McAfee Network Security Platform

Next Generation Intrusion Prevention System (NGIPS)

Security Assessment

March 2020

DR191231F

Miercom

Miercom.com

Contents

1.0 Executive Summary

Network threats vary so much in type, vector and approach that security appliances may not have the sophistication to detect or prevent them. An Intrusion Prevention System (IPS) provides protection that other security products may miss, or simply not offer. The granularity, visibility and layered security of IPS makes it a must-have for any enterprise organization.

Detect and block known and unknown threats across the network perimeter, data center and cloud environments seamlessly with McAfee Network Security Platform (NSP). Using multiple signature-less detection technologies including file analysis and network behavior analytics, McAfee Network Security Platform can find malicious activity and lateral movement across the entire threat lifecycle. Combined with on-box IPS enforcement, in- and out-bound SLL inspection, and intelligent workflows, McAfee Network Security Platform 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, IPS 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.

Aggregated workloads inside private and public clouds are supported using virtual machines (VMs) that allow flexibility, dynamic scalability and seamless integration with software-defined networking (SDN) platforms that orchestrate VMs and associated workloads. McAfee supports these unique demands with a Virtual Network Security Platform version that is available on AWS Marketplace, Azure Marketplace, and Oracle's OCI Marketplace, providing the same centralized management, inspection technologies, high availability, disaster recovery, and load balancing performance as its hardware appliance counterpart.

McAfee engaged Miercom to independently assess its NSP Next Generation IPS (NGIPS) solution for security, performance and hands-on use to provide unbiased verification of McAfee'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 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

- 100% malware prevention over FTP and 97% prevention over HTTP – blocking complex threats such as zero-day, polymorphic, ransomware and evasive threats
- 100% prevention against high-damage Ixia BreakingPoint IPS Critical Strike pack vulnerabilities
- Handled a total transmitted flow of 32 TiB of data with no packet loss and up to 40 Gbps HTTP throughput; connections and response times under 10ms
- Sustained real-world load conditions of 60% bandwidth, and extended attack load conditions of 90 percent bandwidth, with no notable drop in throughput or security efficacy

- Successfully handled protocol fuzzing test scenarios, routing over 7 million traffic mutated frames generated by the Ixia BreakingPoint Stack Scrambler and maintained dropped corrupted and mutated frames with low loss and no notable drop in performance
- 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 McAfee Cloud and Edge services with malware signatures found using heuristic analysis and advanced virus detection techniques to provide robust security
- 39.5 Gbps stateless firewall throughput and achieved high data rates with security layers applied – maintaining 31.6 Gbps with all security enabled
- Successfully prevented 100% malicious traffic and exploits mounted by the Evader tool used to harden security by testing evasion attempts via exploits with mutated traffic

Based on our findings, the McAfee Network Security Platform demonstrates competitively superior security and performance tested with real-world exploits and stressful conditions. We proudly award the McAfee Network Security Platform the ***Miercom Certified Secure*** certification.

Robert Smithers
CEO, Miercom

2.0 Test Summary

Summary of McAfee NS9x00[1] Test Results: Security Efficacy and Performance

Tests	Page	Vendors
Security Efficacy	10	McAfee NS9x00
Malware Detection (HTTP)	11	96.9
Malware Detection (FTP)	11	100
IPS Exploit Detection	12	100*
URL Filtering	13	PASS

≥85 percent	51-84 percent	≤50 percent

Performance	14	McAfee NS9x00
UDP – FW	14	39.5 Gbps
UDP – FW + IPS	14	34 Gbps
UDP – FW + IPS + AppCtrl	14	33.6 Gbps
UDP – Full Security Stack	14	31.6 Gbps
HTTP – Full Security Stack	15	40 Gbps
HTTP – Total Data Transmitted	15	32 TiB
60% Load	16	24 Gbps
90% Load (Extended attack)	17	35 Gbps
Protocol Mutation and Fuzzing (No data corruption)	18	PASS
Protocol Mutation and Fuzzing (Data corruption enabled)	18	PASS
Data Persistence	20	PASS

*Note: A challenge arises in the delay between identified vulnerabilities, created mitigations and database definitions and pushed updates to end user devices. To test any device with the latest strike of the day could not result in a 100 percent efficacy score. We tested using the NOV-2019 Ixia BreakingPoint ATI Critical Strike Pack.

[1] The McAfee NS9100 was used for this test; efficacy and performance results would be similar or better on other McAfee NS9x00 systems.

3.0 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 which 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 puts a load 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.

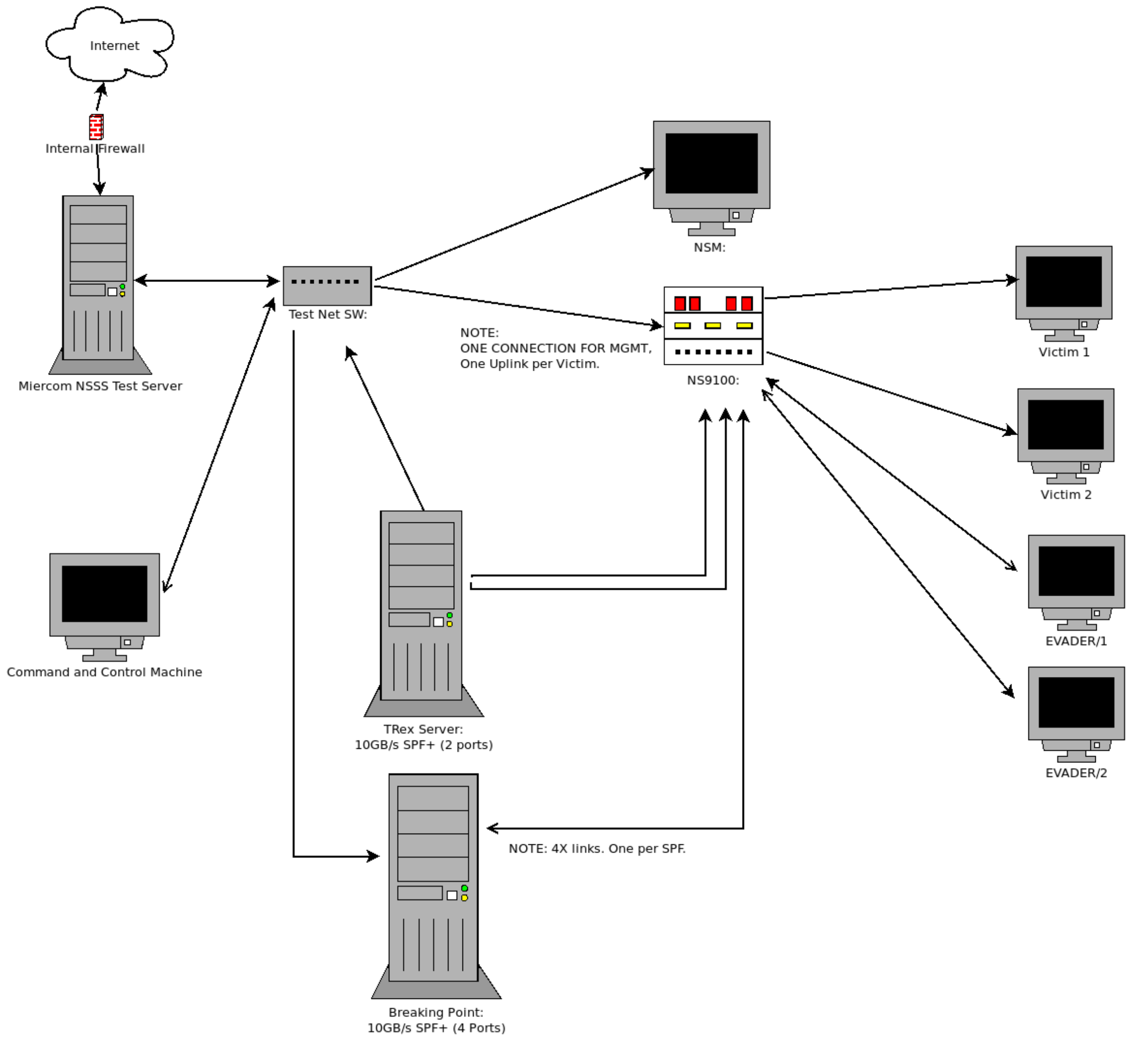
Testing focused on the following:

- Malware defense
- Intrusion Prevention System (IPS)
- Performance
- URL Filtering
- Ease of Use
- Management
- Reporting
- Deployment
- Unique features

4.0 How We Did It

Using a realistic network environment, we tested three devices: McAfee Network Security Manager (NSM), McAfee Network Sensor NS9x00 and McAfee Advanced Threat Detection (ATD) Sandbox.

Test Bed Overview



Source: Miercom 2020

To test the McAfee Network Security System, we deployed a simulated network with Internet and Local Area Networks (LANs) accessing the Internet through the NS9x00 device. All traffic was routed via Layer 2 switching hardware on the NS9x00 appliance. When verifying performance capabilities, we deployed the NS9x00 device within a secondary test setup where the Ixia BreakingPoint and Cisco 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 our Miercom Security Test Suite of offensive attacks and exploits while handling real-world loads from the Ixia BreakingPoint and Cisco TRex tools. For most tests, the McAfee NGIPS had its signature-less engines enabled.

Device/Feature	Version
McAfee Network Security Manager	9.2.9.12.6
McAfee NS9x00	1.20 (hardware), 9.2.5.136 (software)
Signature Set	10.8.2.4
GAM Callback Detector	2527.0
GAM DAT	6946
GAM DAT Engine	7001.2017.3112
Antivirus DAT	9476
Antimalware Engine	5900.7806

Security and Performance Testing Connections

Connections to the Internet were handled through a firewall, with no external connections except for those needed to validate security features on services and protocols accessible over the Wide Area Network (WAN).

The NS9x00 appliance, victim endpoints and switches were connected using CAT6 Ethernet in Gigabit full duplex mode. Connectivity between the NS9x00, TRex server and Ixia BreakingPoint appliance were accomplished using 830nm SFP+ 10-Gigabit full duplex fiber links. Our high performance, proprietary Security and Network Test Suite Server (NTSS) was connected via 2x10-Gigabit SFP ports to our aggregation switch.

Security Testing

To perform an exhaustive security review of the devices under test, we replicated a standard Internet Service Provider (ISP) setup with DHCP IP Address allocation, as seen with modern cable and fiber providers. Instead of delivering Internet via fiber or cable uplink, Internet was delivered using Ethernet cables, trunking straight into a high-bandwidth aggregation switch previously configured to serve as the backbone of our ISP.

Performance Testing

Performance was evaluated over several scenarios which replicate real-world usage of the McAfee suite in enterprise networks:

- Baseline L2
- Baseline with Full Configuration
- Light-Load
- Medium-Load
- Heavy-Load
- Torture Test

Test Tools

The following tools are a representative list of software tools and exploits we used to carry out our analysis.

Ixia BreakingPoint, v8.50

BreakingPoint 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 2019).

Linux Attacker/Control Machine

Using Debian 10 with Kernels 4.1.x and 5.1.x. We tested using 64-bit Linux.

Linux Test Client

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

qperf 0.4.11

qperf measures bandwidth and latency between two nodes. It can work over TCP/IP as well as the RDMA transports. On one of the nodes, qperf is typically run with no arguments designating it the server node. One may then run qperf on a client node to obtain measurements such as bandwidth, latency and CPU utilization.

iperf 3.6

iperf3 is a tool for performing network throughput measurements, testing TCP, UDP, or SCTP throughput.

Nmap 7.70 + Zenmap

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan networks using raw IP packets in novel ways to determine what available hosts, offered services (application 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

TRex 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

Apache 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.

Postfix 3.4.7

Postfix is a free and open-source Mail Transfer Agent (MTA) that routes and delivers email. Approximately 34% of the public-accessible email servers run Postfix; making it the second most popular MTA after Exim. Postfix is compatible with SMTP, SMTPS and Submission protocols.

Dovecot 2.3.4.1

Dovecot is a free and open source IMAP and POP3 server for UNIX-like systems written with security primarily in mind. Dovecot is a lightweight, stable and easy-to-use mail server that provides IMAP/IMAPS and POP3/POP3S access to mailboxes.

VSFTPd 3.0.3

VSFTPd is the Very Secure File Transfer Protocol Daemon. It provides an open source, standards-compliant server for the FTP and FTPS protocols to be used during testing.

5.0 Security

5.1 Malware Defense

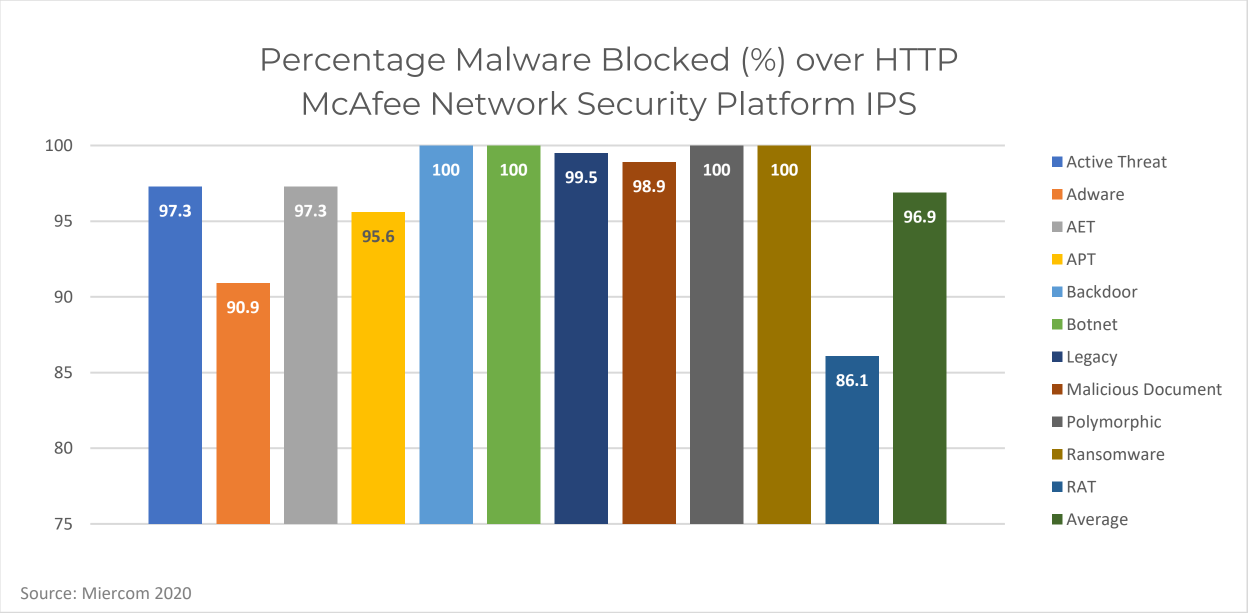
Malware is delivered to networks using different methods. An NGIPS solution needs to be prepared to handle any attack, on any protocol. Common malware (e.g. botnets, legacy files) should be detected. More sophisticated malware – polymorphic, evasive and persistent threats, that are not already known by any intelligence database – are more challenging to block. An emphasis is placed on the advanced threats as they are complex and harder to prevent.

Using more than a thousand samples from our proprietary malware suite, we assessed the antivirus engine of the NGIPS solution. The Miercom Malware Suite includes a broad range of samples:

Common Malware	
Adware	Potentially unwanted program (PUP) that displays advertisements
Backdoor	Remote attacks use port binding, control and command servers, and dormant malware to infiltrate networks using legitimate services to go unrecognized
Botnet	Communicating programs delivering spam and distributed DoS attacks
Legacy	Variants of known malware older than 30 days (e.g. virus, worms)
Malicious Documents	Mix of Microsoft and Adobe documents with macro viruses, APTs, worms
Ransomware	Malicious software that locks down file systems until ransom is paid
Remote Access Trojans (RATs)	Trojans disguised as legitimate software remotely controlling victim once activated
Advanced Malware	
Active Threats	Custom-crafted, constantly changing evasive malware
Advanced Evasive Techniques (AETs)	Combined evasion tactics that create multi-layer access
Advanced Persistent Threats (APTs)	Continuous hacking with payloads opened at the administrative level
Polymorphic, Zero-Day Malware	Constantly changing, difficult to detect; exploit known vulnerabilities

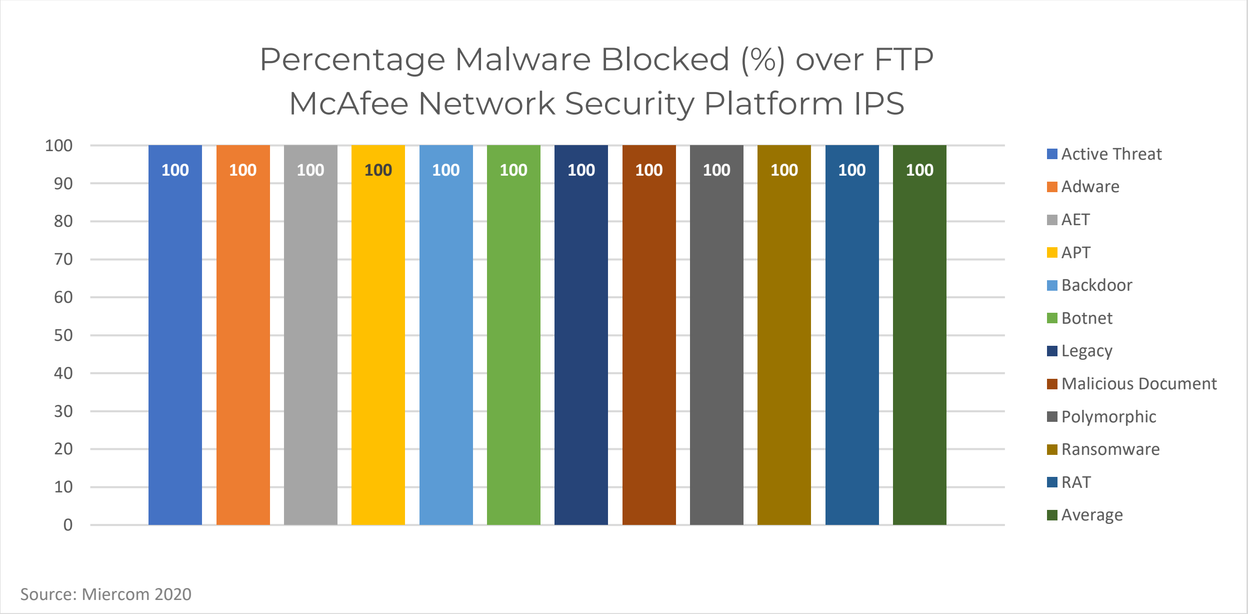
The McAfee NSP NGIPS was deployed between untrusted and trusted zones of a simulated network with a switch, firewall and endpoint devices to represent a real-world environment. An attacker in the untrusted zone (our Miercom Malware Suite) attempted to deliver malware to the trusted zone over two common protocols – HTTP and FTP. Any successfully transferred sample to a target endpoint was considered a failing mark. Security efficacy was recorded as the percentage of samples blocked out of the total set attempted. Blocked samples were analyzed to determine visibility and intelligence of the NGIPS solution.

Results



Source: Miercom 2020

All malware samples were delivered to target hosts using an HTTP server. Given the granular scanning services offered, we expected reliable malware detection of 85 percent efficacy or better. McAfee NGIPS detected 100 percent of backdoor, botnet, polymorphic and ransomware samples. These are advanced samples that have complex and costly consequences. Other areas of high detection rates were active threats, adware, evasive threats, persistent threats and remote access Trojans. The average security efficacy of McAfee NGIPS was 96.9 percent.



Source: Miercom 2020

All malware samples were delivered to target hosts using an FTP server. We expected similar, if not identical, results to the HTTP analysis since the scanning engine mechanisms are the same across protocols. Efficacy across FTP was higher, with perfect detection of all sample types.

5.2 Intrusion Prevention System

The refined NGIPS security feature continuously monitors a network for malicious activity. This allows the administrator to immediately remediate by adjusting configurations, policies or access control.

To test the McAfee NS9x00 appliance for NGIPS protection, we launched a series of attacks using the Ixia BreakingPoint tool. BreakingPoint uses a Critical Strike Pack – a dynamic collection of evolving attacks updated with hundreds of current, dangerous exploits and vulnerabilities – to reflect a real-world threat scenario. Using the IPS Strike List, we assessed the NGIPS detection efficacy.

BreakingPoint Strike is an attack suite containing:

- Over 6,000 strikes (SQL injections, cross-site scripting, buffer overflow)
- Natively implemented exploits, as opposed to capture replayed events
- Over 100 evasion techniques to hide attacks from security
- Over 35,000 malware
- Distributed Denial-of-Service (DDoS) attacks in parallel with application traffic (L2 through L4)
- Fragmentation, flood and DNS reflection attacks

The NGIPS should scan traffic across all major protocols to detect and block threats. The NGIPS database of reputed exploits and patterns should be frequently updated. NGIPS patterns should contain rules for detecting ransomware-related activities. Detection and prevention are expected to be performed for all traffic attempting to cross the security perimeter in real-time.

Results

Blocked exploits were logged by the Ixia BreakingPoint. The McAfee NGIPS detected 100 percent for Ixia BreakingPoint Critical Strike Pack exploits. These high-damage vulnerabilities are the most important exploits an enterprise appliance is expected to prevent. The Critical Strike Pack is updated by Ixia daily; we evaluated using version NOV-2019. We expect an excellent score to be greater than 95 percent prevention efficacy.

McAfee successfully blocked 100 percent of the November 2019 Critical Strike Pack exploits.

(Note: A challenge arises in the delay between identified vulnerabilities, created mitigations and database definitions and pushed updates to end user devices. To test any device with the latest strike of the day could not result in a 100 percent efficacy score).

5.3 URL Filtering

The McAfee NSP NGIPS is the first line of defense during Internet access. It can prevent users from reaching malicious locations which put the endpoint and network at risk for infection. The NGIPS should block known, harmful locations regardless of an attacker's antivirus bypassing technique.

Malicious locations change quickly, so our proprietary malware suite used a new set of malicious URLs. Automated scripts simulated an endpoint attempting to access each website through the NGIPS. If the site was reached, it received a failing mark. If the NGIPS makes the site inaccessible, or a block page is displayed, the sample was reported as blocked. Results were recorded as a percentage of blocked URL samples out of the total samples attempted.

Results

Pass. The NGIPS engine successfully passed this test; it showed excellent protection against malicious URLs – above the industry average.

6.0 Performance

Network security requires many high-quality services to process traffic, checking it for malware and compliance. Despite the security enhancement, this places a load on performance, so while security solutions aim to minimize risk, they must also maintain competitive performance. Security solutions capable of optimally balancing security and performance with superior engineering design are the first to be considered for business networks.

6.1 Stateless Traffic Performance

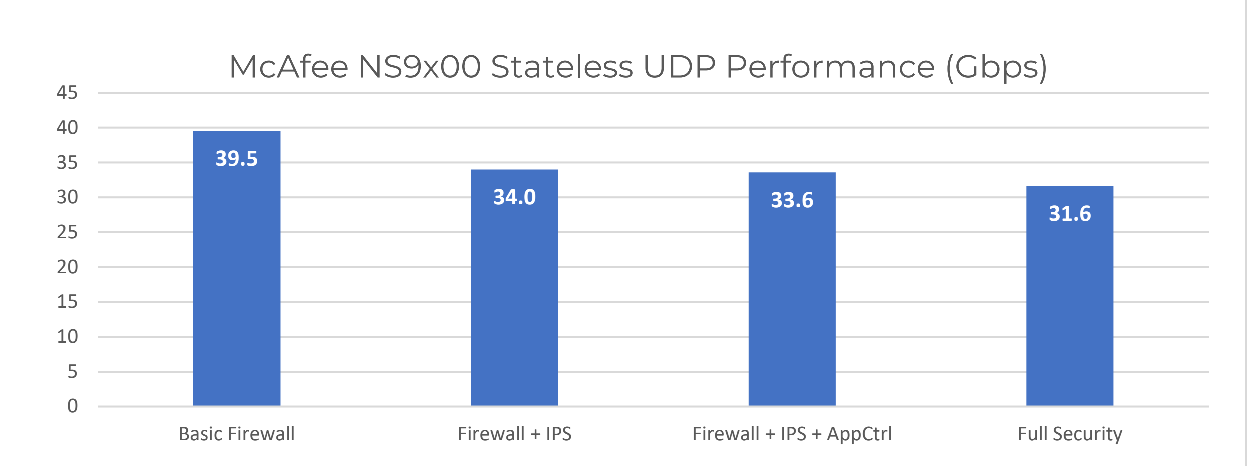
Non-stateful UDP traffic was sent through the McAfee NS9x00, resulting in performance metrics and statistics recorded in several modes:

- Firewall only
- Firewall and individually enabled features
- Full Security (all features enabled simultaneously with firewall)

The firewall-only performance is expected to yield the highest throughput. Full security mode is expected to be the lowest because of the additional security processing loads running on the device.

We expect the NS9x00 to sustain real-world traffic at the rated device throughput over extended periods of time with no more than 20 percent measurable drop in throughput as additional NSM security features are enabled. The throughput is increased in measured increments, starting at 1 Gbps, stepping up until packet loss is observed.

Results



Source: Miercom 2020

The McAfee NS9x00 displayed excellent performance. The device meets and exceeds the stated datasheet figures of merit. Over a test that lasted well over 24 hours, we did not witness, observe or record any noticeable drop in performance even when the complete security stack was enabled on the sensor appliance. Traffic was reliably routed, filtered and analyzed quickly and transparently while delivering guaranteed throughput.

6.2 Stateful HTTP Traffic Performance

Processing of stateful traffic is a realistic indicator of how the NGIPS appliance will operate in a real-world environment. This result was expected to be lower than stateless throughput since more processing is required for the application layer (HTTP).

A 44KB payload was generated from the server side of the Ixia BreakingPoint tool. The client sends GET requested to download the binary and randomized 44KB payload. The NS9x00 inspected the file under different configuration scenarios over WAN (untrusted) to LAN (trusted) network. We increased traffic and connections per second until packet loss was observed.

We expected the NS9x00 to handle up to 90 percent of its stateless traffic performance as HTTP flows.

Results

The McAfee NS9x00 was able to handle a total transmitted flow of approximately 32 Tebibytes (TiB) of data, with 100 percent of data received reliably without packet loss. Its high performance of 40 Gbps was proven when successfully connecting and sustaining thousands of HTTP connections per second, with no real observable degradation in throughput rate or user experience. Almost all established connections were under 10 milliseconds (ms), and response times were well beneath the 10ms threshold.

7.0 Stability and Reliability

7.1 Loaded Protection

The McAfee NS9x00 was expected to detect malicious attacks while handling a load of normal, real-world traffic without experiencing a significant reduction in effectiveness or a negative impact on network performance.

A traffic profile of reasonable percentage load (60 percent of total capable bandwidth) was sent through the device. Normal CPU load should not exceed 60 percent. Previously detected malware was sent within normal traffic along with HTTP requests generated by the Ixia Breaking Point tool.

Under no condition, should the reasonable traffic load create a condition which exceeds CPU loads of 60 percent on the NS9x00 appliance. Normal filtering and throughput should remain constant and predictable – there should be no packet loss and no drop in security protection efficacy.

At 60 percent load, we expect approximately 24 Gbps of stateful traffic to remain consistent and no degradation of protection, regardless of the network and processing load that the device is subject to. The CPU load should never exceed 60 percent.

Results

The McAfee NS9x00 successfully and repeatedly met the expected conditions under sustained, real-world load conditions of approximately 60 percent of total bandwidth. The NS9x00 demonstrated effective performance without notable loss.

7.2 Protection under Extended Attack

Not unlike the Loaded Protection segment of our test, this section focuses on attempting to defeat the device's protection mechanisms and/or degrade its network performance beyond usefulness. In this case, the generated traffic is 90 percent of available bandwidth.

Under no condition, should the McAfee NS9x00 begin dropping traffic at 90 percent load. The CPU load should never exceed 90 percent and there should be no notable drop in malware detection.

At 90 percent load, approximately 35 Gbps of stateful traffic, the NS9x00 should perform equally as well with response time and protection against malware. CPU load should never exceed 90 percent.

Result

The McAfee NS9x00 always met the expected conditions over multiple test iterations. Under sustained conditions replicating real-world loads of 90 percent bandwidth, the NS9x00 demonstrated impressive performance and no notable loss.

7.3 Protocol Mutation and Fuzzing

This test was carried out using the Ixia BreakingPoint Stack Scrambler test profile. The Ixia BreakingPoint Stack Scrambler generated randomized mutated and fuzzed protocols at 2 Gbps with up to 10,000 simultaneous data flows. We programmed the Stack Scrambler to fuzz packets with and without corruption. These were then introduced to the network environment for the McAfee NS9x00 appliance to detect.

The objective is to torture the device in hopes of causing either traffic to become unroutable or for the device to display instability or unpredictable behavior under attack. The result of scrambling the packages until they either caused the device to fail (in the case of corrupted traffic) or be unable to route traffic (in the case of non-corrupted frames) was recorded.

The McAfee NS9x00 was expected to produce an alert, block the traffic or reset the connection while remaining stable and operational during the test. The NS9x00 should continue to function normally, accepting normal network traffic and rejecting all mutated and fuzzed protocols.

In the context of a Distributed Denial-of-Service (DDoS) attack, a device that cannot handle corrupted traffic frames correctly would fail. To test this, we use two scenarios: traffic without corruption and traffic with corruption enabled. Without corruption, the NS9x00 was expected to correctly route frames with less than 10 percent loss. With corruption enabled, the NS9x00 was expected to correctly route frames with less than 50 percent loss.

Results

Test 1: No data corruption

In our opinion, the device is expected to route over 90 percent of mutated traffic correctly without showing unstable or unpredictable behavior to be considered having acceptable routing performance under a DDoS storm of mutated traffic. Without any strange behavior, the device performance should not drop under 90 percent, either in packets per second or total frames delivered; bandwidth should also not drop significantly.

We generated 7,073,426 frames of mutated traffic. Of these, the NS9x00 correctly routed 93.6 percent of them.

The McAfee NS9x00 passed.

Test 2: Data corruption enabled

Regarding corrupted and mutated traffic, the device should not display a notable drop in performance as in the previous non-corrupted test element. No more than 50 percent packet loss should be observed during mutated traffic storms.

We transmitted 2,684,587 mutated frames. The McAfee NS9x00 correctly routed 62.7 percent of the frames which it determined to be too corrupted to forward, discarding without any notable drop in performance or security efficacy. This resulted in a loss of 37.3 percent – well under the expected 50 percent.

The McAfee NS9x00 passed.

With data corruption enabled:

The McAfee NS9x00 passed.

In both cases, the McAfee NS9x00 correctly handled the storm of mutated traffic. All routable traffic was correctly delivered. In cases that mutated or corrupted traffic rendered the packet undeliverable, it was simply dropped without causing unexpected behavior in the device.

7.4 Data Persistence

Power outages, electrical surges and power disruptions should not cause the NS9x00 to lose valuable information – configurations, settings, logs, policies, credentials, certificates or any other critical data.

We expect the tested devices (NSM, NS9x00 and ATD) to not lose any data or configuration after we forcibly power them down by removing the power three times.

Results

The McAfee NS9x00 passed.

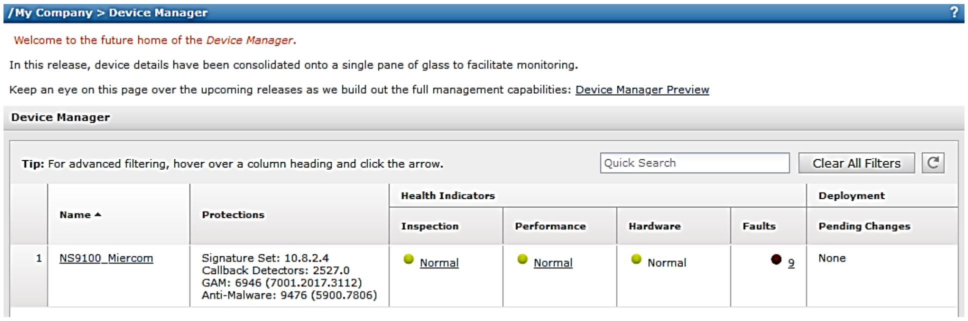
We observed no data loss, corruption or errors generated by the abrupt removal of the power source.

8.0 Quality of Experience

An NGIPS product may be excellent in terms of security and minimal effect on performance, but quality of experience differentiates it as a top choice for deployment. This section addresses the front-end experience of the out-of-box set up, console visibility and reporting.

8.1 User Action

The McAfee NS9x00 interface was simple and straightforward, offering clear organization and instructions for viewing and dissecting threats.



Welcome to the future home of the *Device Manager*.

In this release, device details have been consolidated onto a single pane of glass to facilitate monitoring.

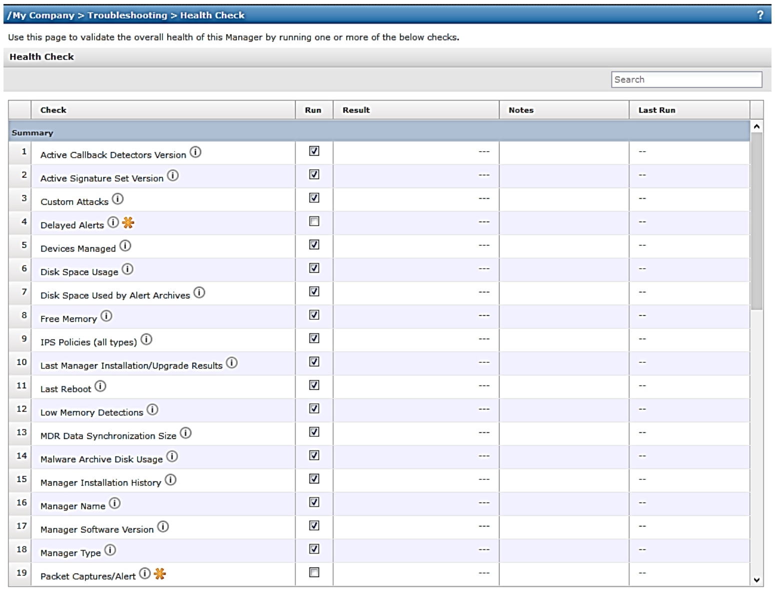
Keep an eye on this page over the upcoming releases as we build out the full management capabilities: Device Manager Preview

Device Manager

Tip: For advanced filtering, hover over a column heading and click the arrow.

	Name ▲	Protections	Health Indicators				Deployment
			Inspection	Performance	Hardware	Faults	Pending Changes
1	NS9100_Miercom	Signature Set: 10.8.2.4 Callback Detectors: 2527.0 GAM: 6946 (7001.2017.3112) Anti-Malware: 9476 (5900.7806)	● Normal	● Normal	● Normal	● 9	None

The Device Manager allows the administrator to see the health indicators in terms of security, performance, hardware, critical issues and changes.

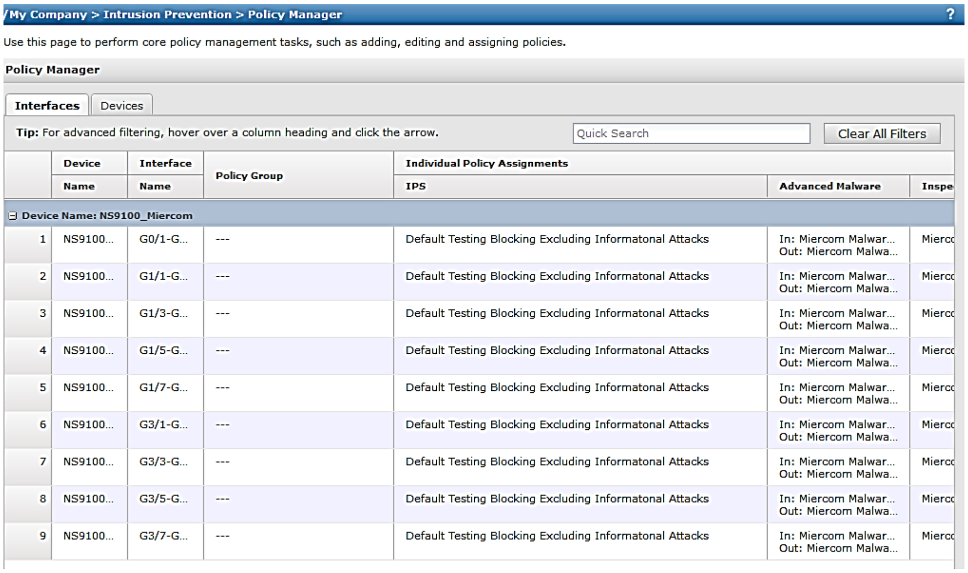


Use this page to validate the overall health of this Manager by running one or more of the below checks.

Health Check

	Check	Run	Result	Notes	Last Run
Summary					
1	Active Callback Detectors Version ⓘ	☑	---		--
2	Active Signature Set Version ⓘ	☑	---		--
3	Custom Attacks ⓘ	☑	---		--
4	Delayed Alerts ⓘ ✱	□	---		--
5	Devices Managed ⓘ	☑	---		--
6	Disk Space Usage ⓘ	☑	---		--
7	Disk Space Used by Alert Archives ⓘ	☑	---		--
8	Free Memory ⓘ	☑	---		--
9	IPS Policies (all types) ⓘ	☑	---		--
10	Last Manager Installation/Upgrade Results ⓘ	☑	---		--
11	Last Reboot ⓘ	☑	---		--
12	Low Memory Detections ⓘ	☑	---		--
13	MDR Data Synchronization Size ⓘ	☑	---		--
14	Malware Archive Disk Usage ⓘ	☑	---		--
15	Manager Installation History ⓘ	☑	---		--
16	Manager Name ⓘ	☑	---		--
17	Manager Software Version ⓘ	☑	---		--
18	Manager Type ⓘ	☑	---		--
19	Packet Captures/Alert ⓘ ✱	□	---		--

The Device Manager allows the administrator to see the health indicators in terms of security, performance, hardware, critical issues and changes.



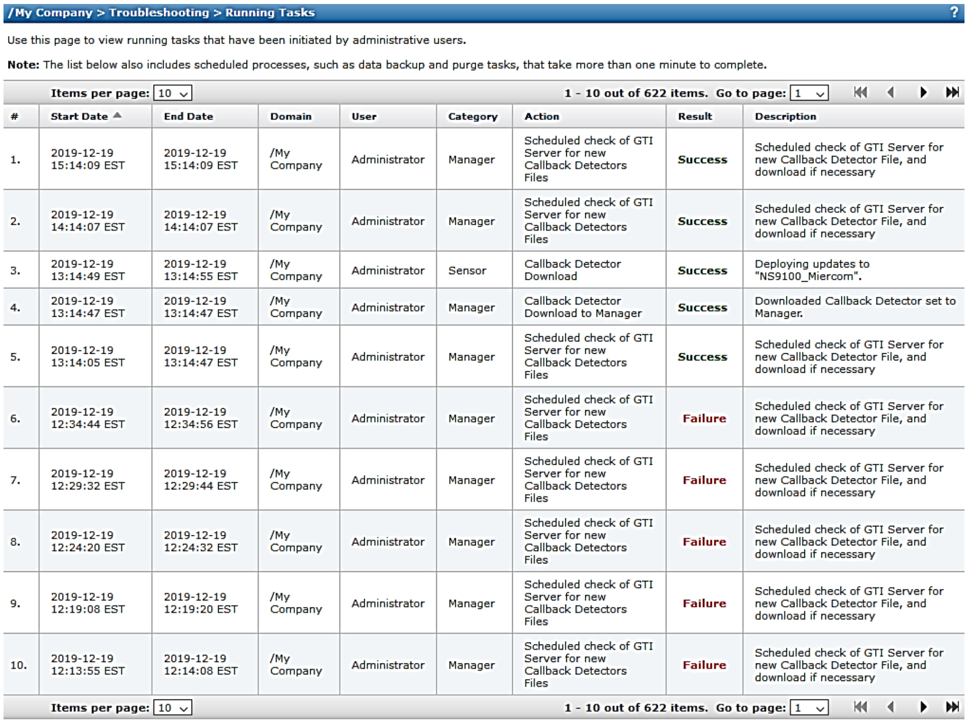
Use this page to perform core policy management tasks, such as adding, editing and assigning policies.

Policy Manager

Tip: For advanced filtering, hover over a column heading and click the arrow.

	Device	Interface	Policy Group	Individual Policy Assignments		
	Name	Name		IPS	Advanced Malware	Inspe
⊟ Device Name: NS9100_Miercom						
1	NS9100...	G0/1-G...	---	Default Testing Blocking Excluding Informatonal Attacks	In: Miercom Malwar... Out: Miercom Malwa...	Mierc
2	NS9100...	G1/1-G...	---	Default Testing Blocking Excluding Informatonal Attacks	In: Miercom Malwar... Out: Miercom Malwa...	Mierc
3	NS9100...	G1/3-G...	---	Default Testing Blocking Excluding Informatonal Attacks	In: Miercom Malwar... Out: Miercom Malwa...	Mierc
4	NS9100...	G1/5-G...	---	Default Testing Blocking Excluding Informatonal Attacks	In: Miercom Malwar... Out: Miercom Malwa...	Mierc
5	NS9100...	G1/7-G...	---	Default Testing Blocking Excluding Informatonal Attacks	In: Miercom Malwar... Out: Miercom Malwa...	Mierc
6	NS9100...	G3/1-G...	---	Default Testing Blocking Excluding Informatonal Attacks	In: Miercom Malwar... Out: Miercom Malwa...	Mierc
7	NS9100...	G3/3-G...	---	Default Testing Blocking Excluding Informatonal Attacks	In: Miercom Malwar... Out: Miercom Malwa...	Mierc
8	NS9100...	G3/5-G...	---	Default Testing Blocking Excluding Informatonal Attacks	In: Miercom Malwar... Out: Miercom Malwa...	Mierc
9	NS9100...	G3/7-G...	---	Default Testing Blocking Excluding Informatonal Attacks	In: Miercom Malwar... Out: Miercom Malwa...	Mierc

The Policy Manager gives complete control on how application traffic is processed.



Use this page to view running tasks that have been initiated by administrative users.

Note: The list below also includes scheduled processes, such as data backup and purge tasks, that take more than one minute to complete.

Items per page: 10 1 - 10 out of 622 items. Go to page: 1

#	Start Date ▲	End Date	Domain	User	Category	Action	Result	Description
1.	2019-12-19 15:14:09 EST	2019-12-19 15:14:09 EST	/My Company	Administrator	Manager	Scheduled check of GTI Server for new Callback Detectors Files	**Success**	Scheduled check of GTI Server for new Callback Detector File, and download if necessary
2.	2019-12-19 14:14:07 EST	2019-12-19 14:14:07 EST	/My Company	Administrator	Manager	Scheduled check of GTI Server for new Callback Detectors Files	**Success**	Scheduled check of GTI Server for new Callback Detector File, and download if necessary
3.	2019-12-19 13:14:49 EST	2019-12-19 13:14:55 EST	/My Company	Administrator	Sensor	Callback Detector Download	**Success**	Deploying updates to "NS9100_Miercom".
4.	2019-12-19 13:14:47 EST	2019-12-19 13:14:47 EST	/My Company	Administrator	Manager	Callback Detector Download to Manager	**Success**	Downloaded Callback Detector set to Manager.
5.	2019-12-19 13:14:05 EST	2019-12-19 13:14:47 EST	/My Company	Administrator	Manager	Scheduled check of GTI Server for new Callback Detectors Files	**Success**	Scheduled check of GTI Server for new Callback Detector File, and download if necessary
6.	2019-12-19 12:34:44 EST	2019-12-19 12:34:56 EST	/My Company	Administrator	Manager	Scheduled check of GTI Server for new Callback Detectors Files	**Failure**	Scheduled check of GTI Server for new Callback Detector File, and download if necessary
7.	2019-12-19 12:29:32 EST	2019-12-19 12:29:44 EST	/My Company	Administrator	Manager	Scheduled check of GTI Server for new Callback Detectors Files	**Failure**	Scheduled check of GTI Server for new Callback Detector File, and download if necessary
8.	2019-12-19 12:24:20 EST	2019-12-19 12:24:32 EST	/My Company	Administrator	Manager	Scheduled check of GTI Server for new Callback Detectors Files	**Failure**	Scheduled check of GTI Server for new Callback Detector File, and download if necessary
9.	2019-12-19 12:19:08 EST	2019-12-19 12:19:20 EST	/My Company	Administrator	Manager	Scheduled check of GTI Server for new Callback Detectors Files	**Failure**	Scheduled check of GTI Server for new Callback Detector File, and download if necessary
10.	2019-12-19 12:13:55 EST	2019-12-19 12:14:08 EST	/My Company	Administrator	Manager	Scheduled check of GTI Server for new Callback Detectors Files	**Failure**	Scheduled check of GTI Server for new Callback Detector File, and download if necessary

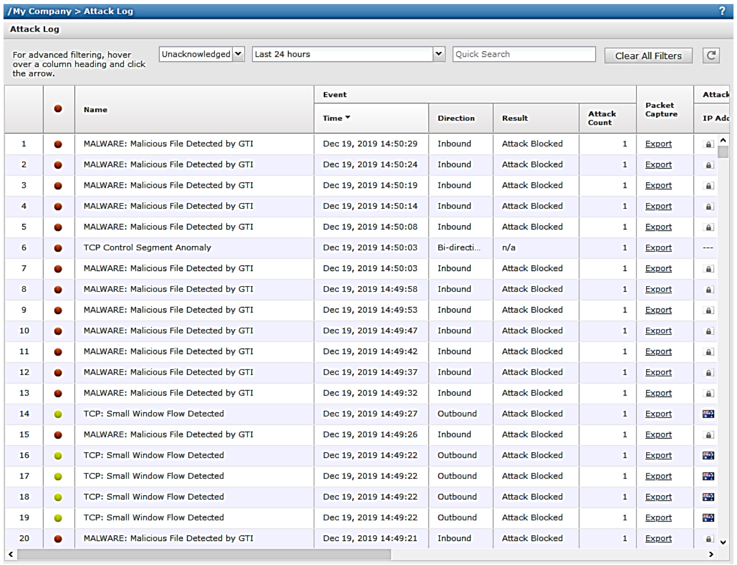
Items per page: 10 1 - 10 out of 622 items. Go to page: 1

For troubleshooting, the administrator can access a list of scheduled tasks and see the action, description and result to determine what remains to be remediated.

8.2 Logging and Reporting

Whenever a policy is violated or security event is triggered, the administrator should be notified. All reports should be searchable, saved, exportable and logged in real-time for later analysis. Visibility should be granular and support remediation.

The McAfee NS9x00 allows monitoring, recording and storage of all application activity, content and users across the network in real-time. Its robust searching capabilities provide instant visibility into log records over multiple periods, data types and domains.



/My Company > Attack Log

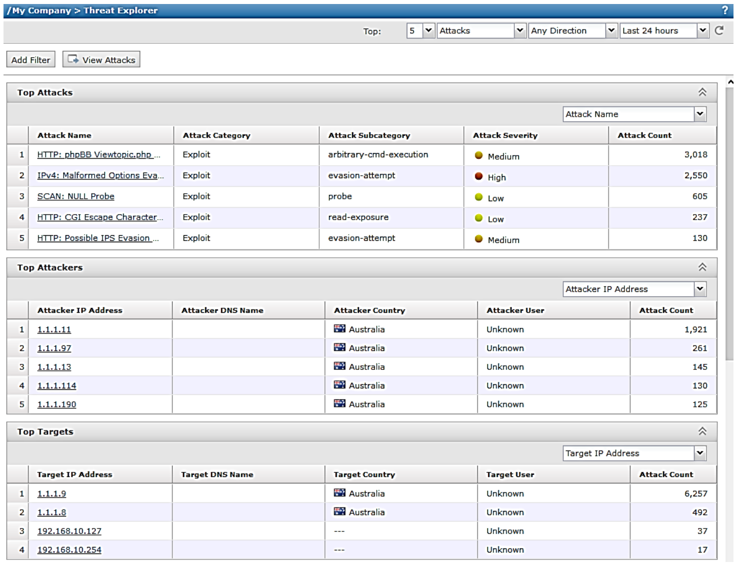
Attack Log

For advanced filtering, hover over a column heading and click the arrow.

Unacknowledged | Last 24 hours | Quick Search | Clear All Filters

	●	Name	Event				Packet Capture	Attack
			Time ▾	Direction	Result	Attack Count		IP Adc
1	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:50:29	Inbound	Attack Blocked	1	Export	🔒
2	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:50:24	Inbound	Attack Blocked	1	Export	🔒
3	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:50:19	Inbound	Attack Blocked	1	Export	🔒
4	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:50:14	Inbound	Attack Blocked	1	Export	🔒
5	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:50:08	Inbound	Attack Blocked	1	Export	🔒
6	🔴	TCP Control Segment Anomaly	Dec 19, 2019 14:50:03	Bi-directi...	n/a	1	Export	---
7	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:50:03	Inbound	Attack Blocked	1	Export	🔒
8	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:49:58	Inbound	Attack Blocked	1	Export	🔒
9	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:49:53	Inbound	Attack Blocked	1	Export	🔒
10	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:49:47	Inbound	Attack Blocked	1	Export	🔒
11	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:49:42	Inbound	Attack Blocked	1	Export	🔒
12	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:49:37	Inbound	Attack Blocked	1	Export	🔒
13	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:49:32	Inbound	Attack Blocked	1	Export	🔒
14	🟡	TCP: Small Window Flow Detected	Dec 19, 2019 14:49:27	Outbound	Attack Blocked	1	Export	🇦🇺
15	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:49:26	Inbound	Attack Blocked	1	Export	🔒
16	🟡	TCP: Small Window Flow Detected	Dec 19, 2019 14:49:22	Outbound	Attack Blocked	1	Export	🇦🇺
17	🟡	TCP: Small Window Flow Detected	Dec 19, 2019 14:49:22	Outbound	Attack Blocked	1	Export	🇦🇺
18	🟡	TCP: Small Window Flow Detected	Dec 19, 2019 14:49:22	Outbound	Attack Blocked	1	Export	🇦🇺
19	🟡	TCP: Small Window Flow Detected	Dec 19, 2019 14:49:22	Outbound	Attack Blocked	1	Export	🇦🇺
20	🔴	MALWARE: Malicious File Detected by GTI	Dec 19, 2019 14:49:21	Inbound	Attack Blocked	1	Export	🔒

The McAfee NS9x00 Attack Log shows blocked threats with a timestamp, direction, count, packet capture and IP address for further investigation.



/My Company > Threat Explorer

Top: 5 | Attacks | Any Direction | Last 24 hours

Add Filter | View Attacks

Top Attacks

Attack Name

	Attack Name	Attack Category	Attack Subcategory	Attack Severity	Attack Count
1	HTTP: phpBB Viewtopic.php ...	Exploit	arbitrary-cmd-execution	🟠 Medium	3,018
2	IPv4: Malformed Options Eva...	Exploit	evasion-attempt	🔴 High	2,550
3	SCAN: NULL Probe	Exploit	probe	🟡 Low	605
4	HTTP: CGI Escape Character...	Exploit	read-exposure	🟡 Low	237
5	HTTP: Possible IPS Evasion ...	Exploit	evasion-attempt	🟠 Medium	130

Top Attackers

Attacker IP Address

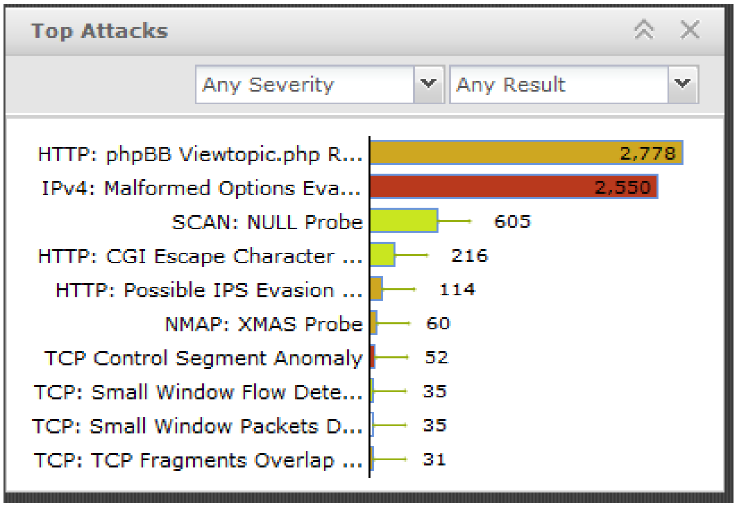
	Attacker IP Address	Attacker DNS Name	Attacker Country	Attacker User	Attack Count
1	1.1.1.11		🇦🇺 Australia	Unknown	1,921
2	1.1.1.97		🇦🇺 Australia	Unknown	261
3	1.1.1.13		🇦🇺 Australia	Unknown	145
4	1.1.1.114		🇦🇺 Australia	Unknown	130
5	1.1.1.190		🇦🇺 Australia	Unknown	125

Top Targets

Target IP Address

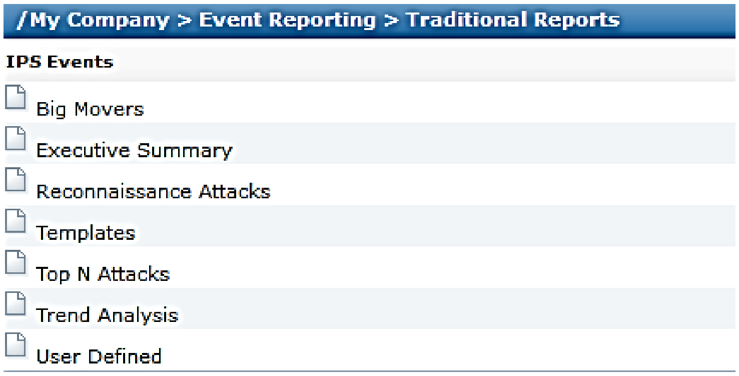
	Target IP Address	Target DNS Name	Target Country	Target User	Attack Count
1	1.1.1.9		🇦🇺 Australia	Unknown	6,257
2	1.1.1.8		🇦🇺 Australia	Unknown	492
3	192.168.10.127		---	Unknown	37
4	192.168.10.254		---	Unknown	17

The Threat Explorer shows the attack name, category, subcategory, severity and count of the top attacks. These attacks are also organized by IP address and location of attacker and target.



By looking at the Top Attacks, the administrator can identify the biggest threat vector and take appropriate actions to eliminate related vulnerabilities that most frequently put the network at risk.

The McAfee NS9x00 provided both out-of-box-report templates and the ability to customize reports.

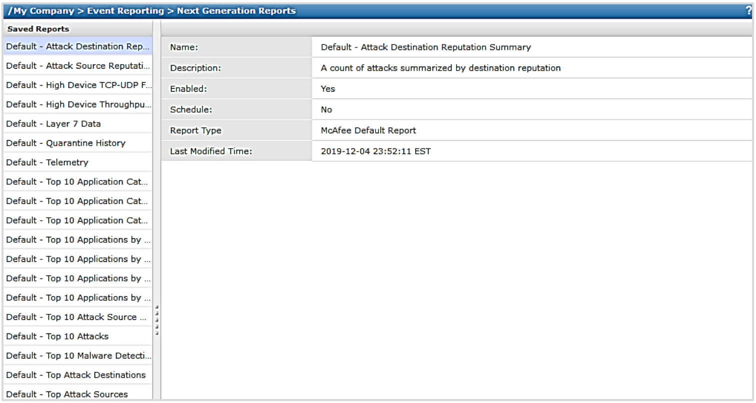


/My Company > Event Reporting > Traditional Reports

IPS Events

- Big Movers
- Executive Summary
- Reconnaissance Attacks
- Templates
- Top N Attacks
- Trend Analysis
- User Defined

Reporting can be done through any of the traditional reporting templates offered by the McAfee NS9x00 sensor.



/My Company > Event Reporting > Next Generation Reports

Saved Reports

- Default - Attack Destination Rep...
- Default - Attack Source Reputati...
- Default - High Device TCP-UDP F...
- Default - High Device Throughpu...
- Default - Layer 7 Data
- Default - Quarantine History
- Default - Telemetry
- Default - Top 10 Application Cat...
- Default - Top 10 Application Cat...
- Default - Top 10 Application Cat...
- Default - Top 10 Applications by ...
- Default - Top 10 Applications by ...
- Default - Top 10 Applications by ...
- Default - Top 10 Applications by ...
- Default - Top 10 Attack Source ...
- Default - Top 10 Attacks
- Default - Top 10 Malware Detecti...
- Default - Top Attack Destinations
- Default - Top Attack Sources

Name:	Default - Attack Destination Reputation Summary
Description:	A count of attacks summarized by destination reputation
Enabled:	Yes
Schedule:	No
Report Type	McAfee Default Report
Last Modified Time:	2019-12-04 23:52:11 EST

Customizable, next generation reports can be created for specific sets of criteria relevant to the network's needs.

9.0 Advanced Threat Defense (ATD) Integration

The McAfee ATD integrates as a virtual sandbox solution that takes suspicious samples and executes them in controlled environments to determine if they are malicious. It performs other heuristics and advanced virus detection techniques, working like a virtual honeypot to catch malware and separate samples from the data stream.

This solution also feeds the McAfee Cloud and Edge services with malware samples in real-time to enable immediate malware definitions – creating an impressive combination of NSM and ATD as a strong perimeter defense for enterprise networks seeking to comply with high data security and integrity standards.

10.0 Evader

The Evader is a ready-made attack lab that enables a quick mount of attacks against known vulnerabilities in Internet-accessible servers and client computers. This tool then mutates traffic in increasingly complex patterns in attempt to defeat intrusion prevention or detection systems as target exploits. The exploits tested in this case were the W32 RDP Cornficker exploit and PHPBB Post overflow exploit. We configured the Evader tool to execute all possible mutations of these attack variants with the McAfee NS9x00 in between our attacker and victim virtual machines.

In total, we launched 43,200 different evasions (unique IP/TCP fragmentation/scrambling mixtures) for each of the two attacks for a total of 86,400 strikes. The NS9x00 successfully prevented all evasion attempts, embedded in known malicious traffic and exploits.

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, 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.

By downloading, circulating or using this report 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.