



Miercom

August 2023
DR230809Q



Cisco Security and SD-WAN
Efficacy and Performance Evaluation

Table of Contents

1.0 Executive Summary	3
2.0 Introduction	5
2.1 Scope of Evaluation	5
2.2 Security and SD-WAN Products Evaluated	6
3.0 How We Did It	7
4.0 Malware Efficacy	8
4.1 Threat Categories Miercom AOST	9
5.0 Cisco Meraki Malicious URL Filtering	11
6.0 Cisco Catalyst Malicious URL Filtering	13
7.0 Cisco Meraki Malware Detection Efficacy	15
8.0 Cisco Catalyst Malware Detection Efficacy	17
9.0 Cisco Meraki Performance	19
10.0 Cisco Catalyst Performance	20
11.0 About Miercom	21
12.0 Customer Use and Evaluation	21
13.0 Use of This Report	21

1.0 Executive Summary

Cisco engaged Miercom to conduct a review of their converged security and SD-WAN technologies available through Catalyst and Meraki WAN appliances. Six models were reviewed in total, four Catalyst and two Meraki. Testing was comprised of security efficacy and throughput performance. The performance tests were conducted with SD-WAN configured for one of two environments. The first with directly attached internet (DIA) had all security features enabled on the devices under test (DUTs). The second environment - Secure SD-WAN overlay employed IPsec for encrypted transport and had other security features enabled.

Security services Miercom validated for this testing include:

- Application aware firewall
- Intrusion detection and prevention
- URL / content filtering
- Advanced malware protection
- Secure overlay services

Secure SD-WAN use cases validated by Miercom include:

- Direct Internet Access – NGFW, Advanced Malware Protection, URL-filtering, App control/Deep Packet inspection, Intrusion prevention and NAT
- Secure SD-WAN Overlay - IPsec, QoS, NGFW, App control/Deep Packet inspection, Intrusion prevention

Independent Testing Key Findings:

- Security efficacy testing for malware including “in the wild” sample sets proved Cisco Meraki and Catalyst WAN appliances were 25% better than the industry average for leading competitive solutions.
- Security efficacy testing with the latest phishing and polymorphic malicious URLs proved Cisco Meraki and Catalyst WAN appliances block 95 to 99% of these threats first exposure and 100% upon retest.
- Throughput achieved exceptional performance with an enterprise mix of traffic (EMIX) and achieved ZERO application transaction failures for Catalyst and Meraki WAN appliances in both tested scenarios – Direct Internet Access and Secure SD-WAN Overlay.

"Miercom Engineers proved in hands on extensive testing exceptional security efficacy and performance of Cisco's security and SD-WAN technologies delivered through Catalyst and Meraki WAN appliances.



The products proved in testing competitively superior protection against malware, malicious URLs, and other exploits.

Encrypted performance tests proved exceptional throughput with an enterprise mix of traffic (EMIX) and achieved ZERO application transaction failures.

Their security extension across a distributed workforce was easily implemented with a single configuration for each WAN appliance evaluated, affording consistent and effective protection.

Congratulations Cisco for achieving ***Miercom Certified Secure.***"

Rob Smithers
CEO, Miercom

2.0 Introduction

In the industry, security and SD-WAN vendors have different metrics and criteria to represent performance and security specifications on their datasheets. These range through file size, payload, ciphers, capacities, applications, weighted traffic/flows, and packet size. Some vendors will not publish critical specifications for properly sizing a use case deployment. The key objectives of this test review were to show the security and SD-WAN performance capabilities of Cisco Catalyst and Meraki WAN appliances in real-world scenarios.

Miercom conducted tests on two Cisco Meraki DUTs and four Cisco Catalyst DUTs. They included a series of security efficacy and performance tests with different features enabled/disabled using the same test methodology.

2.1 Scope of Evaluation

Miercom evaluated six Cisco WAN appliances: two Cisco Meraki DUTs (MX85 and MX68) and four Cisco Catalyst DUTs (C8300-2N2S-42TX, C8300-1N1S-6T, C8200-1N4T, and ISR 1100X) using real-world scenarios to compare their performance and the ability to measure any degradation seen from security enablement.

Testing focused on the following:



- Security Efficacy testing challenged Cisco's six WAN appliances' ability to block the latest malware and phishing URL threats. These modern web-based attacks increase the threat level against organizations globally, the majority of which exploit weaknesses at the network perimeter. But due to Cisco's advanced threat learning, we saw incredible threat blocking for all samples tested.
- Performance testing measured throughput using two scenarios:
 - Direct Internet Access – NGFW, Advanced Malware Protection, URL-filtering, App control/Deep Packet inspection, Intrusion prevention, and NAT.
 - Secure SD-WAN Overlay – IPsec, QoS, NGFW, App control/Deep Packet inspection, and Intrusion prevention.

2.2 Security and SD-WAN Products Evaluated

Cisco Meraki and Catalyst WAN appliances deliver a wide array of enterprise security and SD-WAN capabilities and provide the building blocks of SASE architecture. With a range of models for small branches to datacenters, feature highlights include:

Security	SD-WAN
<ul style="list-style-type: none">• Next-generation firewall (NGFW)• URL/content filtering• Advanced malware protection• Intrusion detection and prevention• Native Cisco Umbrella and 3rd party SSE integration	<ul style="list-style-type: none">• High quality application-based SD-WAN fabric technologies• Multicloud onramps with deep public cloud provider integrations• Advanced end-to-end visibility with ThousandEyes• 5G fixed wireless access

Cisco Meraki and Catalyst WAN appliances together are recognized to address the most enterprise use cases on the market.

Meraki WAN Appliances	Catalyst WAN Appliances
	
<i>Enterprises looking to streamline branch operations and improve security with SD-WAN</i>	<i>Enterprises looking to integrate SD-WAN and security into existing environments</i>
https://meraki.cisco.com	https://www.cisco.com/...

3.0 How We Did It

Testing employed state of the art test systems, including Miercom's Advanced Offensive Security Test Suite (AOST) and other third-party test and measurement systems from Spirent and Keysight Technologies.

Miercom uses our Advanced Offensive Security Test Suite to assess security products for their ability to detect and block malware, malicious URLs and stress data loss prevention techniques using real-world scenarios. Our comprehensive testing process can replicate controlled induced catastrophic breach events. Miercom AOST consists of zero-day malware samples collected from honeypots from locations around the world. Miercom also has custom vulnerability and attack scripts for conducting white hat penetration and resiliency testing.

BreakingPoint 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.

Engineers examined the throughput performance of the Cisco Meraki and Catalyst appliances in configurations with security services fully enabled. Testing was intended to measure the effect - if any - that security services enablement would have on the DUT's throughput performance. Miercom used the vendor recommended configuration on all the devices tested, unless otherwise specified.

Keysight (Ixia) BreakingPoint
Version 9.30.128

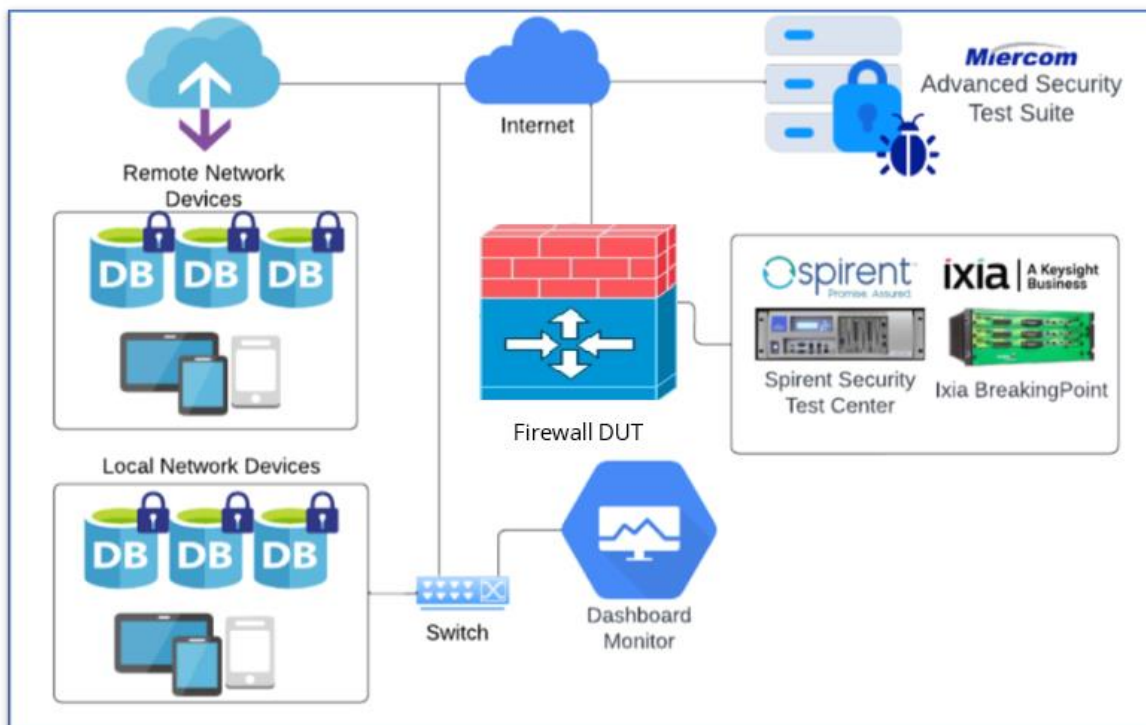
This network testing appliance delivers increasing loads of TCP traffic to the network through the DUT to determine maximum throughput rates. It also provides a robust and realistic environment for security testing.

4.0 Malware Efficacy

Testing focused on the protection against a multitude of threat categories (see list on page 9). The Miercom Security Test Suite Server used in this testing can simulate a hacker's attack and also serves as the hosts and collector from honeypot sources of hundreds of thousands of malware samples each day that are used in testing to characterize the breadth of protection for the device under test.

Samples from the Miercom malware server are used in industry-wide studies to index different product classes for their malware prevention and other network security countermeasures. Common malware types are botnets and Remote Access Trojans (RATs). An emphasis is placed on active threats, advanced evasion techniques and advanced persistent threats which are more complex and challenging categories for security solutions to identify.

Simulated attacks from the untrusted zone consisted of an attempted download of malicious files. A successful block is logged when the simulated victim client either cannot download the malware sample, or otherwise can neutralize the malicious sample, place it in quarantine, sandbox, etc.



4.1 Threat Categories Miercom AOST

Active Threat
Current threats that are lethal, recent, and prevalent in the threat-scape for businesses today. This type of malware actively does irreparable harm to the host victims.
Backdoor
Remote access attacks that use port binding, control, command servers and dormant malware to infiltrate networks using legitimate programs or platform to go unrecognized.
Botnets
Communicating programs delivering spam and Distributed Denial of Service (DDoS) attacks. This type of malware is used to conduct wider scale attacks. It may be any component to help proliferate a botnet exploit.
Legacy
Malware that is mature and should be considered “well known” and expected to be detected by most signature-based detection countermeasures. This malware set is the most extensive and challenging to countermeasures with limited device memory for signature detection.
Malicious Documents
Seemingly benign electronic documents (e.g., MS Word, Adobe PDF) that contain malicious coding “macros” alongside plain-text data to seem legitimate while infecting the system upon opening.

Remote Access Trojans (RATs)

Malware an attacker uses to gain full administrative privileges and remote control of a target computer. RATs are often downloaded along with seemingly legitimate user-requested programs such as video games or via phishing email.

Tor Trojan Exploit (TOR)

Malware that interacts with TOR browser and/or uses the TOR network with multi-layer encryption that collects personal data and sends to a C&C server.

Advanced Evasion Techniques (AETs)

Threats that are most obfuscated to block with conventional malware scanners and IPS. The threats are often delivered in components that work together once they reestablish connection at the infected host.

Advanced Persistent Threats (APTs)

Threats that allow for continuous hacking with payloads opened at the administrative level. Even after first discovery and attempts to remove, the malware persists on the infected hosts and elsewhere in the network.

Modified Malware

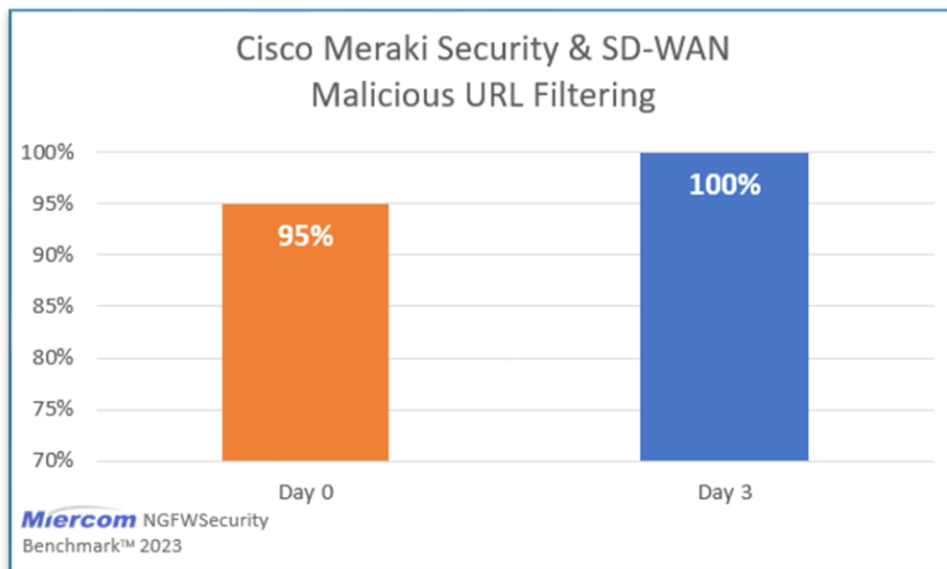
Original malware, detectable by public repositories, but is modified with techniques that allow it to now evade most signature-based detection countermeasures.

Polymorphic, Zero-Day Malware

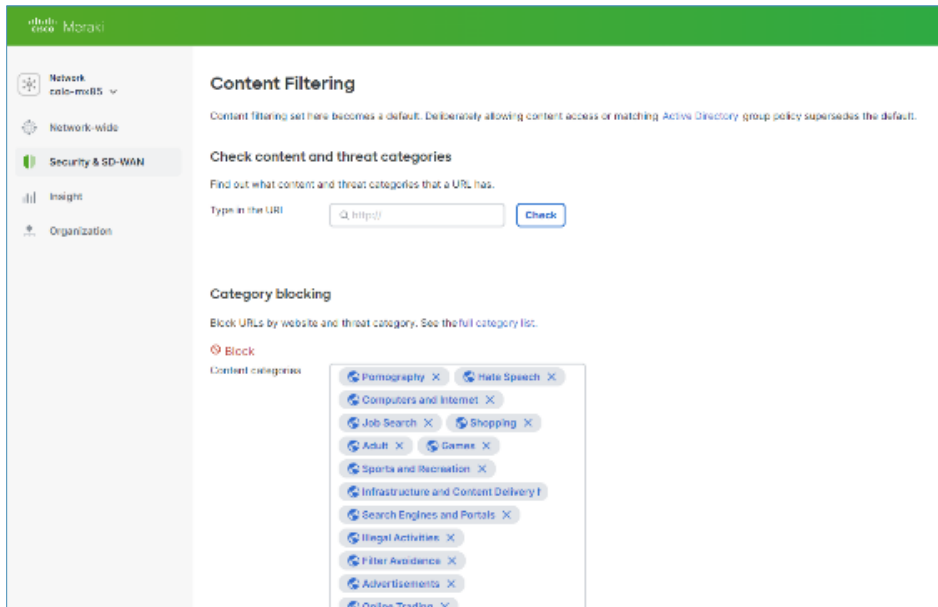
Malware that self-mutates, presenting as new threat as if modifies itself. This constantly changing effect makes this malware strain more difficult to fully detect the new strains of malware.

5.0 Cisco Meraki Malicious URL Filtering

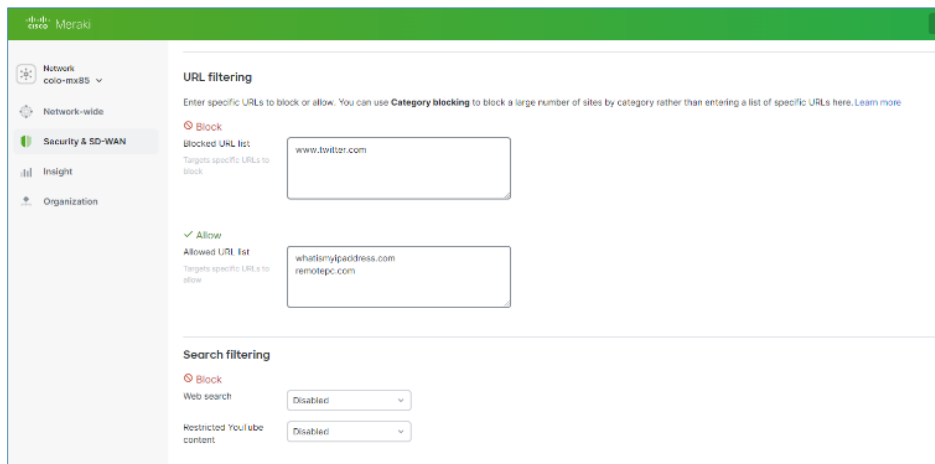
Miercom conducted Malicious URL Filtering tests on the Cisco Meraki WAN appliances. Cisco Meraki successfully proved 95% effective at Malicious URL Filtering, blocking samples from five sets of tests each with 500 malicious phishing and business email compromise URLs. Cisco Meraki achieved a perfect score blocking phishing and other malicious URLs after retesting sample sets within 72 hours. Samples were obtained open source from OpenPhish.com (same day) and other sources.



Cisco Meraki successfully proved a 95% block rate on first exposure to DAY 0 Malicious URLs including phishing and business email compromise samples. Meraki blocked 475 out of 500 malicious URLs tested that were fresh, not more than 24 hours known by commercial threat intelligence. No false positives, false blocked URLs detected. Samples were obtained open source and honeypots (same day samples). No false positives, false blocked URLs detected. Upon a retest DAY 3, 100% of the malicious URLs were blocked due to Cisco's advanced threat learning.

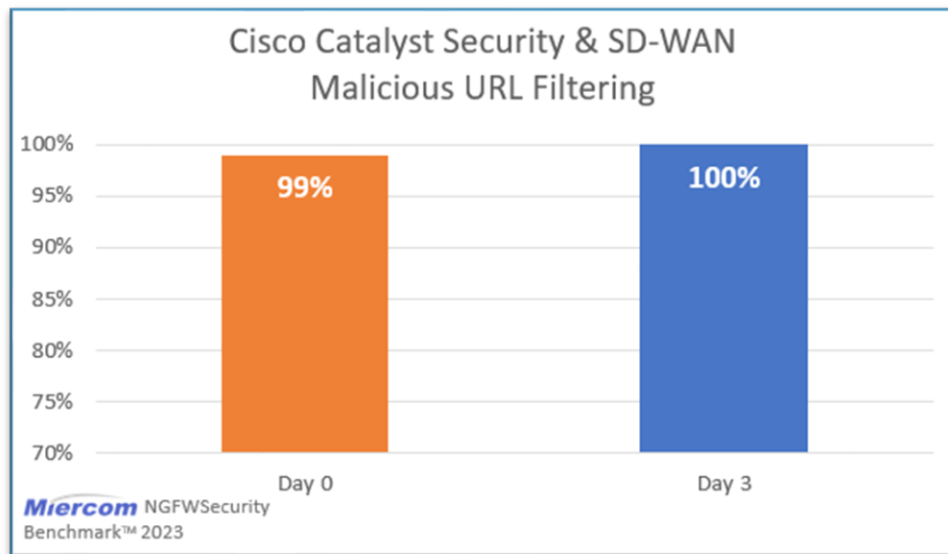


Cisco Meraki features a graphical user interface that was extremely easy to use including setting up for web/URL filtering. Their breadth and ease of this interface allow for quicker more effective time to deploy as well as reduction of human error bottom line leading to more effective secure protected network and QOE.

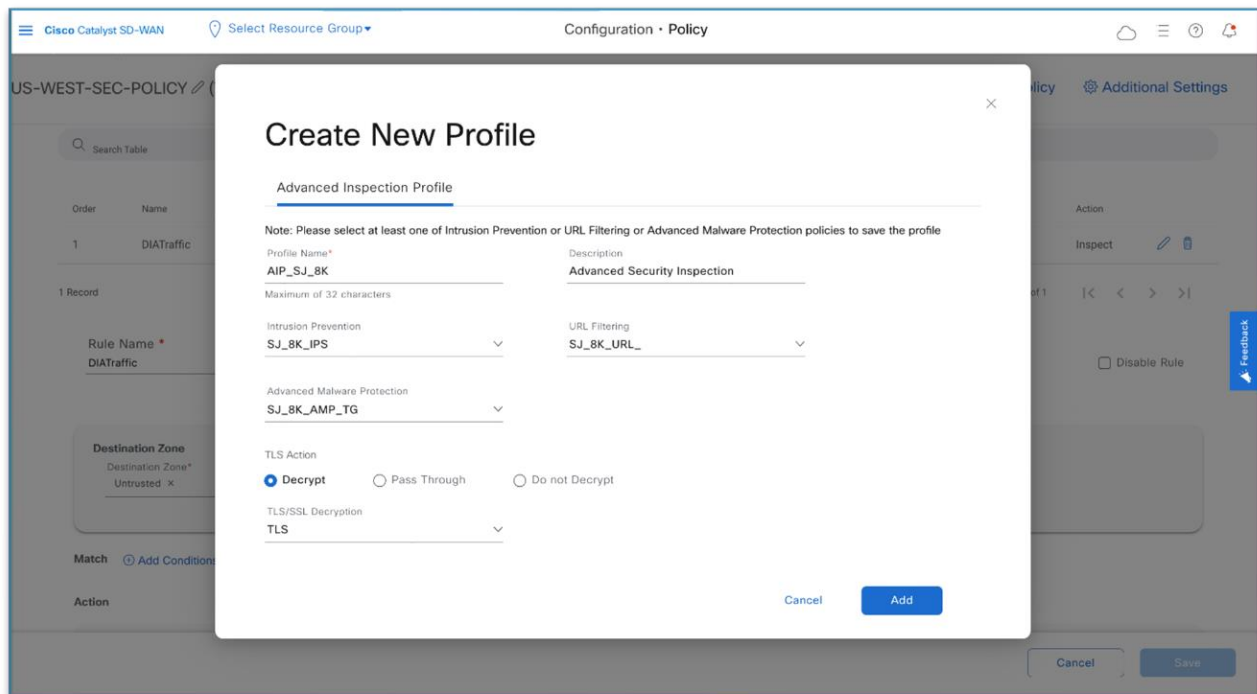
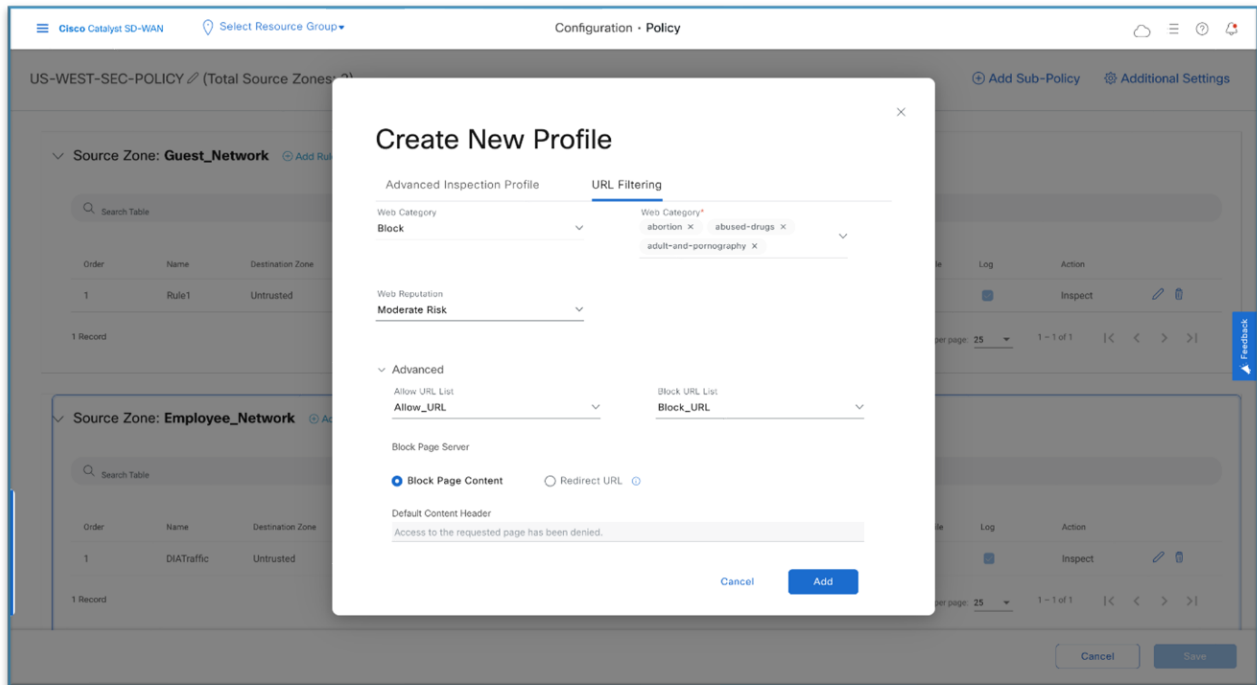


6.0 Cisco Catalyst Malicious URL Filtering

Miercom conducted Malicious URL filtering tests on the Cisco Catalyst WAN appliances. Cisco Catalyst successfully proved 99% effective at Malicious URL filtering, blocking five sets of tests each with 500 malicious phishing and business email compromise URLs. Catalyst achieved a perfect score blocking phishing and other malicious URLs after retesting sample sets within 72 hours. Samples were obtained open source from OpenPhish.com (same day) and other sources.



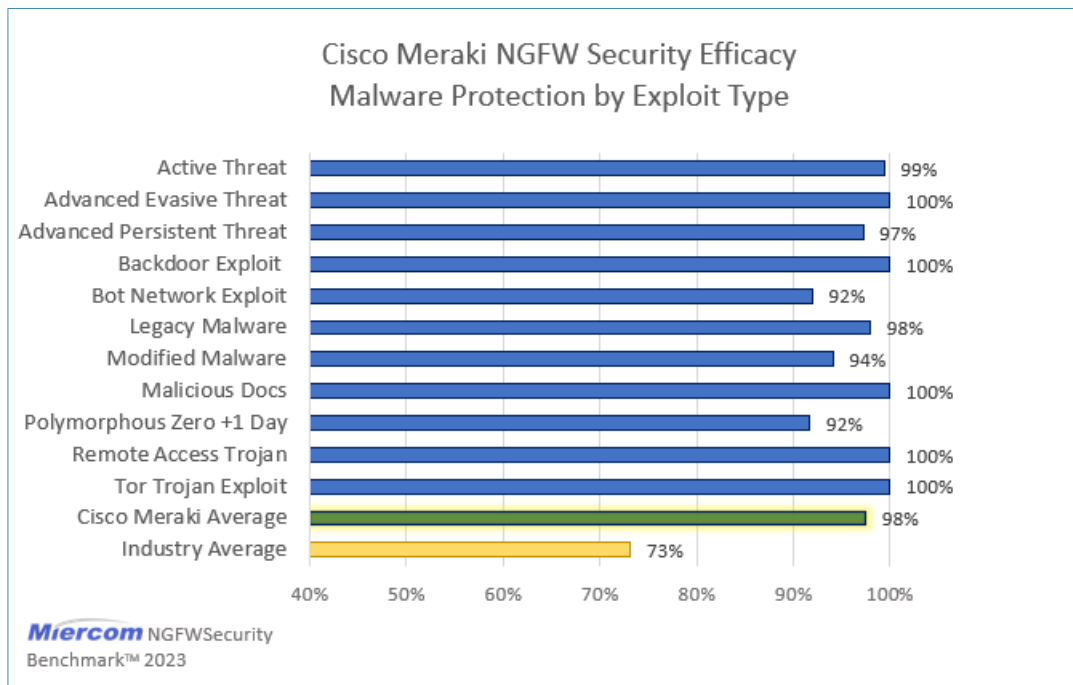
Cisco Catalyst successfully proved 99% block rate on first exposure to DAY 0 Malicious URLs including phishing and business email compromise samples. Catalyst achieved a near perfect score blocking newly discovered phishing and other malicious URLs. Samples were obtained open source from OpenPhish.com (same day samples). No false positives, false blocked URLs detected. Upon a retest DAY 3, 100% of the malicious URLs were blocked due to Cisco's advanced threat learning.



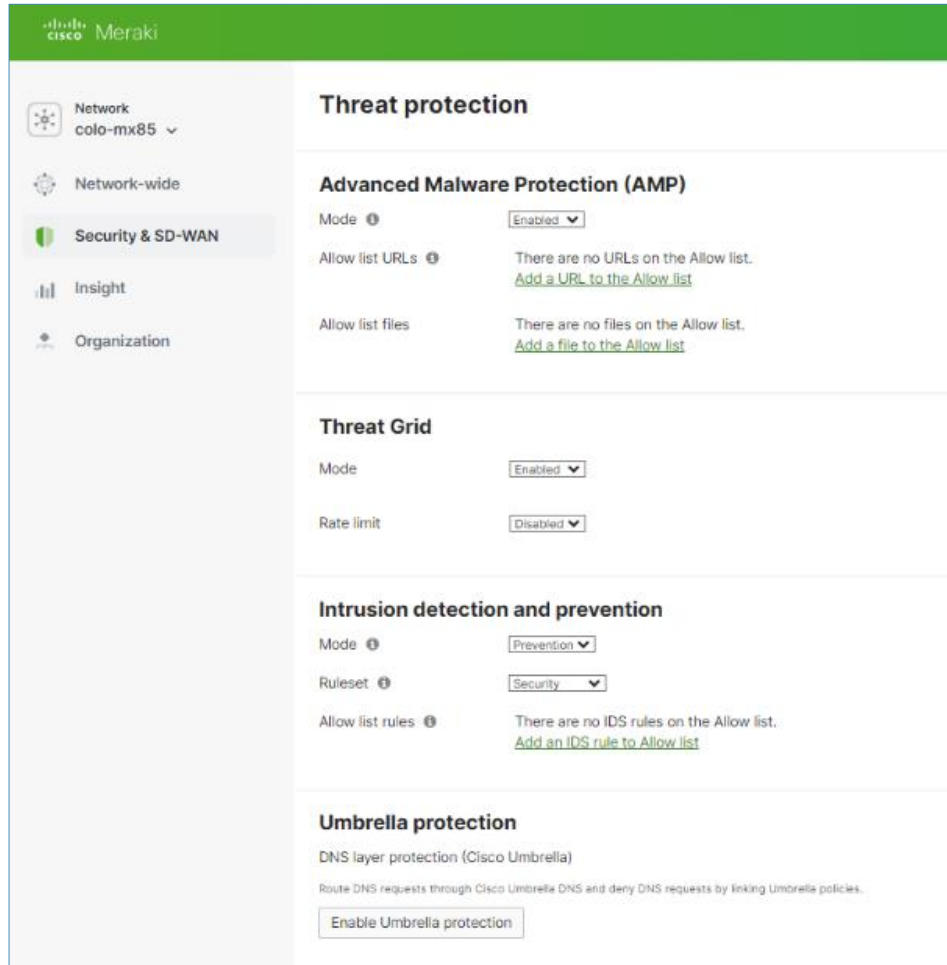
Cisco Catalyst also features a graphical user interface that was extremely easy to use including setting up for web/URL filtering. Their breadth and ease of this interface allow for quicker more effective time to deploy as well as reduction of human error bottom line leading to more effective secure protected network and QOE.

7.0 Cisco Meraki Malware Detection Efficacy

Miercom conducted Security Efficacy Malware Protection tests by exploit type on the Cisco Meraki DUTs. Cisco Meraki WAN appliances proved 98% effective at Malware Detection Efficacy, 25% better overall compared to the competitive industry average of other NGFW security products tested. Cisco Meraki WAN appliances prevented 100% of AET, Backdoor, Malicious Docs, RAT, and TOR exploits. It had excellent protection against both active and modified threats.



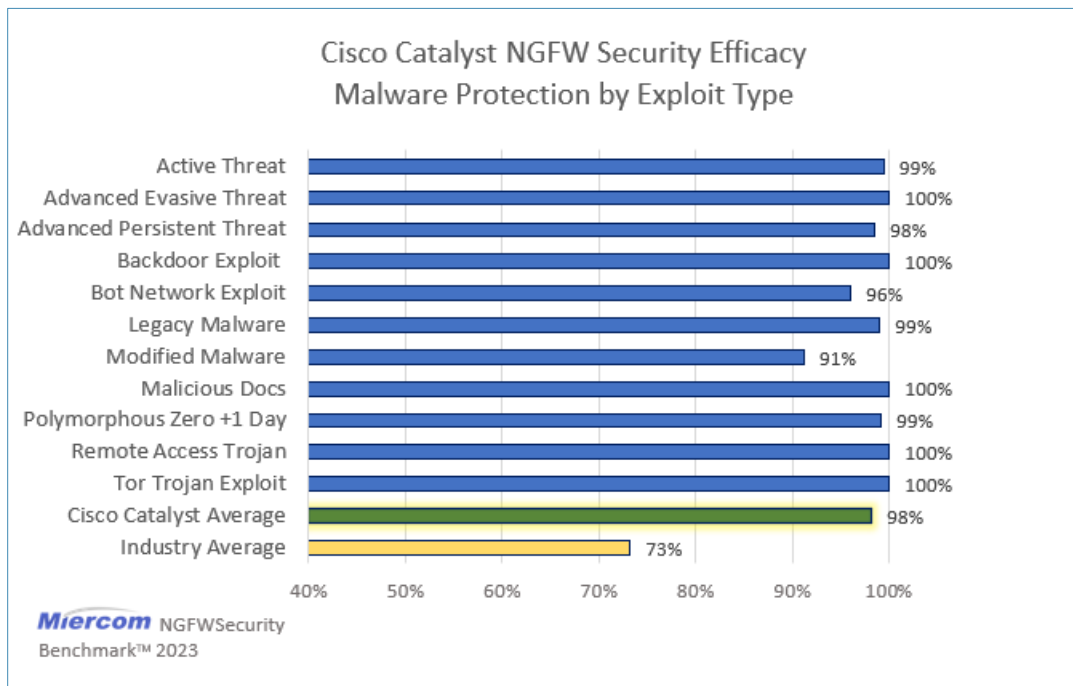
Cisco Meraki proved 98% Malware Detection Efficacy, 25% better overall compared to competitive industry average of other NGFW security products tested. Cisco Meraki prevented 100% of AET, Backdoor, Malicious Docs, RAT, and TOR exploits. It had excellent protection against both active and modified threats. Active threat and modified malware are fresh 2023 malware samples likely not in any signature databases.



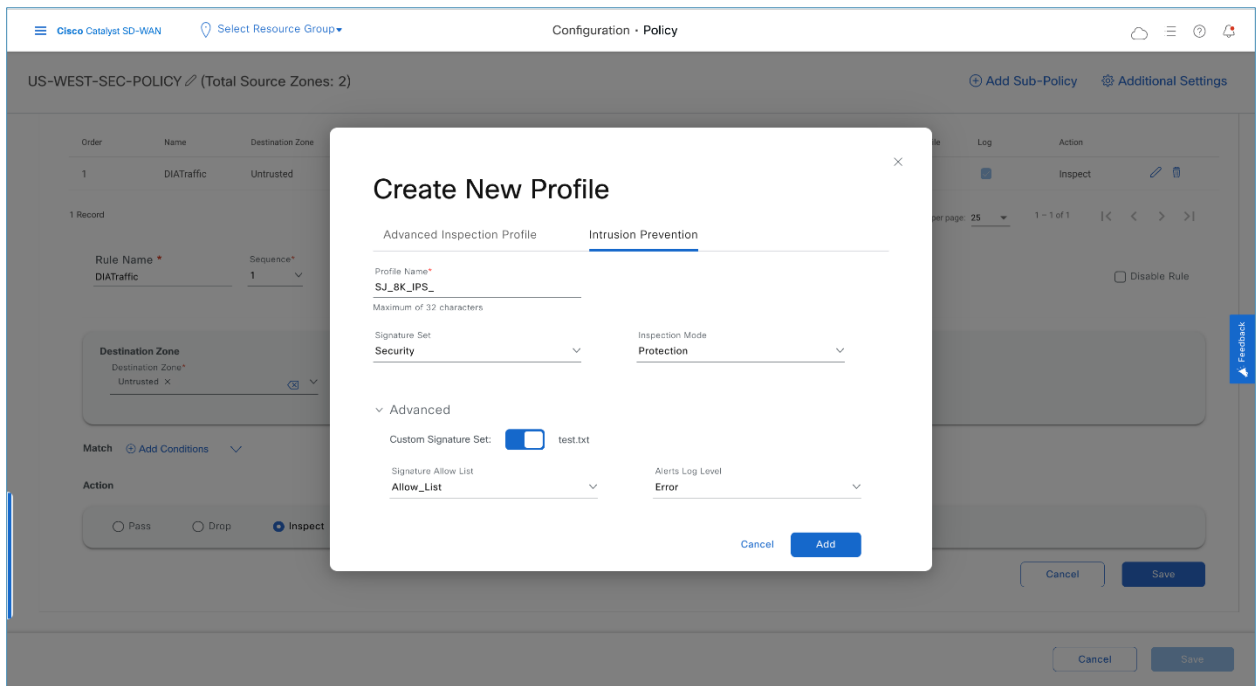
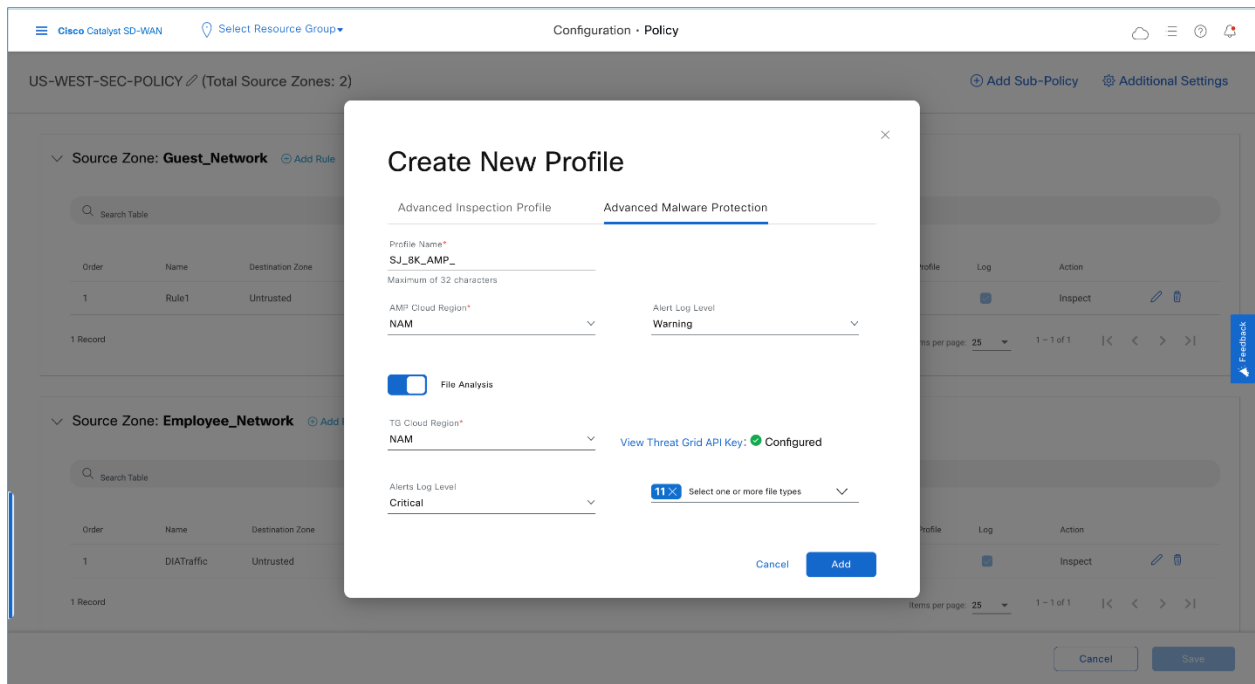
Cisco Meraki features a graphical user interface that was extremely easy to use including setting up for intrusion detection prevention and Advanced Malware Protection (AMP). Their breadth and ease of this interface allow for quicker more effective time to deploy as well as reduction of human error bottom line leading to more effective secure protected network and overall exceptional customer quality of experience.

8.0 Cisco Catalyst Malware Detection Efficacy

Miercom conducted NGFW Security Efficacy Malware Protection tests by Exploit Type on the Cisco Catalyst DUTs. Cisco Catalyst WAN appliances proved 98% Malware Detection Efficacy, 25% better overall compared to competitive industry average of other NGFW security products tested. Cisco Catalyst WAN appliances prevented 100% of AET, Backdoor, Malicious Docs, RAT, and TOR exploits. It had excellent protection against both active and modified threats.



Cisco Catalyst proved 98% Malware Detection Efficacy, 25% better overall compared to competitive industry average. Cisco Catalyst prevented 100% of AET, Backdoor, Malicious Docs, RAT, and TOR exploits. It had excellent protection against both active and modified threats. Active threat and modified malware are fresh 2023 malware samples not likely to be found in any signature databases.

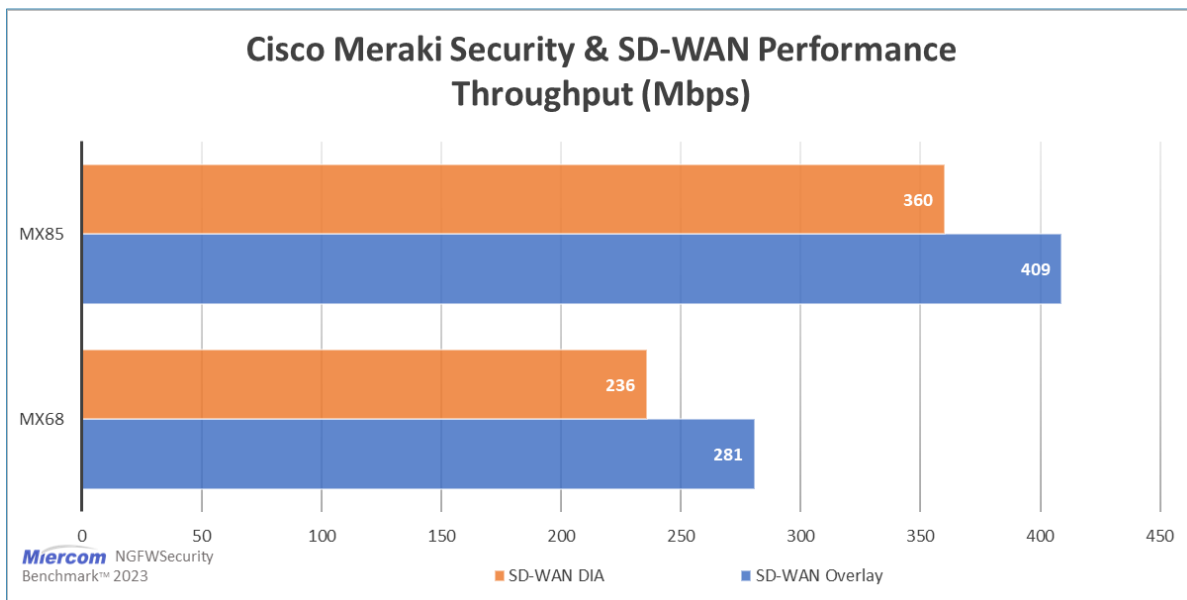


Miercom tested Cisco's newest software release, 17.12 / 20.12 with *guided workflows featuring smart default settings*. These smart templates require minimal customer configuration changes. Minimizing configuration changes required remove human error and allows for a quicker more effective deployment. It also allows for a better protected network and overall improved quality of experience (QOE). Testing was conducted after configuring the DUTs with these guided workflows.

9.0 Cisco Meraki Performance

Miercom conducted Performance Throughput tests on the Cisco Meraki DUTs. Cisco Meraki MX68 and MX85 WAN appliance performance test results shown below provided excellent throughput with both SD-WAN scenarios. 1) Direct Internet Access (DIA) and 2) Secure SD-WAN Overlay.

The DIA use case has all security features enabled including NGFW with Application Control, Advanced Malware Protection, URL Filtering, Intrusion Protection and NAT. The Secure SD-WAN overlay has IPsec enabled, QoS, Application Control, Deep Packet Inspection, and Intrusion Prevention Service. Traffic mix for testing was default delivered using the Keysight BreakingPoint test system.

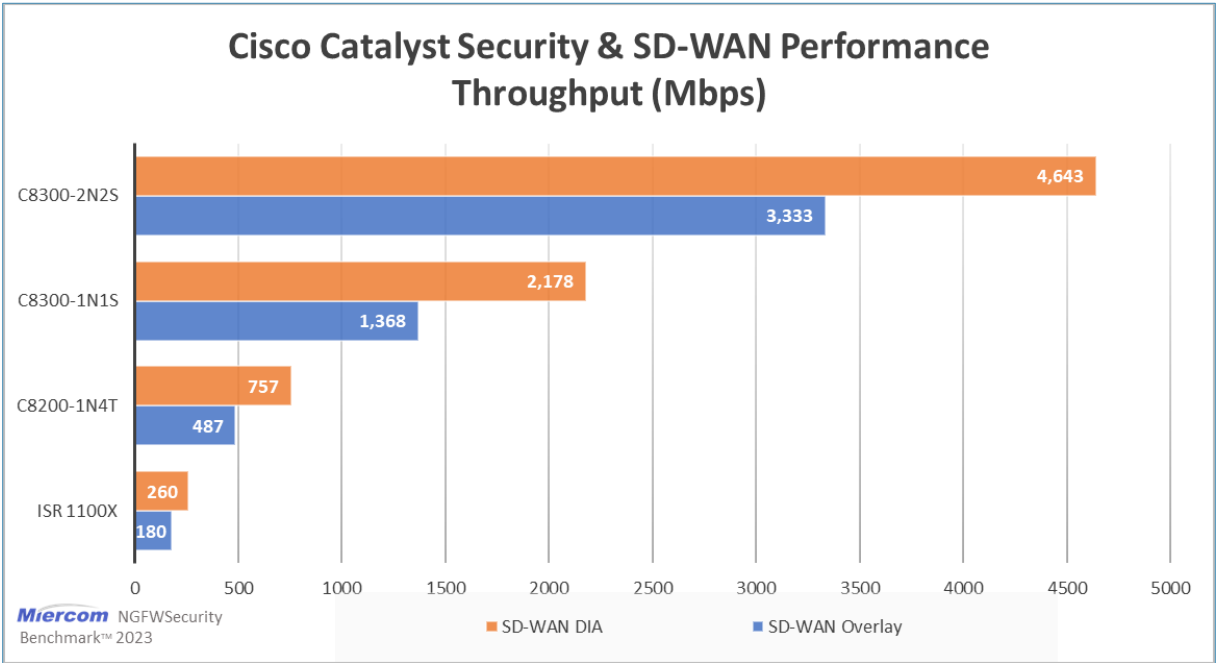


Cisco Meraki MX68 and MX85 performance test results shown above prove excellent throughput with both SD-WAN scenarios: 1) Direct Internet Attached (DIA) and 2) Secure SD-WAN Overlay, Cisco Meraki proved exceptional throughput performance for both encrypted and unencrypted testing. This test employed an enterprise application mix (EMIX) of traffic was used and there was ZERO application transaction failures. The overlay performance outperformed DIA due to malware protection being disabled.

10.0 Cisco Catalyst Performance

Miercom conducted Performance Throughput tests on four Cisco Catalyst DUTs including the Cisco Catalyst 1100X, 8200, and two models of C8300. Performance test results below show these products provide excellent throughput with both SD-WAN scenarios: 1) Direct Internet Access (DIA) and 2) Secure SD-WAN Overlay.

The DIA use case included all security features enabled including NGFW with Application Control, Advanced Malware Protection, URL Filtering, Intrusion Protection and NAT. The Secure SD-WAN Overlay has IPsec enabled, QoS, Application Control, Deep Packet Inspection, and Intrusion Prevention Service. Traffic mix for testing was a default enterprise mix (EMIX) delivered using the Keysight BreakingPoint test system and repeated multiple times..



Cisco Catalyst 1100X, 8200, and 8300 (C8300-2N2S-4T2X and C8300-1N1S-6T) performance test results shown above prove excellent throughput with both SD-WAN scenarios. Testing proved exceptional throughput performance for both encrypted and unencrypted testing. In this test, an enterprise application mix (EMIX) of traffic was used and there was ZERO application transaction failures.

11.0 About Miercom

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

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Additionally, Miercom services comprehensive certification and test programs, including Certified Interoperable, Reliability Assured, 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.

12.0 Customer Use and Evaluation

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform an on-site evaluation.

13.0 Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. 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. By downloading, circulating, or using this report you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit <https://miercom.com/tou>.