Miercom

April 2023
DR230115E

FORTINET

Fortinet FortiGate 200F v. Palo Alto Networks PA-460 NGFW
Competitive Performance Assessment

Table of Contents

1.0 Executive Summary 4

1.1 Summary of the Benchmarking Results 6

2.0 Introduction 7

2.1 Scope of Evaluation 7

2.2 Products Tested 8

3.0 How We Did It 9

3.1 Products Evaluated 10

4.0 NGFW Performance Test 44K & 16K Payload 10

4.1 NGFW Performance Testing: Firewall and IPS 11

5.0 NGFW Performance Testing: Threat Protection 12

5.1 NGFW Performance Testing: Threat Protection (FW + IPS + AV + App Ctrl) 12

6.0 TLS Decryption 13

6.1 TLS 1.2 Decryption Throughput Test 13

6.2 TLS 1.2 Decryption Throughput Test Results 14

6.3 TLS 1.3 Decryption Throughput Test 14

6.4 TLS 1.3 Decryption Throughput Test Results 15

7.0 About the Fortinet FortiGate 16

8.0 Device Under Test Configuration 17

8.1 Fortinet FortiGate 200F Firewall & IPS Configuration 17

8.2 Palo Alto Networks PA-460 Firewall & IPS Configuration 20

8.3 Fortinet FortiGate 200F Threat Protection Configuration 21

8.4 Palo Alto Networks PA-460 Threat Protection Configuration 21

8.5 Fortinet FortiGate 200F SSL Decryption for TLS 1.2 Decryption Configuration 22

8.6 Palo Alto Networks PA-460 SSL Decryption for TLS 1.2 Decryption Configuration 23

8.7 Fortinet FortiGate 200F SSL Decryption for TLS 1.3 Decryption Configuration 25

8.8 Palo Alto Networks PA-460 SSL Decryption for TLS 1.3 Decryption Configuration 26

9.0 Product HW and OS Specifications 28

10.0 Total Cost of Ownership Summary 29

10.1 FortiGate 1 Year 29

Copyright ©2023 Miercom

10.2 FortiGate 3 Year 29
10.3 FortiGate 5 Year 30
10.4 Palo Alto Networks 1 Year 30
10.5 Palo Alto Networks 3 Year 31
10.6 Palo Alto Networks 5 Year 32
11.0 Comparative Price/ Protected Mbps 32
11.1 Comparative Price/ Protected Mbps, 1 Year 32
11.2 Comparative Price/ Protected Mbps, 3 Years 33
11.3 Comparative Price/ Protected Mbps, 5 Years 33
12.0 About Miercom 34
12.1 Use of This Report 34

Copyright ©2023 Miercom

1.0 Executive Summary

Fortinet commissioned Miercom to conduct a Next Generation Firewall (NGFW) test. Competitive firewall testing is a process of evaluating and comparing the effectiveness of firewall products from different vendors. We tested the latest NGFW products from Fortinet and Palo Alto Networks. These include the Fortinet FortiGate 200F and the Palo Alto Networks PA-460. These tests help to determine the vendors' ability to protect against various cyber threats, such as malware, viruses, and hacking attempts.

The results of these tests are then used to compare the performance of different firewall products and to determine which vendor's product is the most effective in detecting threats. We found Fortinet FortiGate 200F outperformed Palo Alto Networks PA-460 on all competitive performance metrics. Firewall testing helps organizations choose the best solution for their needs by providing unbiased, objective data on the performance of competing products. It also helps vendors improve the effectiveness of their firewall solutions by providing them with feedback in areas needing improvement.

Independent Testing Key Findings

- **Superior Performance:** Fortinet FortiGate 200F outperformed Palo Alto Networks PA-460 by an average of 1.7 better on all on NGFW competitive performance tests conducted.
- **Best SSL/TLS Performance:** Fortinet FortiGate 200F outperformed Palo Alto Networks PA-460 by an average of 1.8 better on all SSL/TLS Tests
- **Lower TCP Response Time:** Fortinet FortiGate 200F proved to have a shorter TCP response time than the Palo Alto Networks PA-460, which is desirable because it indicates efficient data transmission and stable device connections.
- **Superior Price and TCO:** Fortinet FortiGate 200F is 68% the cost of the Palo Alto Solution for 1-year TCO and 62% the cost for 5-year TCO.

Copyright ©2023 Miercom

Based on our observations, the Fortinet FortiGate 200F Next-Generation Firewall proved superior when tested in real-world network scenarios with full Threat Prevention security features and malware sandboxing enabled. This Next-Generation Firewall (NGFW) offered superior performance to its competition making it a valuable investment for any network administrator looking to boost security. We proudly present Fortinet the ***Miercom Performance Verified Certification*** in recognition of superior competitive performance and exceptional value.

Robert Smithers
CEO, Miercom

Copyright ©2023 Miercom

1.1 Summary of the Benchmarking Results

		FortiGate 200F	PA-460
Performance (Mbps)	NGFW Performance Testing: Firewall and IPS, 44K Payload (Mbps)	2,864	1,280
	NGFW Performance Testing: Firewall and IPS, 16K Payload (Mbps)	1,838	818
	NGFW Performance Testing: Threat Protection (FW + IPS +AV + App Ctrl), 44K (Mbps)	1,700	1,350
	NGFW Performance Testing: Threat Protection (FW + IPS +AV + App Ctrl), 16K (Mbps)	925	825
	TLS 1.2 Decryption Throughput, 44K (Mbps)	525	300
	TLS 1.2 Decryption Throughput, 16K (Mbps)	290	155
	TLS 1.3 Decryption Throughput, 44K (Mbps)	725	435
	TLS 1.3 Decryption Throughput, 16K (Mbps)	325	200

	FortiGate 200F	PA-460
TCO	with 10 Virtual Domain, Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium), 1 Year, includes SD-WAN	second external power supply, and rack mount, Virtual Systems (1 to 5) plus Advanced Threat Prevention, Advanced WildFire, Advanced URL, DNS Security, SD-WAN, Premium Support
1 Year	$9,424	$13,850
3 Years	$17,186	$26,865
5 Years	$24,948	$40,460

TCO Information above is based on open-source research, Miercom cannot guarantee the accuracy of pricing details from vendor sources.

Copyright ©2023 Miercom

2.0 Introduction

In the industry, NGFW vendors have different metrics and criteria to represent performance specifications on their datasheets. These range through file size, payload, ciphers, capacities, applications, weighted traffic/ flows, and packet size. Some vendors – however - would not publish critical specifications for properly sizing a use case deployment.

Miercom conducted tests on the Fortinet FortiGate 200F and Palo Alto Networks PA-460 NGFWs. They included a series of performance tests with different features enabled/disabled using the same test methodology.

2.1 Scope of Evaluation

Miercom evaluated two Next Generation Firewall products (NGFWs): Fortinet FortiGate 200F and Palo Alto Networks PA-460, using real-world scenarios to compare their performance and the ability to measure any degradation seen from security enablement.

Testing focused on the following:

- Firewall & IPS - HTTP Testing with 44K & 16K payloads
- Threat Protection (FW+IPS+AV+App Ctrl) with 44K & 16K payloads
- SSL/TLS 1.2 - TLS_AES_256_GCM_SHA384 with 2048 key size
- SSL/TLS 1.2 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- SSL/TLS 1.3 - TLS_AES_256_GCM_SHA384 with 2048 key size and 44K & 16K payloads

Copyright ©2023 Miercom

2.2 Products Tested

Fortinet FortiGate 200F

The FortiGate 200F series provides an application-centric, scalable, and secure SD-WAN solution with next generation firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or enterprise branch level. This FortiGate 200F series also protects against cyber threats with system-on-a-chip acceleration and industry leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

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 Firewalls family.

Additional information for the Palo Alto Networks PA-460 series can be found:

Data Sheet:
https://www.paloaltonetworks.com

Copyright ©2023 Miercom

3.0 How We Did It

Keysight BreakingPoint Test System is a network security testing platform designed to help organizations assess the performance and security of their network infrastructure and applications. It allows System Administrators and users to simulate real-world network traffic and security threats, such as 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 the ability to create custom test scenarios, generate high speed traffic, and analyze results in real-time. Engineers examined the throughput performance of Fortinet and the Palo Alto Networks appliances in configurations with security services disabled and again with the services enabled. Testing was intended to measure the effect - if any - that security services enablement would have on the firewalls' 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 network testing appliance delivers increasing loads of TCP traffic to the 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 for optimization of next generation firewalls, IPS and secure web gateways.

Copyright ©2023 Miercom

3.1 Products Evaluated

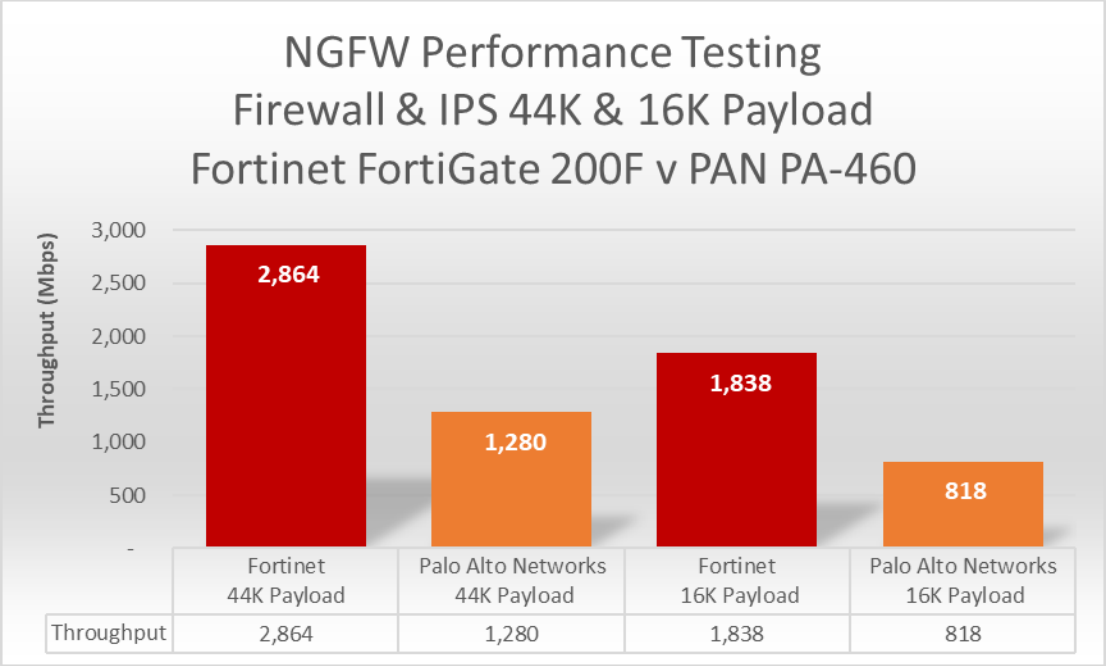
Vendor	Product	Version	Feature
Fortinet	**Fortinet FortiGate 200F** 18 x GE RJ45 (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 4 x 10GE SFP+ slots, NP6XLite and CP9 hardware accelerated, 10 Virtual Domain	7.2.2 build 1255	Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)
Palo Alto Networks	**Palo Alto Networks PA-460** Desktop unit: 8x 1GE, 1 power supply, 1 Virtual System	PAN-OS 10.2.0	Advanced Threat Prevention, Advanced Wildfire, Advanced URL, DNS Security, SD-WAN, Premium Support, 1 Year

4.0 NGFW Performance Test 44K & 16K Payload

Miercom conducted tests on Fortinet FortiGate 200F and Palo Alto Networks PA-460. They were run at 44K and 16K response to test the performance of the network under different load conditions to mimic the characteristics of certain types of network traffic. When running these performance tests, we measured system capability in terms of throughput (i.e., the amount of data that can be processed per second), latency (i.e., the time it takes for a packet to traverse the system), and connection rate (i.e., the number of connections that can be established and maintained simultaneously). The results of this test provide an understanding of the NGFW's ability to handle expected traffic patterns in an enterprise network.

Copyright ©2023 Miercom

4.1 NGFW Performance Testing: Firewall and IPS



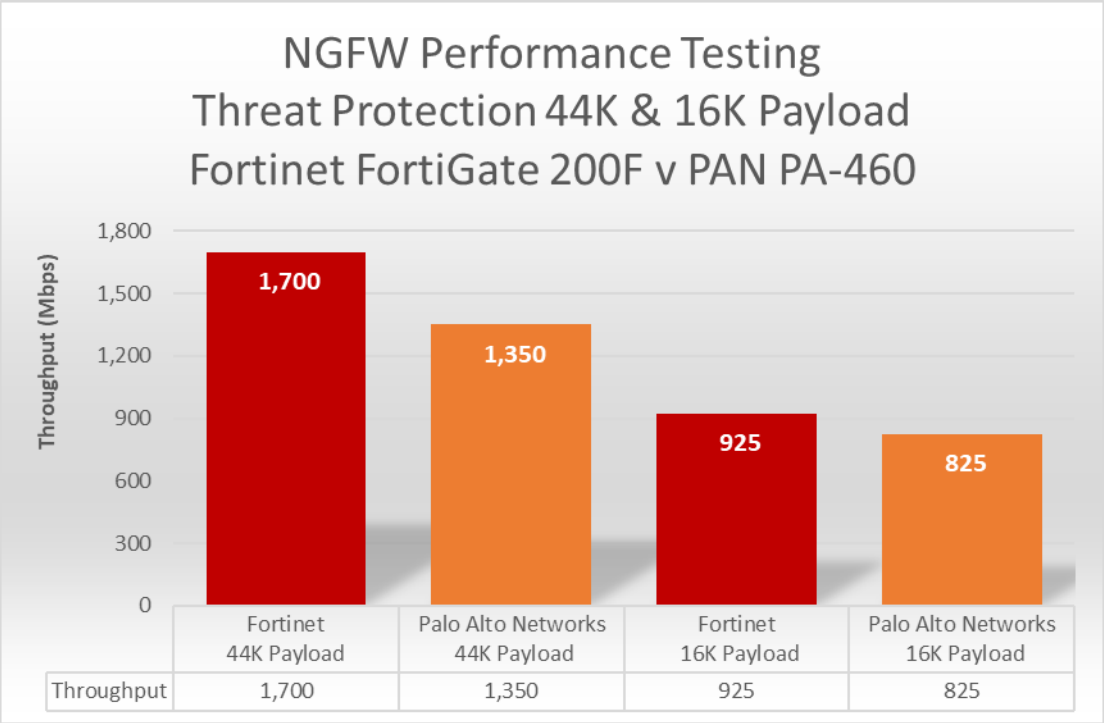
The Fortinet FortiGate 200F provided more than double the throughput than the Palo Alto Networks PA-460 on all tests run with Firewall & IPS enabled. Fortinet proved an average of 224% overall better performance over Palo Alto Networks when testing with 44K 16K payload.

Copyright ©2023 Miercom

5.0 NGFW Performance Testing: Threat Protection

Threat protection refers to the various technologies and measures that are used to secure a network or system against potential security threats. For these tests we included the following Threat Protection technologies: Firewalls, Intrusion Prevention Systems (IPS), Antivirus Software and Application Control Systems.

5.1 NGFW Performance Testing: Threat Protection (FW + IPS + AV + App Ctrl)



The Fortinet FortiGate 200F provided 1.2 times better throughput than the Palo Alto Networks PA-460 on all tests run with Threat Protection enabled. Fortinet proved an average of 119% overall better performance over Palo Alto Networks when testing 44K & 16K Payload.

Copyright ©2023 Miercom

6.0 TLS Decryption

6.1 TLS 1.2 Decryption Throughput Test

Transport Layer Security (TLS) encrypts data sent over the Internet to ensure that eavesdroppers and hackers are unable to see what you transmit which is particularly useful for private and sensitive information like passwords, credit card numbers, and personal correspondence.

Google estimates that 95 percent of its internet traffic uses the encrypted HTTPS protocol, and most industry analysts conclude that between 80-90 percent of network traffic is encrypted.

Fortinet has a partnership with Google Chrome to provide security innovation to support HTTP3/QUIC deep SSL Inspection. It provides security scanning for this protocol with decryption. Fortinet has this feature, while Palo Alto did not at the time of this test.

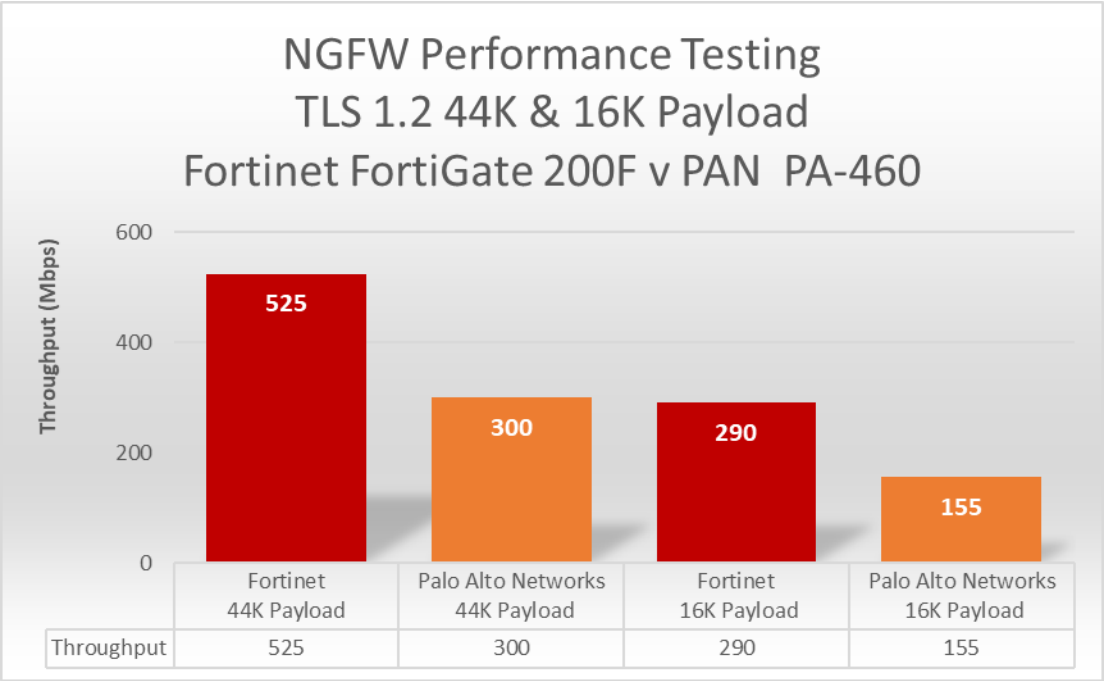
TLS 1.2 decryption performance is an important part of selecting a security solution, as it can impact the overall performance and scalability of the system. Fortinet outperformed Palo Alto Networks on all TLS 1.2 decryption throughput tests. These tests include AES_256_GCM_SHA384 with 2048 key size and ECDHE_RSA_WITH_AES_256_GCM_SHA384 at 44K and 16K response. Fortinet FortiGate 200F proved to have a shorter TCP response time, which is desirable because it indicates that data is being transmitted efficiently and connection between the devices is stable.

At 44K response, Fortinet FortiGate 200F had 1,200 CPS (connections per second) during testing compared to Palo Alto Networks PA-460 with 1,000 CPS. At 16K response, Fortinet FortiGate 200F had 1,650 CPS compared to Palo Alto Networks PA-460 at 700 CPS.

Devices or systems under test with higher decryption throughput performance can handle more traffic and decrypt it more quickly, while those with lower decryption throughput performance may be slower or less scalable. This can be particularly critical in high-traffic environments. It is important to carefully consider the decryption throughput performance of a security solution to ensure that it can meet the needs of the specific environment in which it will be used.

Copyright ©2023 Miercom

6.2 TLS 1.2 Decryption Throughput Test Results



The Fortinet FortiGate 200F provided up to 1.8 times better than the Palo Alto Networks PA-460 on all tests run with TLS 1.2 enabled. Fortinet FortiGate 200F proved an average of 181% overall better performance over Palo Alto Networks PA-460 when testing 44K & 16K Throughput.

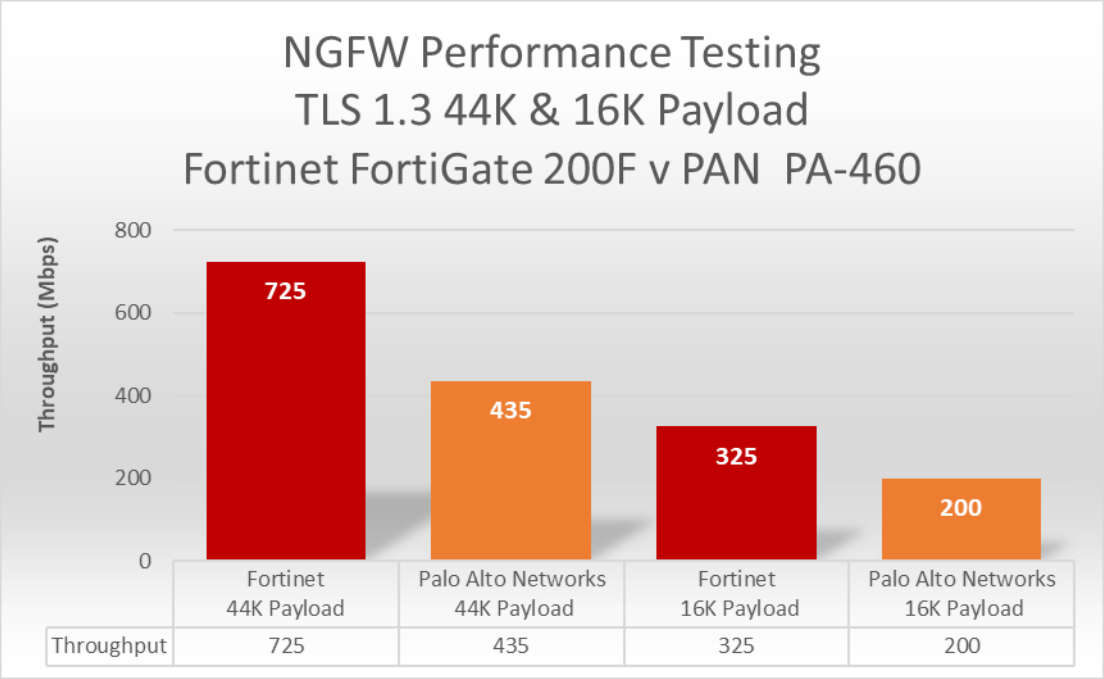
6.3 TLS 1.3 Decryption Throughput Test

Fortinet outperformed Palo Alto Networks on all TLS 1.3 decryption throughput tests on AES_256_GCM_SHA384 with 2048 key size at 44k and 16K response. Higher decryption throughput means that the device or system under test can handle a larger volume of traffic and decrypt it more quickly, which can be particularly important in high-traffic environments. At 44K response, Fortinet FortiGate 200F had 1,600 CPS (connections per second) during testing compared to Palo Alto Networks PA-460 with 1,000 CPS. At 16K response, Fortinet FortiGate 200F had 1,800 CPS compared to Palo Alto Networks PA-460 at 1,100 CPS. Fortinet also proved to have a shorter TCP response time, which is desirable because it indicates that data is being transmitted efficiently and the connection between the devices is stable. It is important to carefully consider the decryption throughput performance of a security solution to ensure that it can meet the needs of the specific environment in which it will be used. TLS 1.3 is expected to provide improved security and performance compared to earlier versions of TLS, due to features such

Copyright ©2023 Miercom

as improved encryption algorithms and the ability to establish secure connections more quickly. However, the actual performance of TLS 1.3 decryption throughput will depend on the specific implementation and hardware being used.

6.4 TLS 1.3 Decryption Throughput Test Results



The Fortinet FortiGate 200F provided 1.6 times better than the Palo Alto Networks PA-460 on all tests run with TLS 1.3 enabled. Fortinet FortiGate 200F proved an average of 165% overall better performance over Palo Alto Networks PA-460 when testing 44K & 16K Throughput.

Note: SSL inspection performance is measured with IPS enable on both FortiGate and Palo Alto.

Copyright ©2023 Miercom

7.0 About the Fortinet FortiGate

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 family 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 are 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.

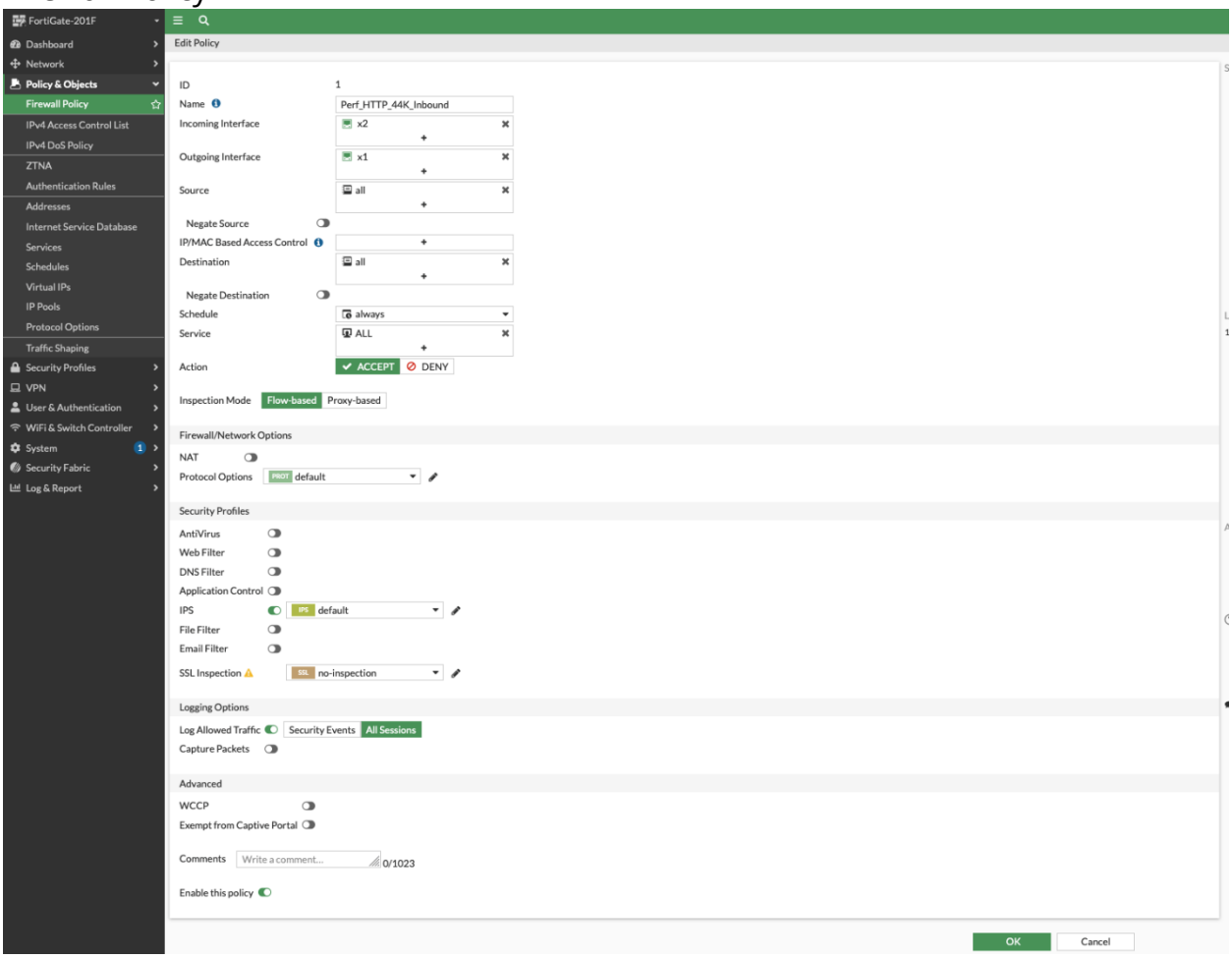
Copyright ©2023 Miercom

8.0 Device Under Test Configuration

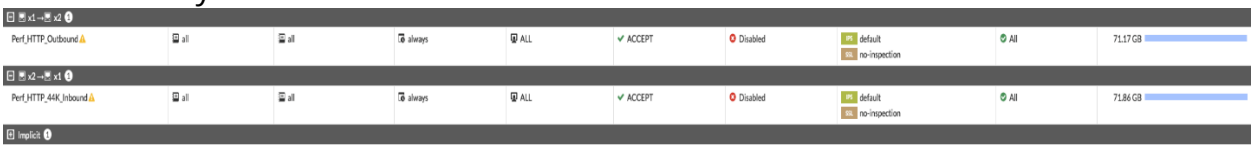
For transparency and the ability to reproduce these test results, the BreakingPoint test system, the FortiGate, and the Palo Alto Networks NGFW configurations are provided below.

8.1 Fortinet FortiGate 200F Firewall & IPS Configuration

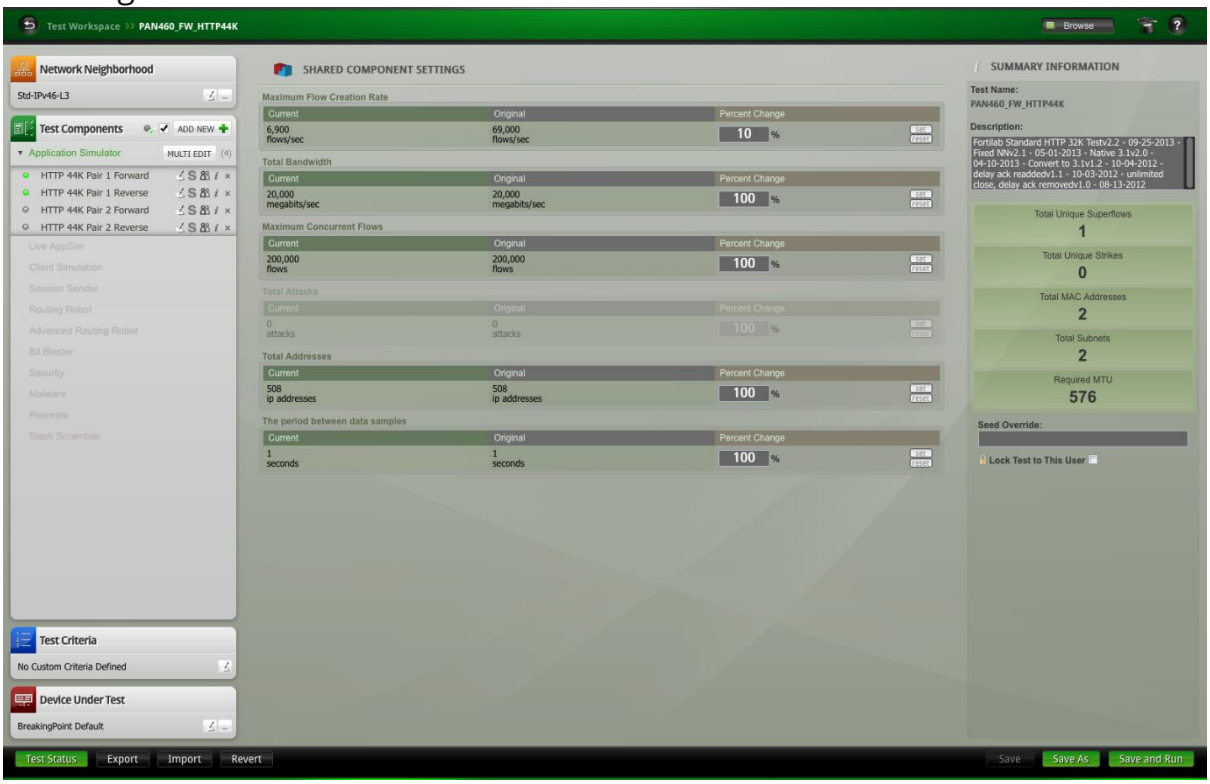
Firewall Policy #1



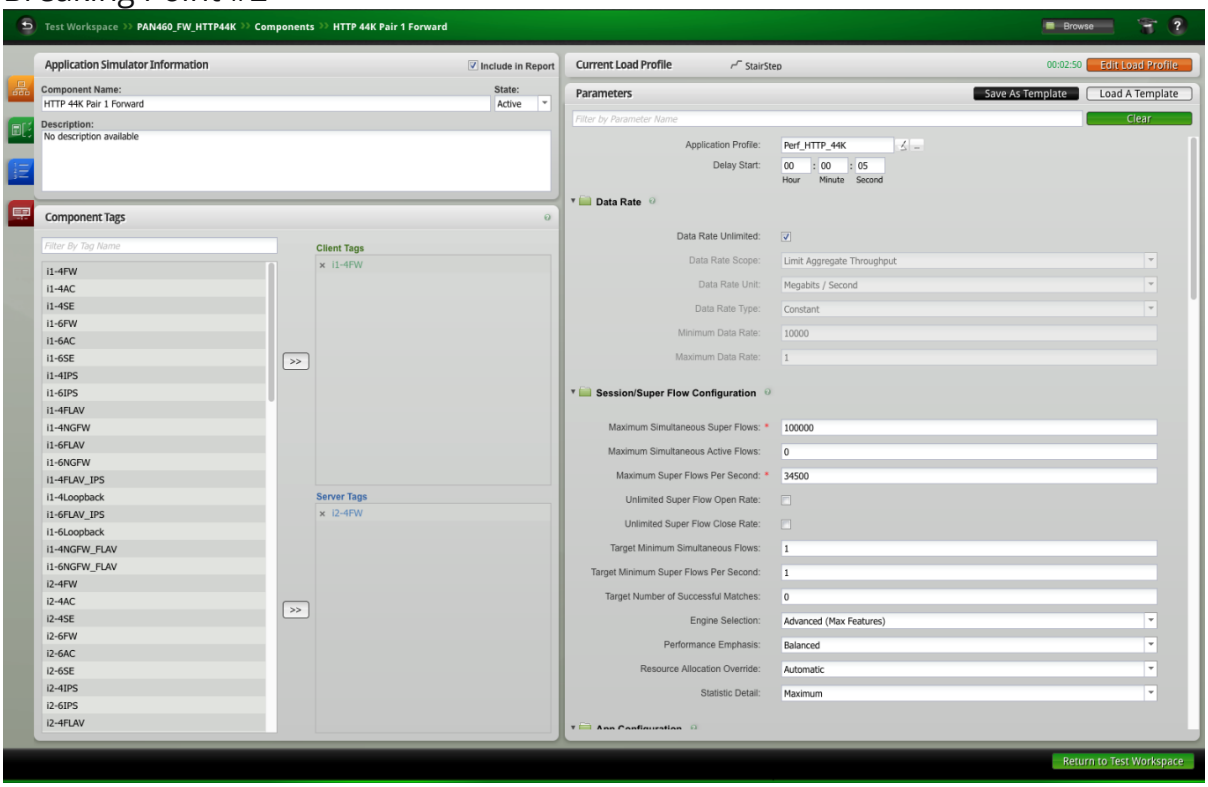
Firewall Policy #2



BreakingPoint Rules #1

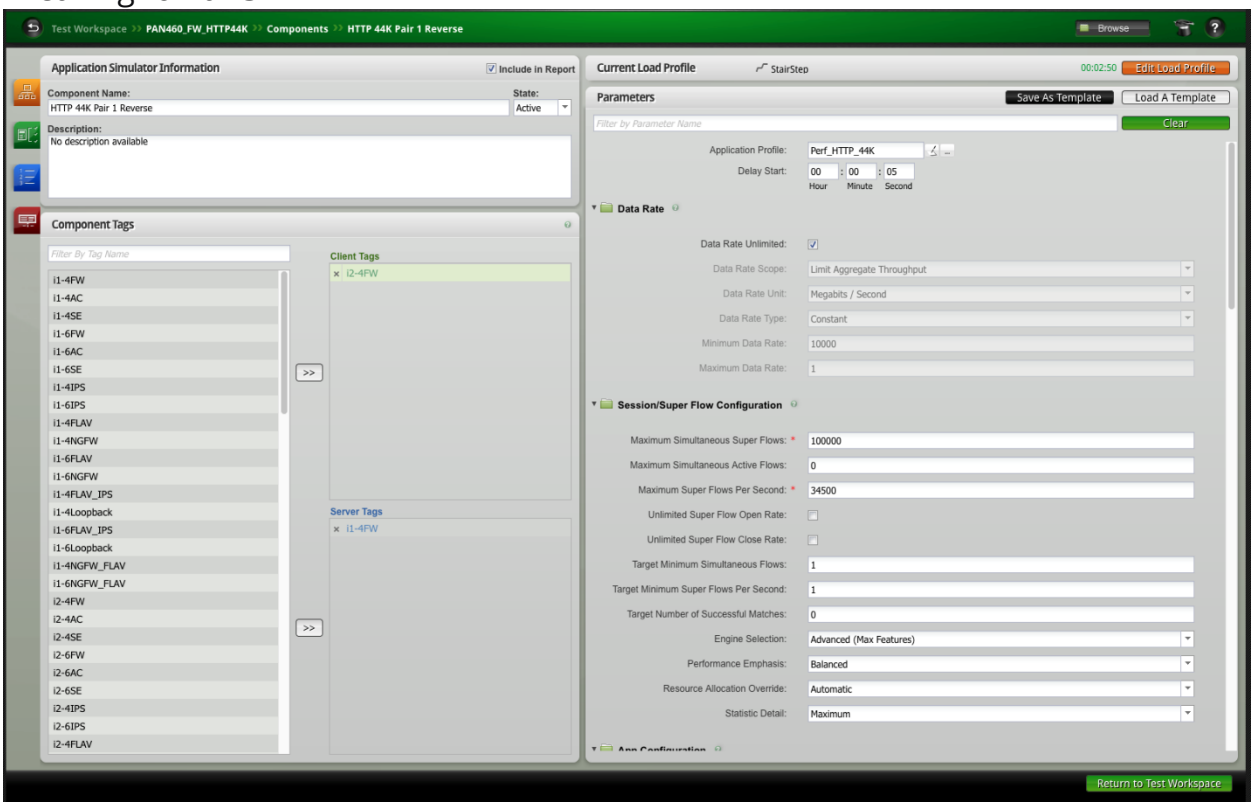


Breaking Point #2



Copyright ©2023 Miercom

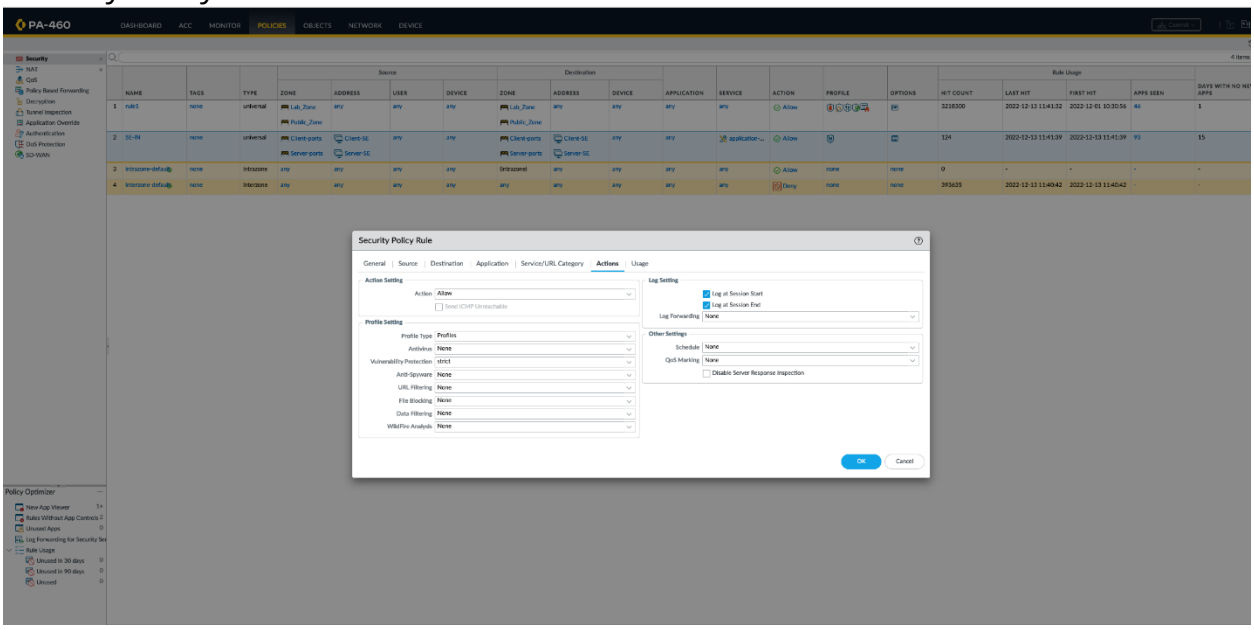
BreakingPoint #3



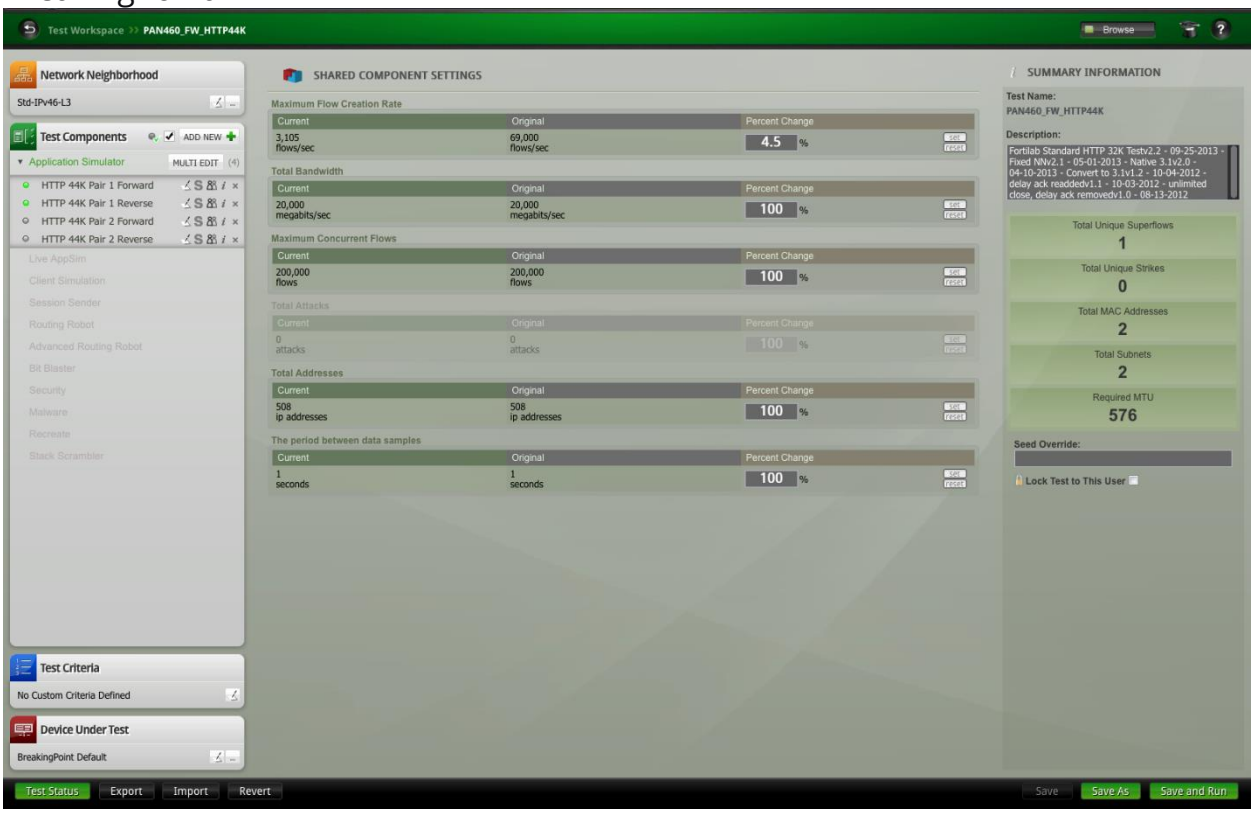
Copyright ©2023 Miercom

8.2 Palo Alto Networks PA-460 Firewall & IPS Configuration

Security Policy #1



BreakingPoint #1



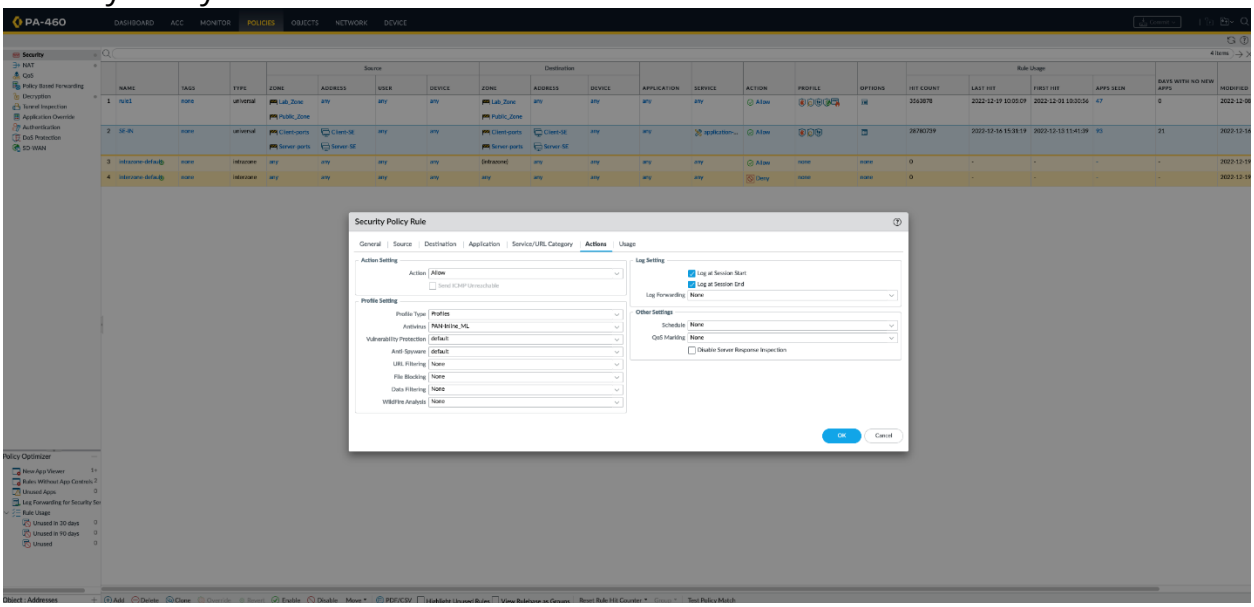
Copyright ©2023 Miercom

8.3 Fortinet FortiGate 200F Threat Protection Configuration

Security Policy #1

8.4 Palo Alto Networks PA-460 Threat Protection Configuration

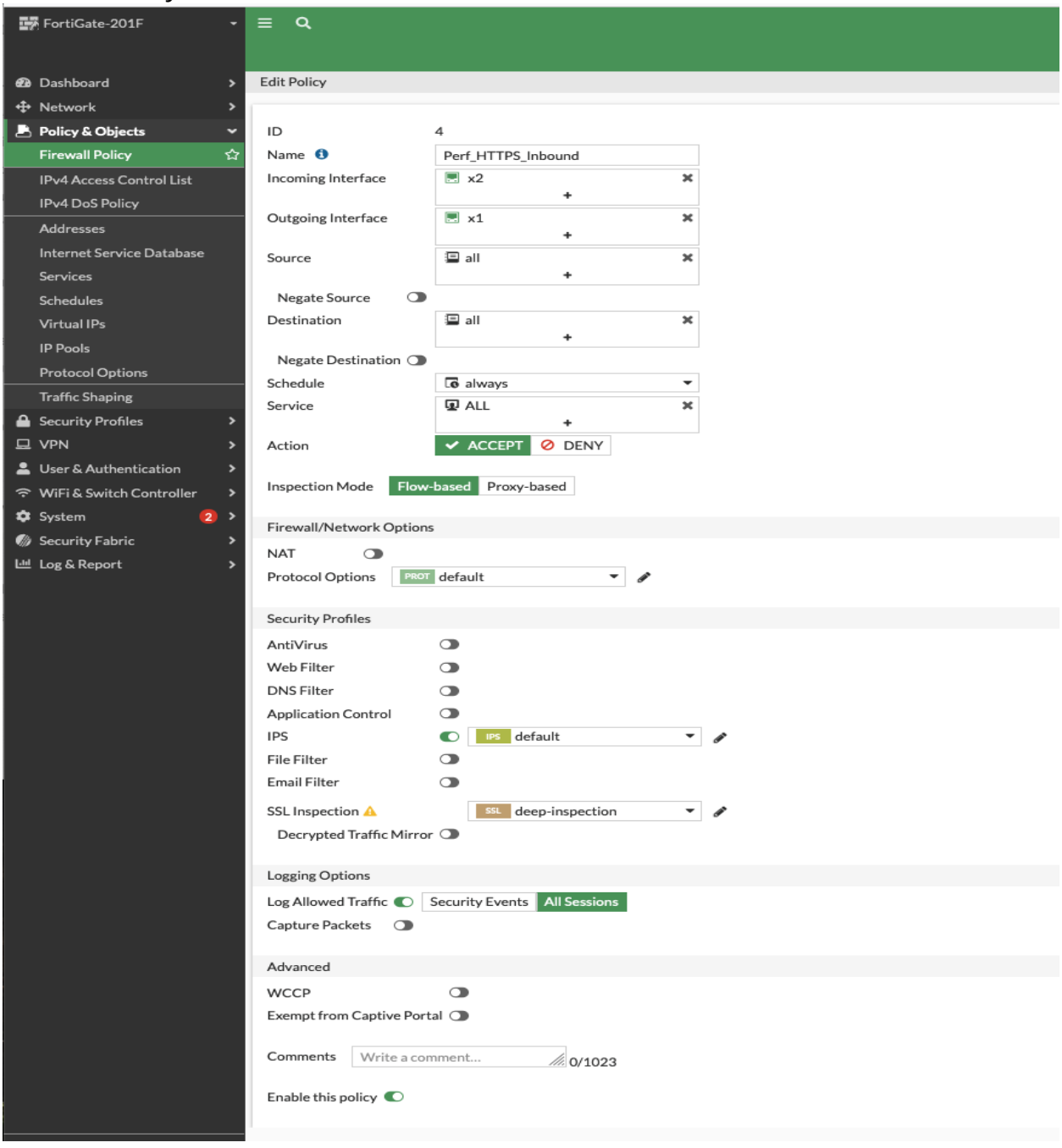
Security Policy #1



Copyright ©2023 Miercom

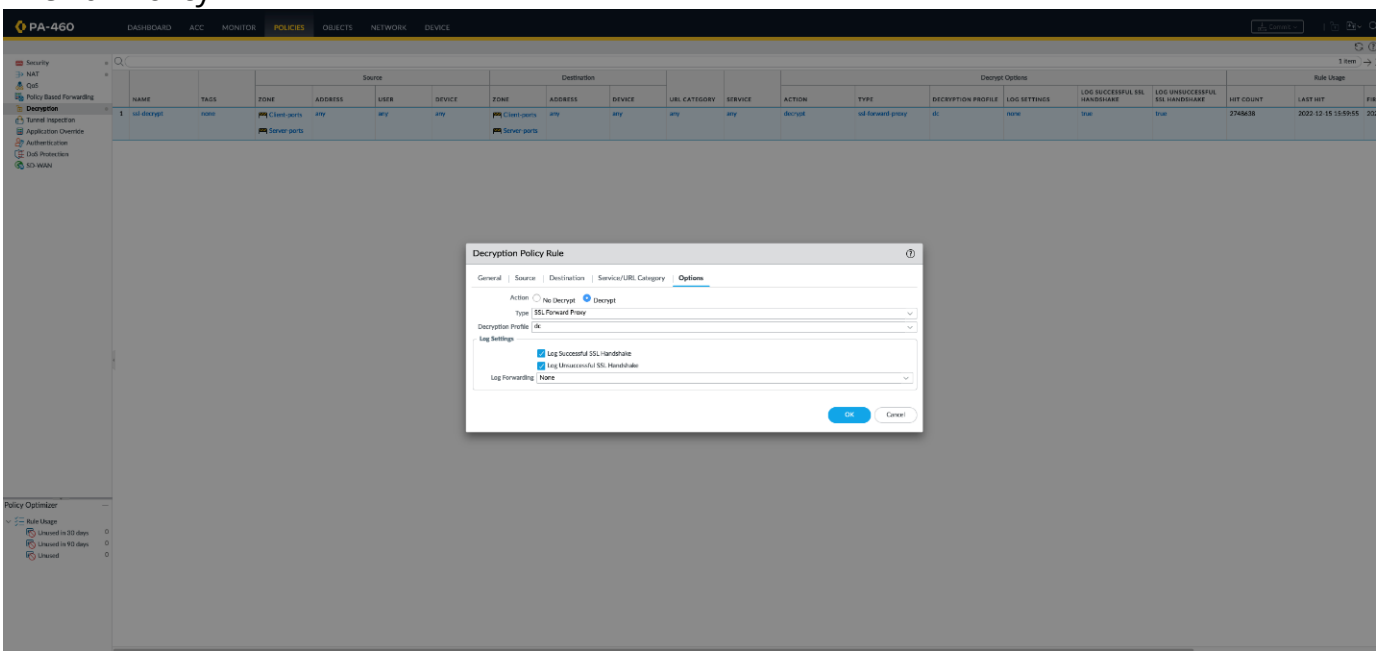
8.5 Fortinet FortiGate 200F SSL Decryption for TLS 1.2 Decryption Configuration

Firewall Policy #1

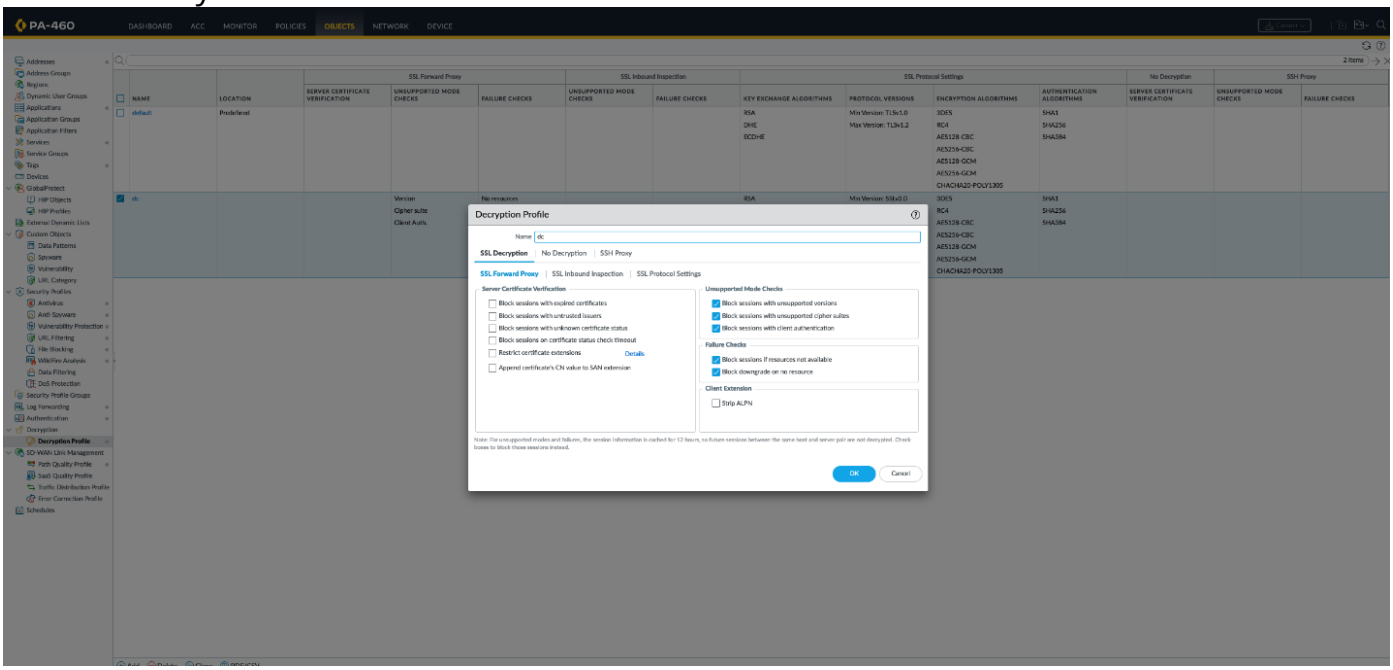


8.6 Palo Alto Networks PA-460 SSL Decryption for TLS 1.2 Decryption Configuration

Firewall Policy #1

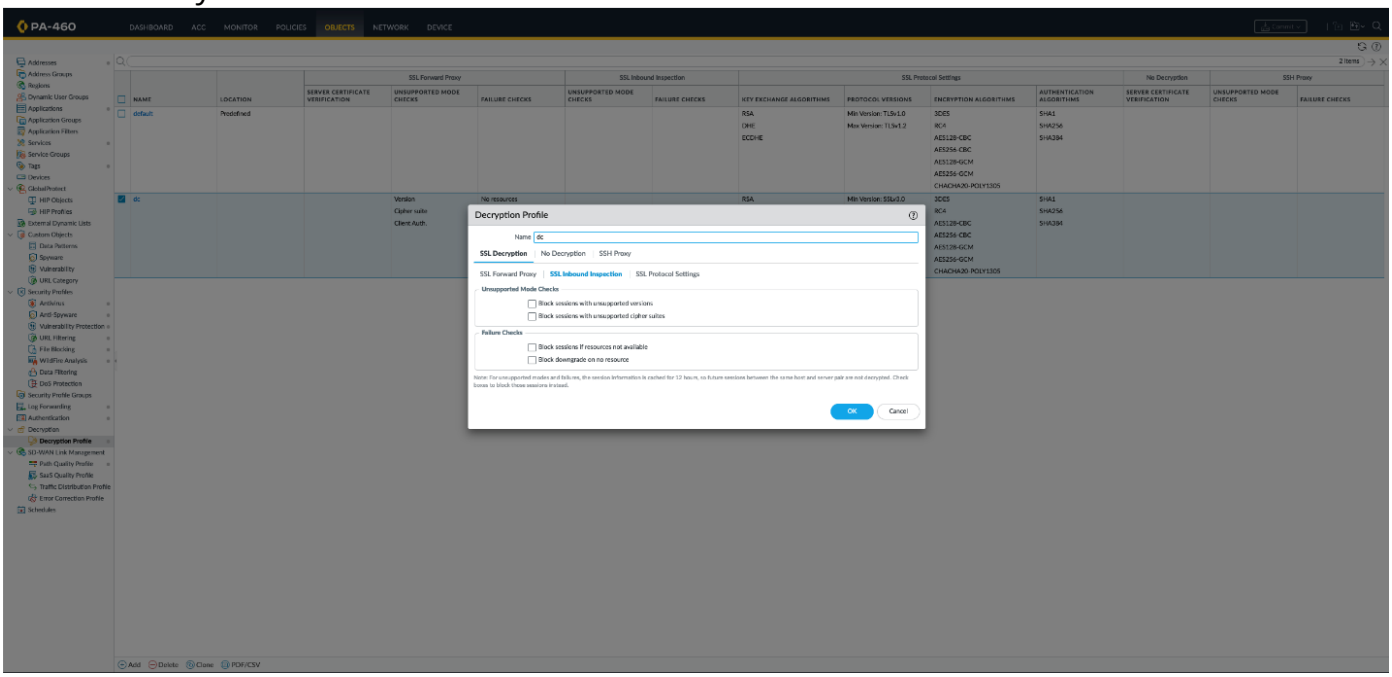


Firewall Policy #2

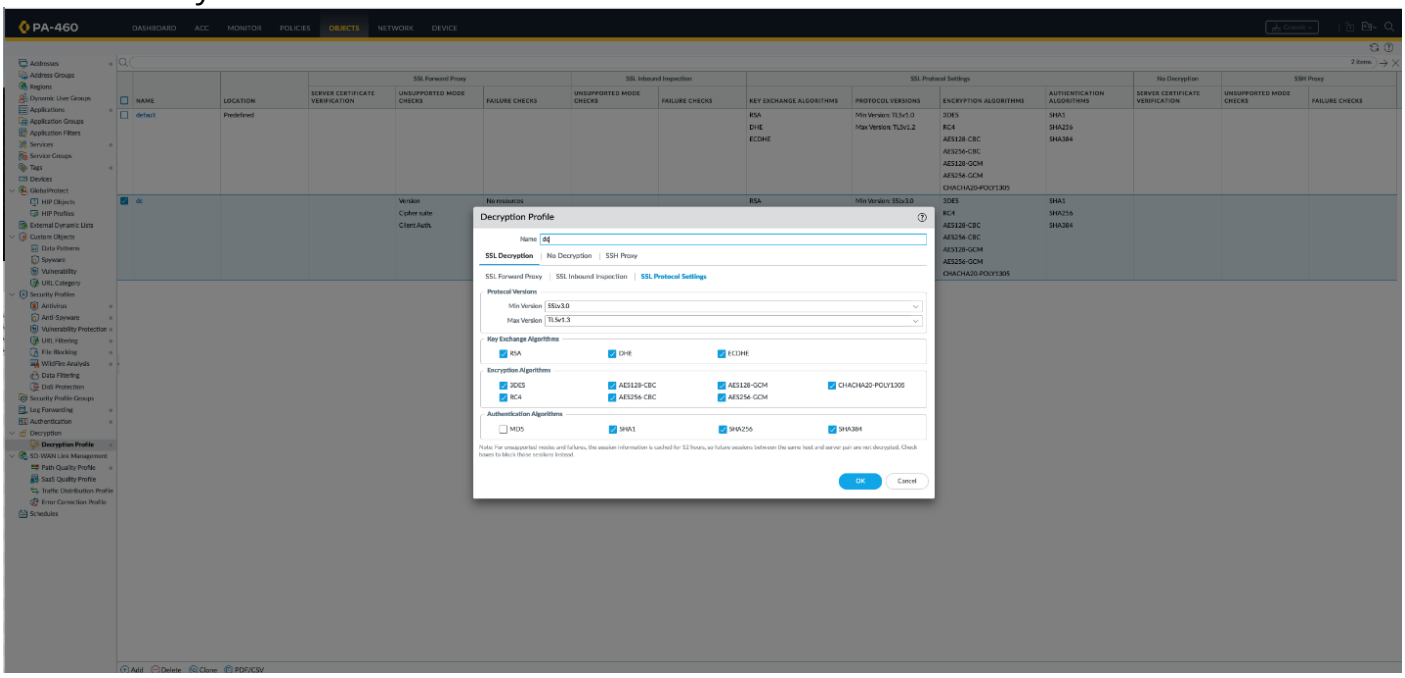


Copyright ©2023 Miercom

Firewall Policy #3



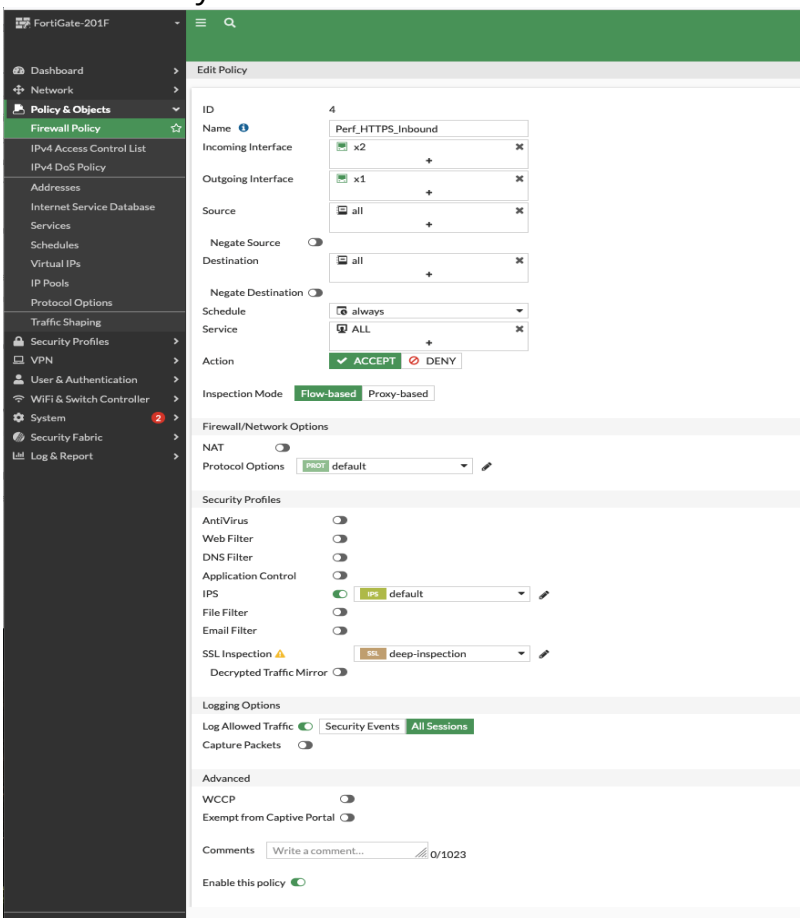
Firewall Policy #4



Copyright ©2023 Miercom

8.7 Fortinet FortiGate 200F SSL Decryption for TLS 1.3 Decryption Configuration

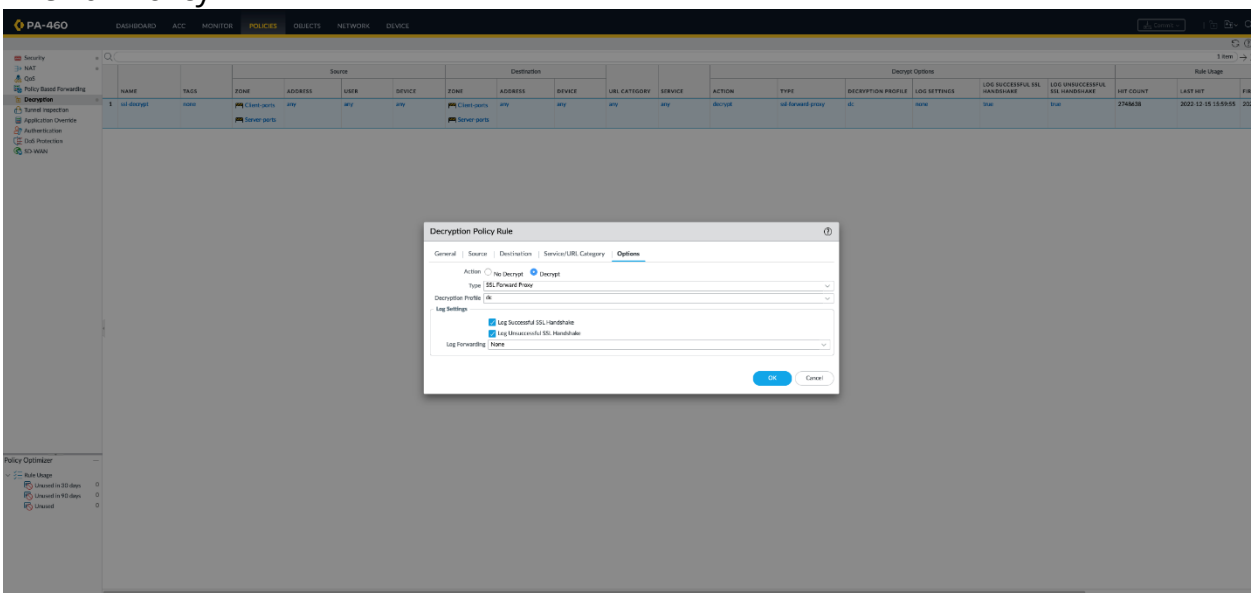
Firewall Policy #1



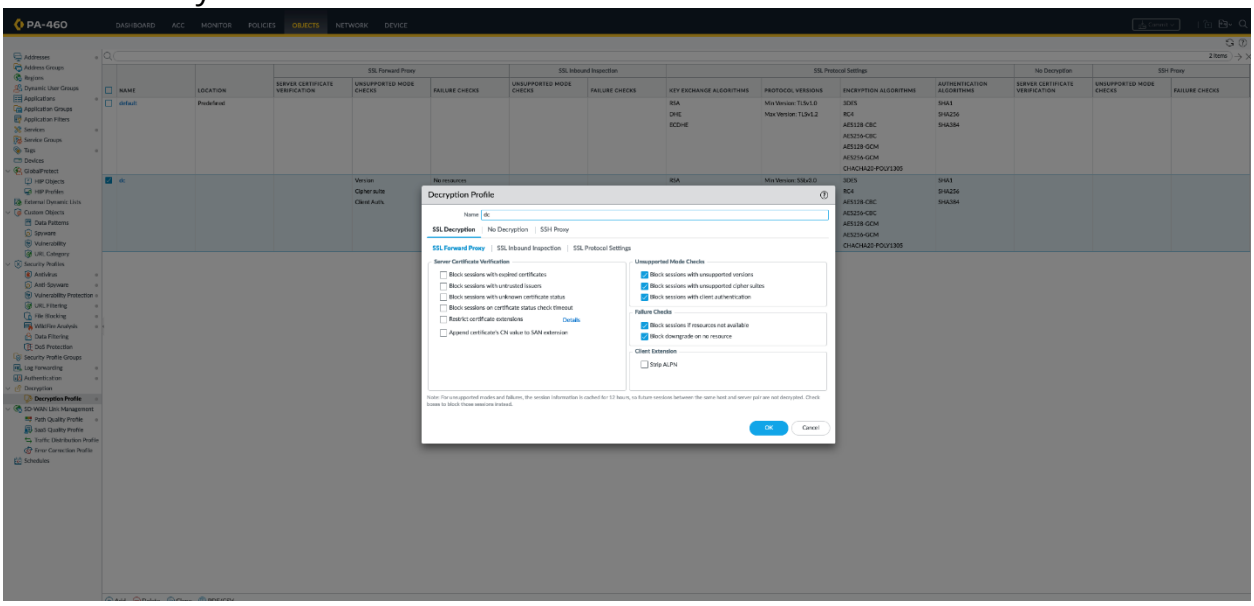
Copyright ©2023 Miercom

8.8 Palo Alto Networks PA-460 SSL Decryption for TLS 1.3 Decryption Configuration

Firewall Policy #1

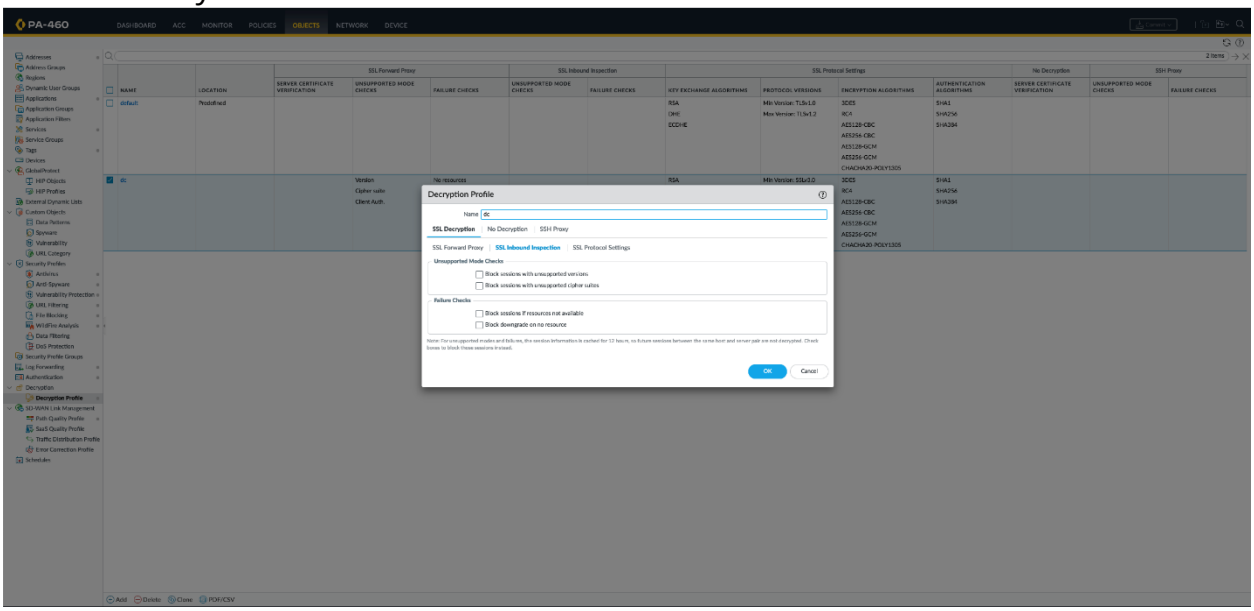


Firewall Policy #2

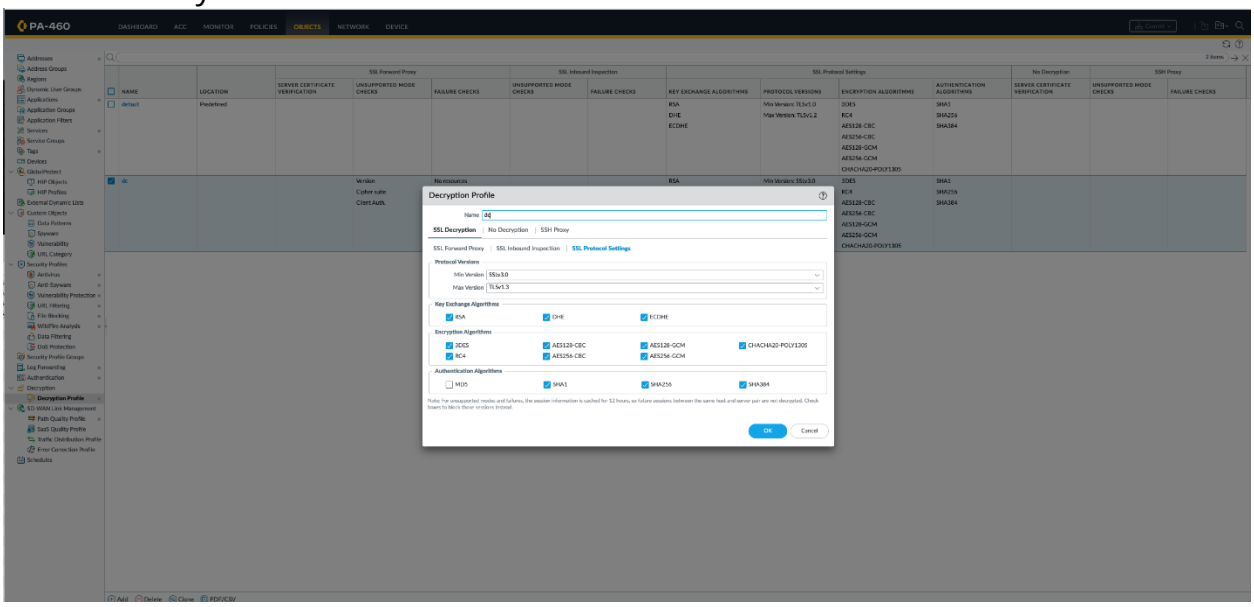


Copyright ©2023 Miercom

Firewall Policy # 3



Firewall Policy #4



Copyright ©2023 Miercom

9.0 Product HW and OS Specifications

		FortiGate 200F	PA-460
System	Network Connectivity	18 x GE RJ45 (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 4 x 10GE SFP+ slots, NP6XLite and CP9 hardware accelerated,	8x RJ45 (GigE)
	Redundant Power Supplies	Integrated internally	Requires power supplies add-on, which is an external
	Rackmount	Yes	Desktop unit Requires rackmount add-on
	Operating System	80 MB	830 MB
	T1 = 1.55 Mbps	7.1 minutes	73.78 minutes
	ADSL+ = 8 Mbps	1.3 minutes	13.83 minutes
	Deploying basic configs	Real-time	Compile, commit, reboot
	Boot time	Less than 2 minutes	> 15 minutes

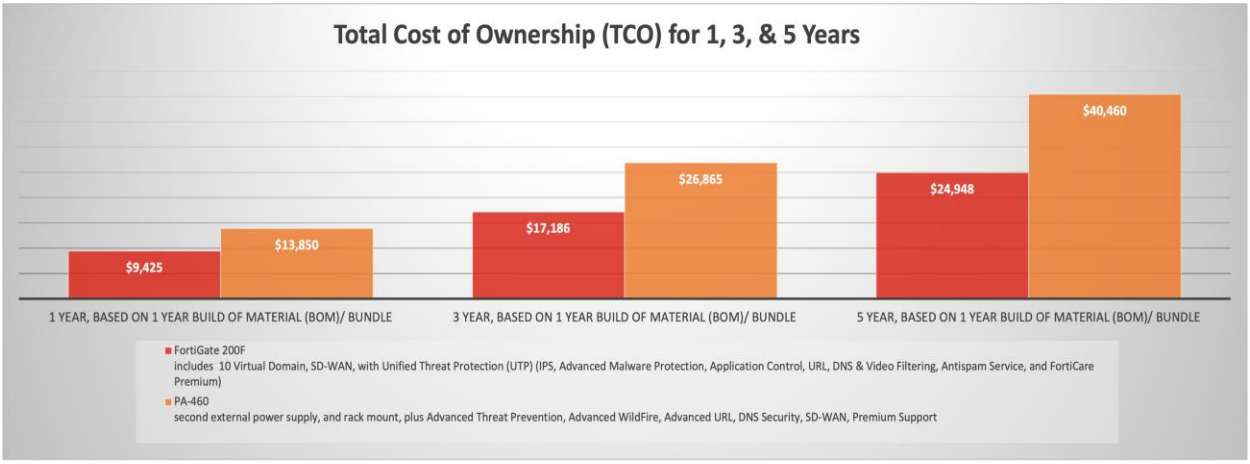
Boot time is the total time to reboot plus the time for the traffic for the protected network to continue, i.e., the device is completely operable providing protection and passing network traffic.

Copyright ©2023 Miercom

10.0 Total Cost of Ownership Summary

In the $5K - $7.5K price band, both the FortiGate 200F and PA-460 were chosen. It is essential to know the TCO analysis is to level set because features and functionality are provided natively without charge, while other competitors would have chargeable add-ons.

For this configuration, Fortinet has one SKU, which includes the hardware, security subscriptions, and support. Palo Alto has 10 SKUs for this use case. Having less SKUs help reduce the complexity of ordering and missing items.



10.1 FortiGate 1 Year

SKU	Product	Price/Unit	Quantity	Total
FG-200F-BDL-950-12	Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP)	$9,424.80	1	$9,424.80 Delete

Total: $9,424.80

10.2 FortiGate 3 Year

SKU	Product	Price/Unit	Quantity	Total
FG-200F-BDL-950-36	Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP)	$17,186.40	1	$17,186.40 Delete

Total: $17,186.40

Copyright ©2023 Miercom

10.3 FortiGate 5 Year

SKU	Product	Price/Unit	Quantity	Total
FG-200F-BDL-950-60	Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP)	$24,948.00	1	$24,948.00 Delete

Total: $24,948.00

10.4 Palo Alto Networks 1 Year

SKU	Product	Price/Unit	Quantity	Total
PAN-PA-460	Palo Alto Networks PA-460	$5,025.00	1	$5,025.00 Delete
PAN-PA-400-RACKTRAY	Rack mountable tray for up to two PA-400s and 4 power adapters for a 4 post rack mount (PA-440/450/460 models only)	$210.00	1	$210.00 Delete
PAN-PWR-50W-AC	50W AC power adapter for PA-440, PA-450 and PA-460	$140.00	1	$140.00 Delete
PAN-PA-460-VSYS-4	Virtual systems upgrade - Additional 4 virtual systems (1 to 5) for PA-460	$1,000.00	1	$1,000.00 Delete
PAN-PA-460-AWF	PA-460, Advanced WildFire subscription, 1 year (12 months), term.	$1,510.00	1	$1,510.00 Delete
PAN-PA-460-ATP	PA-460, Advanced Threat Prevention subscription, 1 year (12 months), term.	$1,520.00	1	$1,520.00 Delete
PAN-PA-460-ADVURL	Advanced URL Filtering subscription, 1-year, PA-460	$1,520.00	1	$1,520.00 Delete
PAN-PA-460-DNS	PA-460, DNS security subscription, 1 year (12 months), term.	$1,010.00	1	$1,010.00 Delete
PAN-PA-460-SDWAN	PA-460, SD-WAN subscription, 1 year (12 months), term.	$1,010.00	1	$1,010.00 Delete
PAN-SVC-PREM-460	PA-460, Premium support, 1 year (12 months), term.	$905.00	1	$905.00 Delete

Total: $13,850.00

Copyright ©2023 Miercom

10.5 Palo Alto Networks 3 Year

SKU	Product	Price/Unit	Quantity	Total
PAN-PA-460	Palo Alto Networks PA-460	$5,025.00	1	$5,025.00 Delete
PAN-PA-400-RACKTRAY	Rack mountable tray for up to two PA-400s and 4 power adapters for a 4 post rack mount (PA-440/450/460 models only)	$210.00	1	$210.00 Delete
PAN-PWR-50W-AC	50W AC power adapter for PA-440, PA-450 and PA-460	$140.00	1	$140.00 Delete
PAN-PA-460-VSYS-4	Virtual systems upgrade - Additional 4 virtual systems (1 to 5) for PA-460	$1,000.00	1	$1,000.00 Delete
PAN-PA-460-AWF-3YR	PA-460, Advanced WildFire subscription, 3 years (36 months), term.	$4,080.00	1	$4,080.00 Delete
PAN-PA-460-ATP-3YR	PA-460, Advanced Threat Prevention subscription, 3 years (36 months), term.	$4,110.00	1	$4,110.00 Delete
PAN-PA-460-ADVURL-3YR	Advanced URL Filtering subscription, 3-year, PA-460	$4,105.00	1	$4,105.00 Delete
PAN-PA-460-DNS-3YR	PA-460, DNS security subscription, 3 years (36 months), term.	$2,740.00	1	$2,740.00 Delete
PAN-PA-460-SDWAN-3YR	PA-460, SD-WAN subscription, 3 years (36 months), term.	$2,740.00	1	$2,740.00 Delete
PAN-SVC-PREM-460-3YR	PA-460, Premium support, 3 years (36 months), term.	$2,715.00	1	$2,715.00 Delete

Total: $26,865.00

Copyright ©2023 Miercom

10.6 Palo Alto Networks 5 Year

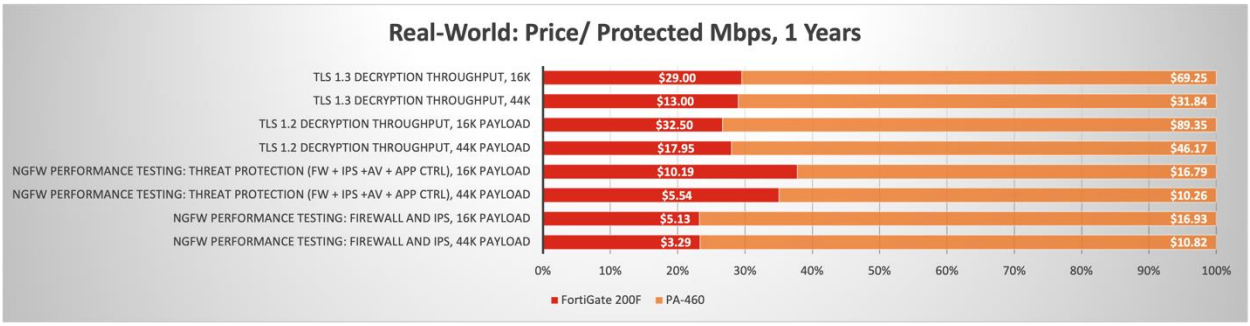
SKU	Product	Price/Unit	Quantity	Total
PAN-PA-460	Palo Alto Networks PA-460	$5,025.00	1	$5,025.00 Delete
PAN-PA-400-RACKTRAY	Rack mountable tray for up to two PA-400s and 4 power adapters for a 4 post rack mount (PA-440/450/460 models only)	$210.00	1	$210.00 Delete
PAN-PWR-50W-AC	50W AC power adapter for PA-440, PA-450 and PA-460	$140.00	1	$140.00 Delete
PAN-PA-460-VSYS-4	Virtual systems upgrade - Additional 4 virtual systems (1 to 5) for PA-460	$1,000.00	1	$1,000.00 Delete
PAN-PA-460-AWF-5YR	PA-460, Advanced WildFire subscription, 5 years (60 months), term.	$6,790.00	1	$6,790.00 Delete
PAN-PA-460-ATP-5YR	PA-460, Advanced Threat Prevention subscription, 5 years (60 months), term.	$6,830.00	1	$6,830.00 Delete
PAN-PA-460-ADVURL-5YR	Advanced URL Filtering subscription, 5-year, PA-460	$6,830.00	1	$6,830.00 Delete
PAN-PA-460-DNS-5YR	PA-460, DNS security subscription, 5 years (60 months), term.	$4,555.00	1	$4,555.00 Delete
PAN-PA-460-SDWAN-5YR	PA-460, SD-WAN subscription, 5 years (60 months), term.	$4,555.00	1	$4,555.00 Delete
PAN-SVC-PREM-460-5YR	PA-460, Premium support, 5 years (60 months), term.	$4,525.00	1	$4,525.00 Delete

Total: $40,460.00

11.0 Comparative Price/ Protected Mbps

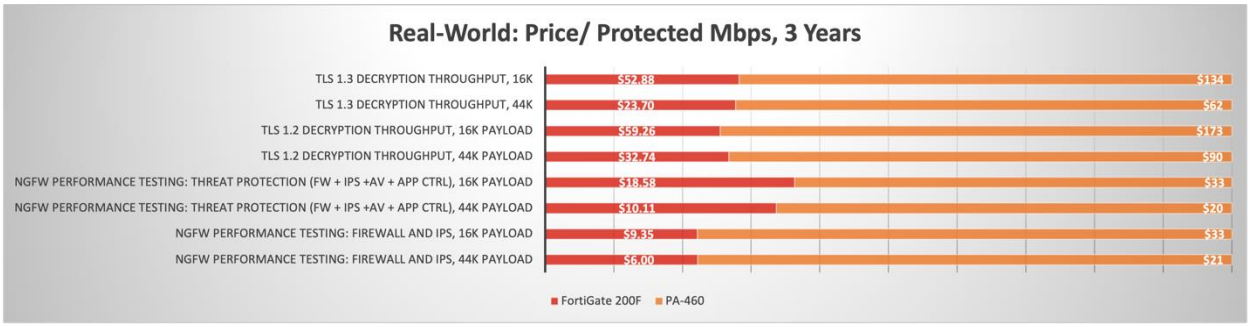
The analysis for Price per Protected Mbps is derived from the total cost of ownership divided by the test results. Both the multi-year TCO and different test results are published in this report.

11.1 Comparative Price/ Protected Mbps, 1 Year

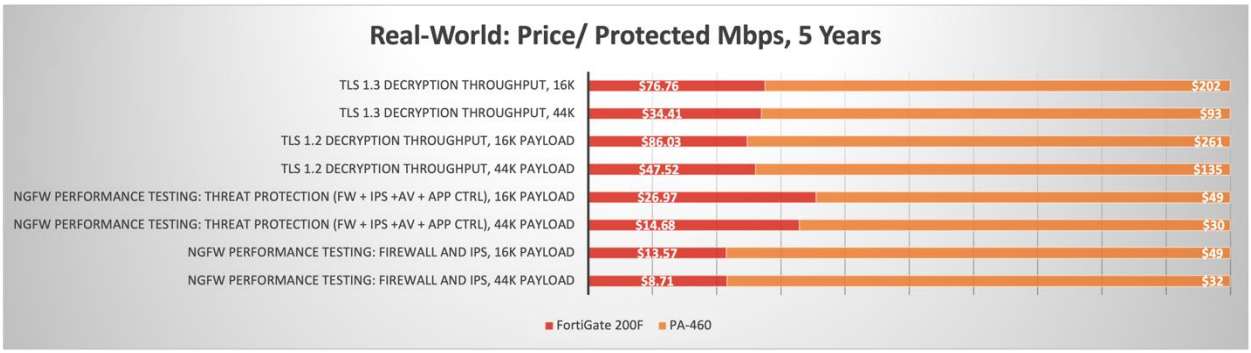


Copyright ©2023 Miercom

11.2 Comparative Price/ Protected Mbps, 3 Years



11.3 Comparative Price/ Protected Mbps, 5 Years



Copyright ©2023 Miercom

12.0 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 testing 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.

12.1 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.

This report is provided through license and restricted use from a copyright source. Downloading, circulating, or using this report in any way, you must agree to Miercom's Terms of Use. If you do not agree with these terms you are not permitted to maintain copy, otherwise use, or reference details within this report. For full disclosure of Miercom's terms, please visit: https://miercom.com/tou.

© 2023 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.