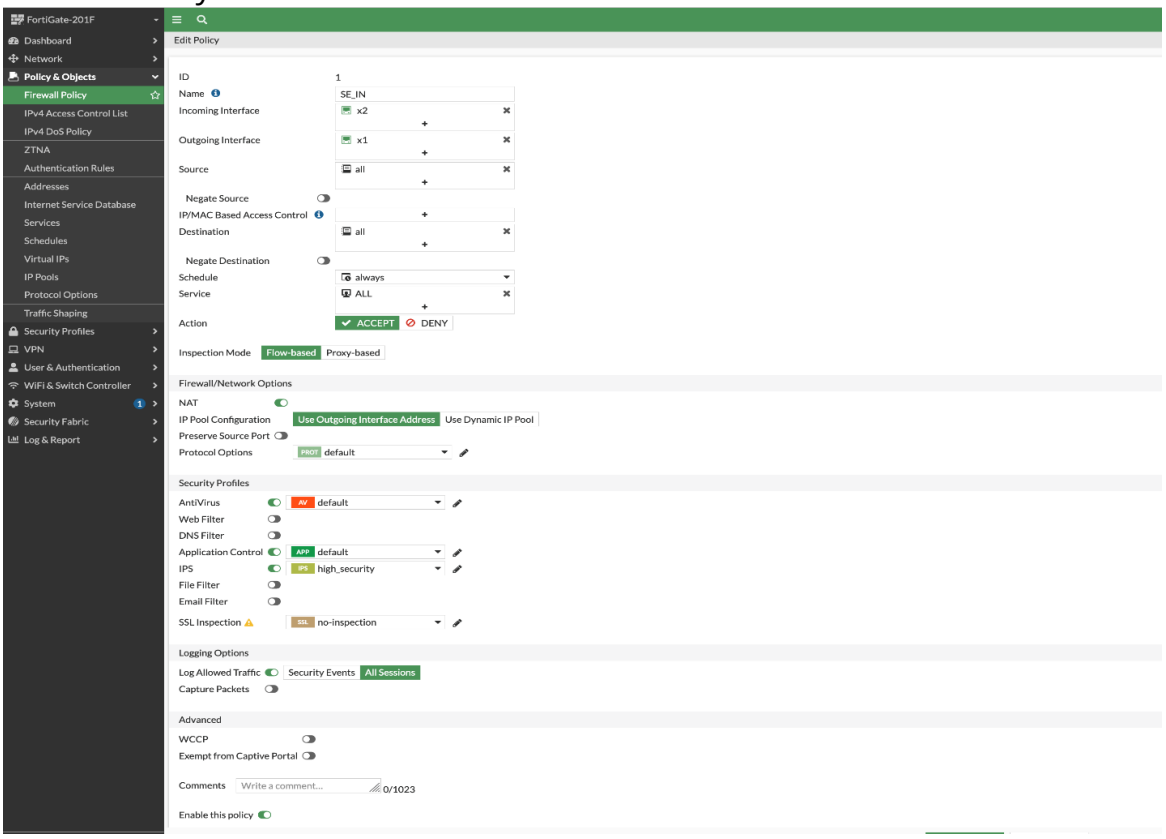
For transparency and the ability to obtain the same test results, BreakingPoint, FortiGate, and Palo Alto Networks NGFW configurations are provided.

8.0.1 Fortinet FortiGate BreakingPoint Ransomware and Malware Test Configuration

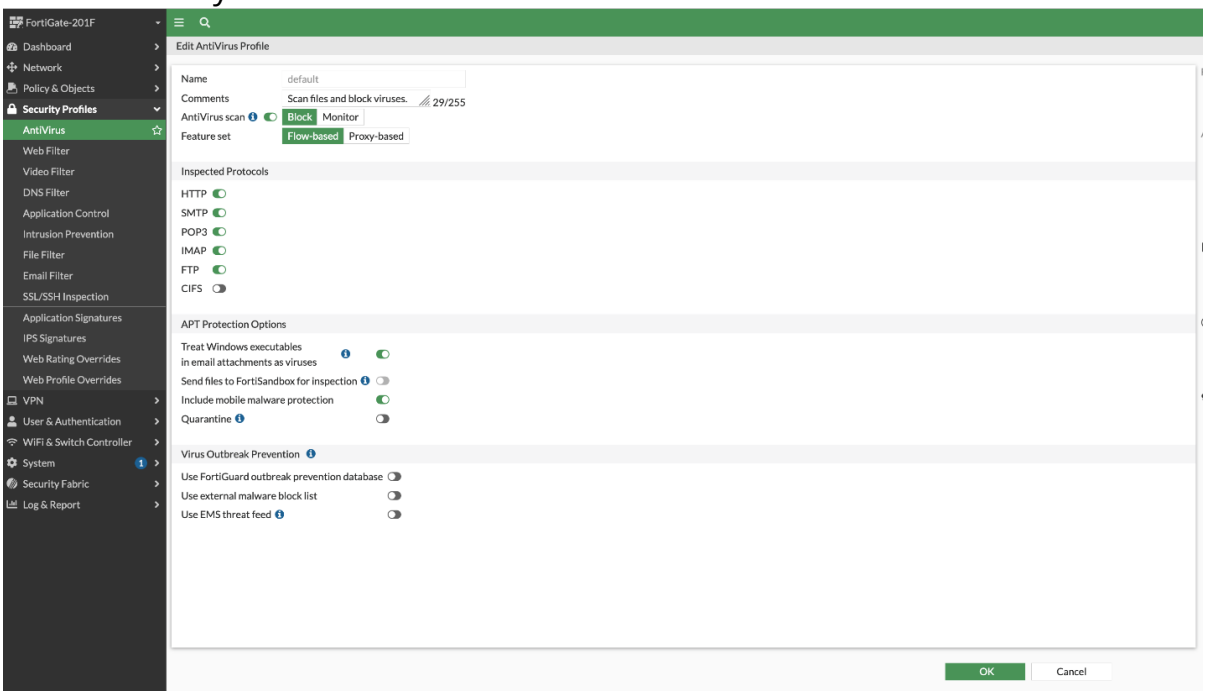
Firewall Policy #1



Firewall Policy #2

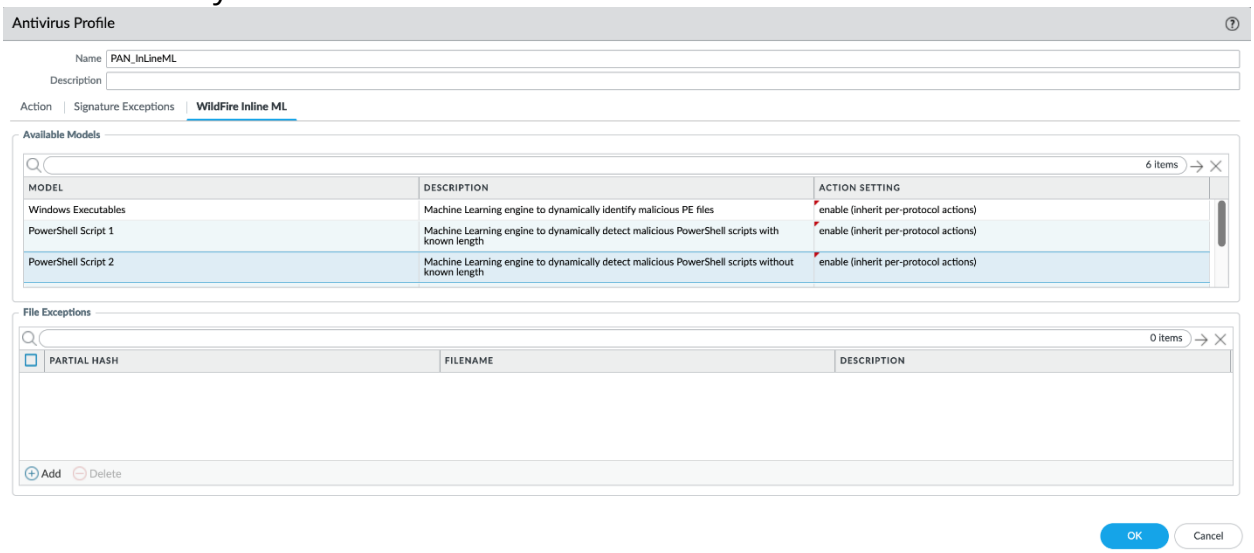


Antivirus Policy #1

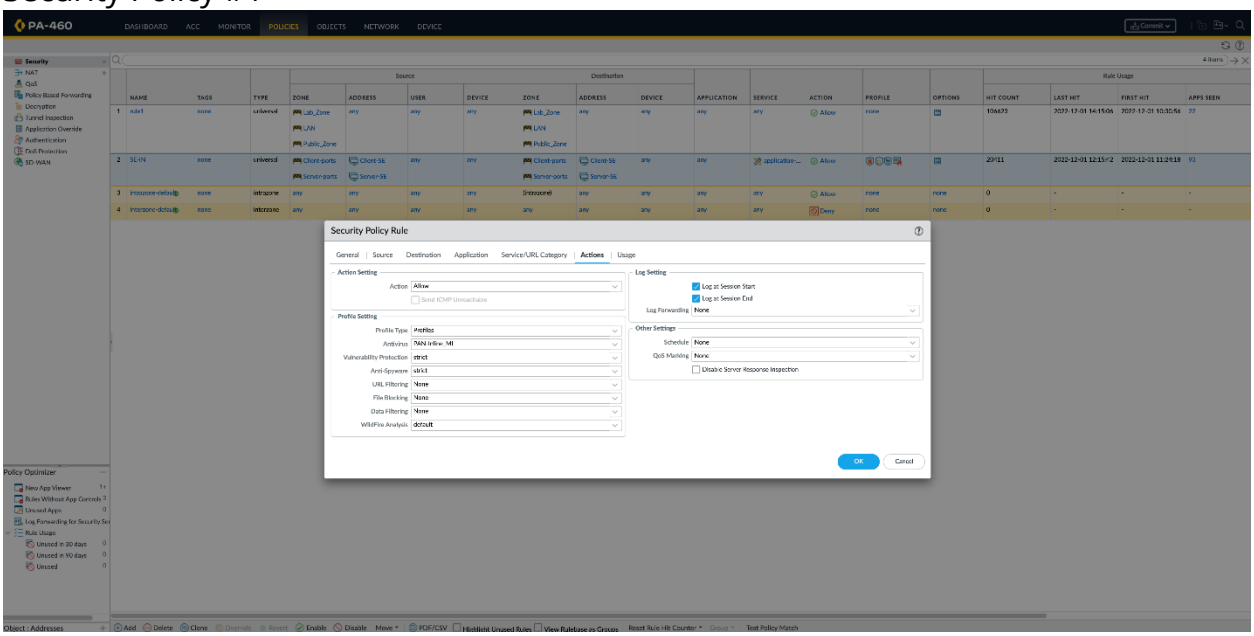


8.0.2 Palo Alto Networks BreakingPoint Ransomware and Malware Test Configuration

Antivirus Policy #1



Security Policy #1



9.0 About Miercom

Miercom 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. Additionally, Miercom services 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.

9.1 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. 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 that may be confusing, misleading, or deceptive or in a manner that disparages us or our information, projects, or developments.

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.