Miercom

Trellix

Trellix

Next Generation Intrusion Prevention System (NGIPS)

Summary Report SR210318E

Security Certification Testing

MIERCOM.COM

CONTENTS

KEY FINDINGS

1

The only thing predictable about network threats is their unpredictability. With an ever-evolving threat landscape, security solutions are constantly facing the challenge of protecting their customers. Independent third-party testing is one of many effective mechanisms for security vendors to index the quality of their product, by measuring both performance and security.

There are many vendors offering Intrusion Prevention Systems (IPS) for granular protection of enterprise networks. The Trellix Intrusion Prevention System (formerly known as McAfee Network Security Platform) stands ahead of competitive IPS products as shown in this report. The system proved seamless detection and blocking of both known and unknown threats across the network perimeter, data center and cloud environments.

Using multiple signature-less detection technologies, including file analysis and network behavior analytics, the Trellix IPS finds malicious activity and lateral movement across the entire threat lifecycle. Combined with on-box Next Generation IPS, (NGIPS) enforcement, inbound and outbound SLL inspection, and intelligent workflows, the Trellix IPS is an advanced threat inspection and protection solution for dynamic environments that delivers a simplified all-in-one approach to threat visibility and minimizes the alert fatigue usually associated with network security solutions. For the highest levels of protection, NGIPS policies can be modified to fit the business intent of the network, customizing attack set profiles for areas of risk that make sense to the individual organization.

Trellix engaged Miercom to independently assess its NGIPS solution for security, performance and hands-on use to provide unbiased verification of Trellix's unique qualities. The NGIPS solution was deployed in a real-world enterprise environment with simulated traffic and endpoints. By subjecting the NGIPS solution to performance tests, multiple iterations of attacks from our proprietary malware suite, and exploits from Ixia BreakingPoint, we observed and validated features and functionality from the perspective of an IT administrator.

Key Findings

- Trellix NS9500 prevented 99.3% of IXIA BreakingPoint IPS Critical Strike Pack vulnerabilities
- Prevented 98.7% of malware from Miercom's Enterprise Critical Protect Malware Set consisting of compound threats, zero-day threats and ransomware (outperforming the industry average by 25%)
- Detected 97.8% of malicious URLs over HTTP with the recommended default configuration (outperforming the competitive industry average by 44%)
- Detected 100% of malicious URLs over HTTP with optimized settings (outperforming the competitive industry average by 47%)
- Proved effective URL filtering by detecting 100% of blacklisted URLs

- Successfully restricted access to all specified applications using firewall policies
- Trellix NS9500 in a standalone configuration with all security features enabled (UTM mode) proved throughput capacity and protection exceeding the licensed capacity of 10 Gbps by 44 percent
- Trellix NS9500 in a stacked configuration with all security features enabled (UTM mode) proved throughput capacity and protection exceeding the license capacity of 40 Gbps by 18%
- Supported 50 Gbps of stateful HTTP throughput and achieved 48.5 Gbps stateful HTTP UTM throughput for a stacked 4-port pair configuration – outperforming its licensed capacity (40 Gbps licensed capacity for stacked configuration) for both 1518-byte frame and IMIX traffic loads by 20%
- Achieved 34.7 million concurrent TCP sessions and 1.04 million TCP connections per second for stacked stateful TCP capacity test
- Surpassed its rated standalone and stack performance for the Enterprise Traffic Mix profile at 18.2 Gbps and 48.5 Gbps, respectively (For 10 Gbps and 40 Gbps licenses)
- Sustained real-world load conditions of 20% bandwidth, and extended attack load conditions of 90% bandwidth, with no notable drop in throughput or security efficacy
- Successfully handled protocol fuzzing test scenarios generated by the Ixia BreakingPoint Stack Scrambler and maintained normal traffic while successfully blocking 100% of attacks
- Seamless failover of link interrupted to pass through or blocking mode as configured. No observed data loss, corruption or errors with individual redundant power source removal
- Straightforward, organized visibility and management over threats, troubleshooting, policies and devices with granular and customizable reporting
- Integration with the Advanced Threat Defense (ATD) virtual sandbox feeds the Trellix Cloud and Edge services with malware signatures found using heuristic analysis and advanced virus detection techniques to provide robust security
- Successfully prevented 100% of evasive malicious traffic and exploits mounted with mutated traffic
- Exceptional scalability with flexible capacity with licensing and stackable architecture to provide as little or as much protected bandwidth for small to large enterprises up to 100Gbps

Based on our findings, the Trellix Intrusion Prevention System (IPS) with NS9500 sensors demonstrates competitively superior security and performance. The Trellix solution was stressed under real-world exploits, both known and not yet discovered, and heavily loaded conditions. By passing these tests with ease, Trellix IPS has rightfully earned the distinction as *Miercom Certified Secure*.

Rob Smithers

CEO, Miercom

Test Summary

2

Security Test	Result
IPS Exploit Detection	**Pass - 99.3% vs Industry Average 83.2%**
Malware Detection (HTTP) - 2020	**Pass - 98.7% vs Industry Average 73.5%**
Malicious URL (with Out-of-Box Settings)	**Pass - 97.8% vs Industry Average 53.5%**
Malicious URL (with Optimized Settings)	**Pass - 100% vs Industry Average 53.5%**
URL Filtering	**Pass**
Application Inspection & Control	**Pass**

Performance Test	Result
UDP 1518-byte (Standalone & Stack UTM Mode) 10G and 40G Capacity License	**18.6 Gbps; 49 Gbps**
UDP IMIX (Standalone & Stack UTM Mode) 10G and 40G Capacity License	**17 Gbps; 47 Gbps**
TCP (Standalone & Stack UTM Mode) 10G and 40G Capacity License	**10.4M Concurrent Sessions, 496K Connections/sec; 34.7M Concurrent Sessions, 1.04M Connections/sec**
HTTP (No HTTP Response Scanning) 40G Capacity License	**50 Gbps**
HTTP (Full Security UTM Mode) 40G Capacity License	**48.5 Gbps**
Enterprise Mix (Full Security UTM Mode) 40G Capacity License	**48.5 Gbps**

Performance Test	Result
20% Load 40G Capacity License	24 Gbps
90% Load (Extended Attack) 40G Capacity License	35 Gbps
Protocol Mutation & Fuzzing	PASS
Data Persistence	PASS

Other Test	Result
User Action	PASS
Logging & Reporting	PASS
ATD Integration	PASS
Evasive Threat Testing	PASS
Scalability	PASS

3 Introduction

Networks, small and large, encounter threats from different vectors that may not always be detected by a basic firewall appliance. Without a reliable and secure network, businesses are left vulnerable to downtime, data loss and decreased revenue from attacks.

Intrusion detection monitors traffic for suspicious activity, but an Intrusion Prevention System (IPS) goes a step further and blocks it. This can be accomplished using any combination of hardware, software, virtual appliances, network security appliances or cloud-based services.

IPS is not one-size-fits-all. It protects networks with customized detection and prevention that fit the needs of the organization, providing more robust protection than other broader security controls, such as a secure web gateway that only examines traffic at the network perimeter. IPS can increase the efficiency of other security products by reducing traffic loads and preventing attacks they would have to process – and in some cases, may never block. IPS uses a combination of technologies to narrow the attack surface that other security solutions may lack.

Most notably, IPS goes beyond signature-based detection and can pinpoint anomalies particular to that specific network. This means distinguishing suspicious activity within normal network operations that other security solutions might miss, making IPS crucial for attack prevention.

Beyond web and email activity, most security products are unable to detect threats in non-web traffic. IPS carries a huge advantage when it comes to identifying these application-based attacks. Networks can be exposed to thousands of applications and without IPS, they are blind to threats from this vector. Additionally, IPS includes features for application whitelisting for more control.

Despite strategic deployment, high-end monitoring and intricate prevention methods, the processing involved in using an IPS can pose a restriction on data throughput. A clear advantage of an IPS is being able to strike a balance between heightened security and performance. It is just as important for the IPS solution to maximize security without degrading user experience and general business productivity.

And lastly, the IPS should be easy to use. Reporting, logging and management of the IPS should be straightforward, with little to no learning curve. A complicated interface can make it harder for IT administrators to make the best use of the IPS, and network security may suffer. The interface is expected to be concise, clear and robust.

Testing focused on the following:

- Intrusion Prevention System (IPS)
- Malware & Malicious URL Defense
- URL Filtering
- Performance
- Stability
- Ease of Use
- Management & Reporting

4 How We Did It

We tested the three devices comprising the Trellix IPS security solution: Trellix IPS Manager, Trellix IPS Sensor NS9500 and Trellix Advanced Threat Detection (ATD) Sandbox. The NS9500 appliance was considered the Device Under Test (DUT) for most tests.

4.1 Test Tools

Ixia BreakingPoint FireStorm v8.50 optimizes security devices by simulating live security attacks and invasions. By sending a mixture of application traffic and malicious traffic, this tool determines IPS and AV capabilities for detecting threats while remaining resilient. The "Critical Strike Pack" uses variants, or randomized path combinations, to exploit. Dynamic, "smart" exploits attack hosts and applications and are customizable for specific scenarios (ATI-Strike Pack 2019, Evergreen 2019, Malware 2019, Daily Malware current as of December 2020).

Linux Attack/Control Machine used Debian 10 with Kernels 4.1.x and 5.1.x. We tested using 64-bit Linux.

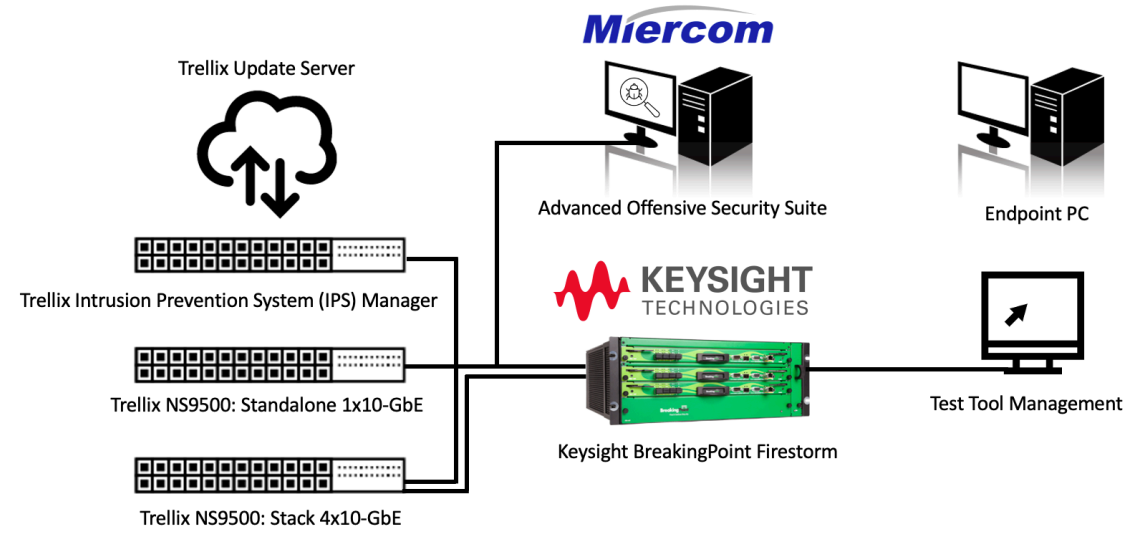
Linux Test Client used Debian 10 with Kernels 4.1.x inside KVM Virtual Machines with physical Ethernet connections via PCIE bridging. We tested using 64-bit Linux.

Nmap 7.70 + Zenmap is an open source tool for network exploration and security auditing, designed to rapidly scan networks using raw IP packets in novel ways. It can determine available hosts, offered services (app name and version), running operating systems (OS versions), types of packet filters/firewalls, and dozens of other characteristics. Nmap is also useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Zenmap is an X11+GTK frontend for Nmap.

TRex-TGN 2.61 is an open source, low cost, stateful and stateless traffic generator fueled by DPDK. It generates L4-7 traffic based on pre-processing and smart replay of real traffic templates. TRex amplifies both client and server-side traffic and can scale up to 200Gb/sec with one UCS. TRex Stateless functionality includes support for multiple streams, the ability to change any packet field and provides per stream statistics, latency and jitter.

Apache 2.4.38 is a highly effective, reliable and secure HTTP/S server. It is responsible for 29% of all web traffic served today. It has played a key role in the growth and development of the Internet. Its ubiquitous nature in the wider internet makes it an ideal software package to test, and simulate website access and delivery, not only of content but of malware.

4.2 Test Bed Diagram



Source: Miercom

Miercom engineers deployed a simulated enterprise network with access to the Internet with LANs protected by the Trellix NS9500. All traffic was routed via L2 switching hardware on the DUT. When verifying performance capabilities, we deployed the DUT within a secondary test setup where the Ixia BreakingPoint and TRex traffic generators simulated intense traffic loads. For both security and performance, a series of Virtual Machines (VMs) were used as client endpoints. These endpoints were victims of a battery of the Miercom Security Test Suite offensive attacks and exploits, while handling real-world loads. For most tests, the Trellix solution had its signature-less engines enabled.

Device/Feature	Version
Trellix Network Security Manager (NSM)	10.1.190.2
Trellix NS9500	10.1.5.24
Signature Set	10.8.15.4

Two modes were tested:

- **Standalone:** Single (1) NS9500 device with 10 Gbps licensed capacity
- **Stack:** Two (2) NS9500 devices with 40 Gbps licensed capacity

5 Security

5.1 Intrusion Prevention System

Ixia BreakingPoint Critical Strike Pack
NGIPS expected to scan major protocols to detect and block threats.

Status: **PASS; 99.3% efficacy vs Industry Average 83.2%**

5.2 Malware Defense

Detection efficacy against Miercom Malware Suite of thousands of malware samples over HTTP.

Status: **PASS; 98.7% efficacy vs Industry Average 73.5%**

5.3 Malicious URL Protection

Detection efficacy (Out-of-Box & Optimized) against thousands of proprietary malicious URLs.

Status: **PASS; 97.8% Out-of-Box and 100% Optimized efficacy vs Industry Average 53.5%**

5.4 URL Filtering

Status: **PASS; 100% efficacy against blacklisted websites**

6 Application Inspection & Control

6.1 Restricted Application Access

Video & Music Streaming, Games, Social Media, and Remote Applications
NGIPS expected to restrict access for specified applications.

Status: **PASS**

Performance

7.1 Stateless UDP Traffic Performance

UDP throughput for UTM Full Security mode for Standalone (10 Gbps) and Stack (40 Gbps) configurations.

Status: PASS; both configurations exceeded licensed capacity

Mode/Test	Capacity (Gbps)
Standalone UTM 1518-byte	18.6 Gbps
Standalone UTM IMIX	17 Gbps
Stack UTM 1518-byte	49 Gbps
Stack UTM IMIX	47 Gbps

7.2 Stateful TCP Capacity

TCP session and connection rate for UTM Full Security mode for Standalone and Stack configurations.

Status: PASS

Mode/Test	Concurrent Sessions (Millions)
Standalone UTM Concurrent TCP Sessions	10.4M
Stack UTM Concurrent TCP Sessions	34.7M

Mode/Test	Connections per Second (Millions)
Standalone UTM TCP Connections per second	0.496M
Stack UTM TCP Connections per second	1.040M

7.3 Stateful HTTP Traffic Performance

HTTP with 44KB payload for Standalone (10 Gbps) and with/without security for Stack (40 Gbps).

Status: PASS; both configurations exceeded licensed capacity

Mode/Test	Capacity (Gbps)
Standalone UTM	18.2 Gbps
Stack No HTTP Response Scanning	50 Gbps
Stack UTM (Full Security)	48.5 Gbps

7.4 Enterprise Traffic Mix Performance

App Simulator measuring max throughput in UTM mode for Standalone (10 Gbps) and Stack (40 Gbps).

Status: PASS; both configurations exceeded licensed capacity

Mode/Test	Capacity (Gbps)
Standalone UTM	18.2 Gbps
Stack UTM	48.5 Gbps

Stability & Reliability

8

8.1 Loaded Protection

HTTP application traffic profile with 20% load at data rate of 4 Gbps with 1,000 malicious samples.
NS9500 expected to block all malicious data with <5% failed transactions and no more than 20% CPU.

Status: **PASS; 100% data passed for over 36.7M connections and 100% blocking efficacy**

8.2 Protection under Extended Attack

Controlled application of malware with aggressive 90% background traffic.
NS9500 expected to maintain traffic connections and malware detection without exceeding 90% CPU.

Status: **PASS**

Test	Blocked Malware Effciacy (%)
Initial Test Run	99.7%
Post-Threat Learning	100%

8.3 Protocol Mutation and Fuzzing

BreakingPoint StackScrambler profile generated randomized mutated and fuzzed protocols at 2 Gbps with up to 10,000 simultaneous data flows.
NS9500 expected to alert, block traffic, or reset connection while maintaining stability and operation.

Status: **PASS; 100% malicious samples blocked**

8.4 Data Persistence

Power outages, electrical surges, and power disruptions should not cause data loss.
NSM and NS9500 expected not to lose data or configuration after forced power down and removal.

Status: **PASS; no data loss, corruption, or errors observed**

9 Quality of Experience

9.1 User Action

Status: **PASS; clear organization for viewing and analyzing threats**

9.2 Logging and Reporting

Status: **PASS; advanced logging, search, and reporting capabilities**

10 Advanced Threat Defense (ATD) Integration

10.1 ATD Integration

Trellix ATD integrates as a virtual sandbox solution, executing and anakyzing suspicious samples in controlled environments to determine if they are malicious. With other heuristics and advanced virus detection techniques, ATD acts as a virtual honeypot to catch malware.

Status: **PASS; Trellix Cloud and Edge services provide real-time malware defense**

An impressive combination of IPS and ATD yielded a strong perimeter defense for the test enterprise network, complying with high data security and integrity standards.

11 Evasive Threat Testing

11.1 Evasive Threat Testing

Launched over 43,000 different evasions (unique IP/TCP fragmentation or scrambling mixtures) for each of the two attacks for a total of more than 86,000 strikes.

Status: **PASS; prevented 100% of all embedded evasion attempts**

12 Scalability

12.1 Scalability

Offer throughput options via software licensing to scale from 10 Gbps to 100 Gbps.

Status: **PASS; multiple options offered with no issues in scalability or performance**

Appliance	Available Throughput Options
NS9500 (Standalone)	10 / 20 / 30 Gbps
NS9500 x 2 (Stack)	40 / 60 Gbps
NS9500 x 4 (Stack)	100 Gbps

About Miercom Certified Secure

This report was sponsored by Trellix. The data was obtained completely and independently by Miercom engineers and lab-test staff as part of our Certified Secure assessment. Testing such as this is based on a methodology that is jointly co-developed with the sponsoring vendor. The test cases are designed to focus on specific claims of the sponsoring vendor, and either validate or repudiate those claims. The results are presented in a report such as this one, independently published by Miercom.

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.

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 to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied; Miercom 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.